Blockchain & Cryptocurrency Regulation

2020

Second Edition

Contributing Editor
Josias N. Dewey

Global Legal Insights
Blockchain & Cryptocurrency Regulation

2020, Second Edition
Contributing Editor: Josias N. Dewey
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS - BLOCKCHAIN & CRYPTOCURRENCY REGULATION

2020, SECOND EDITION

Contributing Editor
Josias N. Dewey, Holland & Knight LLP

Production Editor
Sam Friend

Senior Editors
Caroline Collingwood
Rachel Williams

General Consulting Editor
Alan Falach

Publisher
Rory Smith

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Josias N. Dewey of Holland & Knight LLP for all of his assistance.

Published by Global Legal Group Ltd.
59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 207 367 0720 / URL: www.glgroup.co.uk

ISBN 978-1-912509-97-3
ISSN 2631-2999

Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY
October 2019

CONTENTS

Preface Josias N. Dewey, *Holland & Knight LLP*

Foreword Aaron Wright, *Enterprise Ethereum Alliance*

Glossary The Editor shares key concepts and definitions of blockchain

Industry

Promoting innovation through education: The blockchain industry, law enforcement and regulators work towards a common goal
Jason Weinstein & Alan Cohn, *The Blockchain Alliance* 1

The loan market, blockchain, and smart contracts: The potential for transformative change
Bridget Marsh, *LSTA* & Josias N. Dewey, *Holland & Knight LLP* 5

A year of progress – the Wall Street Blockchain Alliance and the ongoing evolution of blockchain and cryptoassets
Ron Quaranta, *Wall Street Blockchain Alliance* 14

General chapters

Blockchain and intellectual property: A case study
Joshua Krumholz, Ieuan G. Mahony & Brian J. Colandreo
Holland & Knight LLP 18

The custody of digital assets – 2020
Jay G. Baris, *Shearman & Sterling LLP* 35

Cryptocurrency and other digital assets for asset managers
Gregory S. Rowland & Trevor I. Kiviat, *Davis Polk & Wardwell LLP* 52

The yellow brick road for consumer tokens: The path to SEC and CFTC compliance. An update
David L. Concannon, Yvette D. Valdez & Stephen P. Wink,
Latham & Watkins LLP 64

Custody and transfer of digital assets: Key U.S. legal considerations
Michael H. Krimminger, Colin Lloyd & Sandra Rocks,
Cleary Gottlieb Steen & Hamilton LLP 88

An introduction to virtual currency money transmission regulation
Michelle Ann Gitlitz & Michael J. Barry, *Blank Rome LLP* 101

Cryptocurrency compliance and risks: A European KYC/AML perspective
Fedor Poskriakov, Maria Chiriaeva & Christophe Cavin,
Lenz & Staehelin 119

The potential legal implications of securing proof of stake-based networks
Angela Angelovska-Wilson, *DLx Law* &
Evan Weiss, *Proof of Stake Alliance* 133

Legal issues surrounding the use of smart contracts
Stuart Levi, Alex Lipton & Cristina Vasile,
Skadden, Arps, Slate, Meagher & Flom LLP 155

U.S. Federal Income Tax implications of issuing, investing and trading in cryptocurrency
Mary F. Voce & Pallav Raghuvanshi, *Greenberg Traurig, LLP* 171

Stablecoins: A global overview of regulatory requirements in Asia Pacific, Europe, the UAE and the USA
David Adams & Jesse Overall, *Clifford Chance LLP*
Jason Rozovsky, *R3* 182

Blockchain and the GDPR: Co-existing in contradiction?
John Timmons & Tim Hickman, *White & Case LLP* 202

General chapters

Smart contracts in the derivatives space
Jonathan Gilmour & Vanessa Kalijnikoff Battaglia, *Travers Smith LLP* 220

Distributed ledger technology as a tool for streamlining transactions
Douglas Landy, James Kong & Jonathan Edwards, *Milbank LLP* 232

Country chapters

Argentina Juan M. Diehl Moreno & Santiago Eraso Lomaquiz, *Marval, O'Farrell & Mairal* 245

Australia Peter Reeves, *Gilbert + Tobin* 251

Austria Ursula Rath & Thomas Kulnigg, *Schoenherr Attorneys at Law* 263

Bermuda Mary V. Ward & Adam Bathgate, *Carey Olsen Bermuda Limited* 271

Brazil Martim Machado & Julia Fontes Abramof, *CGM Advogados* 282

British Virgin Islands Clinton Hempel & Mark Harbison, *Carey Olsen* 288

Canada Simon Grant, Kwang Lim & Matthew Peters, *Bennett Jones LLP* 294

Cayman Islands Alistair Russell & Dylan Wiltermuth, *Carey Olsen* 308

China Jacob Blacklock & Shi Lei, *Lehman, Lee & Xu* 316

Cyprus Karolina Argyridou, Prodromos Epifaniou & Akis Papakyriacou, *Verita Legal K. Argyridou & Associates LLC* 326

Estonia Priit Lätt, *PwC Legal Estonia* 332

France Christophe Perchet, Juliette Loget & Stéphane Daniel, *Davis Polk and Wardwell LLP* 344

Germany Dr Stefan Henkelmann & Lennart J. Dahmen, *Allen & Overy LLP* 355

Gibraltar Joey Garcia & Jonathan Garcia, *ISOLAS LLP* 367

Guernsey David Crosland & Felicity Wai, *Carey Olsen (Guernsey) LLP* 376

Hong Kong Yu Pui Hang (Henry Yu), *L&Y Law Office / Henry Yu & Associates* 387

India Anu Tiwari & Rachana Rautray, *AZB & Partners* 401

Ireland Maura McLaughlin, Pearse Ryan & Caroline Devlin, *Arthur Cox* 407

Japan Taro Awataguchi & Takeshi Nagase, *Anderson Mōri & Tomotsune* 414

Jersey Christopher Griffin, Emma German & Holly Brown, *Carey Olsen Jersey LLP* 424

Korea Jung Min Lee, Samuel Yim & Joon Young Kim, *Kim & Chang* 433

Liechtenstein Dr Ralph Wanger, *BATLINER WANGER BATLINER Attorneys at Law Ltd.* 440

Malta Malcolm Falzon & Alexia Valenzia, *Camilleri Preziosi Advocates* 445

Mexico Miguel Ángel Peralta García, Pedro Said Nader & Patrick Seaver Stockdale Carrillo, *Basham, Ringe y Correa, S.C.* 455

Montenegro Marija Vlajković & Luka Veljović, *Moravčević Vojnović i Partneri AOD Beograd in cooperation with Schoenherr* 463

Netherlands Björn Schep, Willem Röell & Christian Godlieb, *De Brauw Blackstone Westbroek* 466

Portugal Filipe Lowndes Marques, Mariana Albuquerque & João Lima da Silva *Morais Leitão, Galvão Teles, Soares da Silva & Associados [Morais Leitão]* 476

Russia Vasilisa Strizh, Dmitry Dmitriev & Anastasia Kiseleva, *Morgan, Lewis & Bockius LLP* 486

Serbia	Bojan Rajić & Mina Mihaljčić, *Moravčević Vojnović i Partneri AOD Beograd in cooperation with Schoenherr*	494
Singapore	Franca Ciambella & En-Lai Chong, *Consilium Law Corporation*	500
South Africa	Angela Itzikowitz & Ina Meiring, *ENSafrica*	512
Spain	Alfonso López-Ibor, Pablo Stöger & Olivia López-Ibor, *Ventura Garcés López-Ibor*	519
Switzerland	Daniel Haeberli, Stefan Oesterhelt & Alexander Wherlock, *Homburger AG*	524
Taiwan	Robin Chang & Eddie Hsiung, *Lee and Li, Attorneys-at-Law*	536
United Arab Emirates	Abdulla Yousef Al Nasser, Flora Ghali & Nooshin Rahmannejadi, *Araa Group Advocates and Legal Consultants*	543
United Kingdom	Stuart Davis, Sam Maxson & Andrew Moyle, *Latham & Watkins LLP*	554
USA	Josias N. Dewey, *Holland & Knight*	565
Venezuela	Luisa Lepervanche, *Mendoza, Palacios, Acedo, Borjas, Páez Pumar & Cía. (Menpa)*	575

PREFACE

Over the last two years, an obscure technology once associated only with the virtual currency Bitcoin, has become one of the most important technologies under development today. No longer known only as the technology on which Bitcoin was built, it has either been deployed or is under active development in virtually every industry. Financial services, healthcare, energy, capital markets, and many other industries are seeing legacy technology challenged by proposed blockchain-based solutions.

Blockchain has also exploded in terms of its geographic impact. Once a novelty that was only familiar to people in a handful of countries, the technology is now relevant to the global economy. In some countries, like Venezuela, virtual currency has taken a prominent role in the day-to-day lives of ordinary citizens. Yet, for all of the interest, popularity and media attention, many, including lawyers, struggle to understand the underpinnings of the technology and its implications for policymakers and other officials. This difficulty is compounded by the extraordinarily broad application of the technology across numerous industries. Certain implementations of the technology look very little like others. Some seek to supplement or replace traditional fiat currency, while others have no native virtual currency at all. Some are accessible by anyone with a computer or smart phone, while others are only accessible by those having credentials. This diversity of implementations and use cases, together with misguided statements espousing "absolute truths" about the technology, lead to confusion for most trying to tackle blockchain.

While blockchain has taken a much more prominent role in society, it remains a relatively nascent technology, having existed for less than ten years. This brief history has caused tension when the technology has been deployed in areas traditionally subject to extensive regulation, such as capital-raising and money transmission. Policymakers and other officials have often struggled to apply laws crafted decades ago, in many cases, built on assumptions now being challenged by the technology. In part, this continues to be driven by the technology's ability to disintermediate market participants, many of whom have traditionally been relied upon as unofficial gatekeepers in certain industries. No consistent policy has yet to evolve, with numerous states within the U.S. taking very different approaches to the technology, while the U.S. government has relied on its agencies to navigate the myriad of issues. The picture is no clearer on the international stage, where some nations have sought to foster the growth of the technology, and others have sought to eliminate the technology from their jurisdiction. This uncertainty has contributed to the lack of commercially deployed blockchain solutions, and many of the following chapters focus on these grey areas where much work remains to be done.

Our hope is that this publication will provide the reader with an understanding of some of the most critical issues facing practitioners and others involved in this area of technology and policy. The diversity of jurisdictions covered by this publication also provides a glimpse into how various governments have approached regulating this technology. Many have tried to balance their desire to foster innovation and the development of the technology in their country, while protecting their citizens from fraud or other harm. There is no doubt that this debate has only just begun, but we believe readers of this publication will be able to follow this debate in the future, regardless of what policymakers ultimately decide.

Josias N. Dewey

Holland & Knight LLP

ACKNOWLEDGMENT

The publishers would like to acknowledge the contribution of Joshua Klayman of Linklaters LLP who contributed the *Token Revolution, Token Evolution: Examining the Interplay between Digital Assets and Certain U.S. Federal Securities Laws* chapter to the online version of this book. This chapter is available to read online at: www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations.

Joshua Ashley Klayman

Tel: +1 917 565 0645 / Email: joshua.klayman@linklaters.com

Joshua Ashley Klayman is one of the best known Blockchain and Cryptocurrency lawyers in the world.

Recognised by *Chambers and Partners* as one of only three "Band 1"-ranked U.S. Blockchain & Cryptocurrency lawyers (and the only woman included in such list) for 2019, Josh also is one of the original top 12 global Blockchain & Cryptocurrency lawyers ranked by *Chambers* in its inaugural 2018 global list. Josh serves as U.S. Head of FinTech and Head of Blockchain and Digital Assets at Linklaters LLP and, by background, is a finance and corporate deal lawyer. In addition, she chairs the prominent Wall Street Blockchain Alliance ("WSBA") Legal Working Group and serves on the WSBA's Board of Directors. Josh is also a member of the global WhartonReg@Tech think tank, was appointed by the State of Delaware to serve on its Blockchain Strategy Committee and speaks frequently with regulators from around the world about Blockchain, Smart Contracts and Cryptocurrency matters. She is a Forbes Contributor for Blockchain and Digital Assets and works collaboratively with Blockchain leaders from other law firms, clients and the broader community to advance the industry, anticipate and address regulatory concerns and seize strategic opportunities.

In addition, Josh is a co-founder and director of the non-profit Diversity in Blockchain, Inc. and a founding member of Collective Future. Josh was named #89 on the list of 100 Most Influential People in Crypto for 2019, by *Modern Consensus*, and Innovate Finance has recognised her on its Women in FinTech PowerList, in the "Senior Leaders" category. Previously, Josh founded and served as CEO of both Inflection Point Blockchain Advisors, LLC, a blockchain strategy consulting and advisory firm, and Klayman LLC, a blockchain- and finance-focused boutique law firm. Passionate about the advancement of women and other diverse groups, Josh is the mother of five children and one grandchild, leading some in the industry to nickname her "Mother of Blockchains".

Linklaters LLP

1345 Avenue of the Americas, New York, NY 10105, USA
Tel: +1 212 903 9000 / Fax: +1 212 903 9100 / URL: www.linklaters.com

GLOSSARY

***Alice* decision**: a 2014 United States Supreme Court decision about patentable subject matter.

Cryptocurrencies: a term used interchangeably with virtual currency, and generally intended to include the following virtual currencies (and others similar to these):

- Bitcoin
- Bitcoin Cash
- Ether
- Ethereum Classic
- Litecoin
- Monero
- NEO
- Ripple's XRP
- DASH
- Dogecoin
- Zcash

Cold storage: refers to the storage of private keys on an un-networked device or on paper in a secure location.

Copyleft licence: the practice of offering people the right to freely distribute copies and modified versions of a work with the stipulation that the same rights be preserved in derivative works down the line.

Cryptography: the practice and study of techniques for secure communication in the presence of third parties, generally involving encryption and cyphers.

DAO Report: report issued in July, 2017 by U.S. Securities and Exchange Commission, considering and ultimately concluding that The DAO (*see below*) was a security.

Decentralised autonomous organisation ("The DAO"): a failed investor-directed venture capital fund with no conventional management structure or board of directors that was launched with a defect in its code that permitted someone to withdraw a substantial amount of the $130,000,000 in Ether it raised.

Decentralised autonomous organisation ("a DAO"): a form of business organisation relying on a smart contract *(see below*) in lieu of a conventional management structure or board of directors.

Digital assets: anything that exists in a binary format and comes with the right to use, and more typically consisting of a data structure intended to describe attributes and rights associated with some entitlement.

Digital collectibles: digital assets that are collected by hobbyists and others for entertainment, and which are often not fungible (e.g., CryptoKitties) (*see* **Tokens**, non-fungible).

Digital currency: a type of currency available only in digital form, which can be fiat currency or virtual currency that acts as a substitute for fiat currency.

Digital currency exchange: a business that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money, or one type of cryptocurrency for another type of cryptocurrency.

Digital/electronic wallet: an electronic device or software that allows an individual to securely store private keys and broadcast transactions across a peer-to-peer network, which can be hosted (e.g., Coinbase) or user managed (e.g., MyEtherWallet).

Distributed ledger technology (DLT): often used interchangeably with the term blockchain, but while all blockchains are a type of distributed ledger technology, not all distributed ledger technologies implement a blockchain style of achieving consensus.

Fintech: new technology and innovation that aims to compete with traditional financial methods in the delivery of financial services.

Initial coin offering: a type of crowdfunding using cryptocurrencies in which a quantity of the crowdfunded cryptocurrency is sold to either investors or consumers, or both, in the form of "tokens".

Initial token offering: See *Initial coin offering.*

Internet of Things: a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Licences, software: the grant of a right to use otherwise copyrighted code, including, among others:

- Apache
- GPLv3
- MIT

Mining, cryptocurrency: the process by which transactions are verified and added to the public ledger known as the blockchain, which is often the means through which new units of a virtual currency are created (e.g., Bitcoin).

Money transmitter (U.S.): a business entity that provides money transfer services or payment instruments.

Permissioned network: a blockchain in which the network owner(s) decides who can join the network and issue credentials necessary to access the network.

Platform or protocol coins: the native virtual currencies transferable on a blockchain network, which exist as a function of the protocol's code base.

Protocols: Specific code bases implementing a particular blockchain network, such as:

- Bitcoin
- R3's Corda
- Litecoin
- Ethereum
- Hyperledger Fabric

Private key: an alphanumeric cryptographic key that is generated in pairs with a corresponding public key. One can verify possession of a private key that corresponds to its public key counterpart without exposing it. It is not possible, however, to derive the private key from the public key.

Private key storage:

- *Deep cold storage*: a type of cold storage where not only bitcoins are stored offline, but also the system that holds the bitcoins is never online or connected to any kind of network.
- *Hardware wallet*: an electronic device capable of running software necessary to store private keys in a secure, encrypted state and structure transactions capable of being broadcast on one or more blockchain networks. Two popular examples are Ledger and Trezor.

Public network: blockchain which anyone can join by installing client software on a computer with an internet connection. Best known public networks are Bitcoin and Ethereum.

Qualified custodian: a regulated custodian who provides clients with segregated accounts and often places coins or tokens in cold storage (see above).

Robo-advice/digital advice: a class of financial adviser that provides financial advice or investment management online, with moderate to minimal human intervention.

Sandbox (regulatory): a programme implemented by a regulatory agency that permits innovative start-ups to engage in certain activities that might otherwise require licensing with one or more governmental agencies.

Security token: a token intended to confer rights typically associated with a security (e.g., stock or bond), and hence, generally treated as such by regulators.

Smart contract: a piece of code that is written for execution within a blockchain runtime environment. Such programs are often written to automate certain actions on the network, such as the transfer of virtual currency if certain conditions in the code are met.

Tokens: a data structure capable of being fungible (ERC-20) or non-fungible (ERC-721) that is capable of being controlled by a person to the exclusion of others, which is typically transferable from one person to another on a blockchain network.

Utility token: a token intended to entitle the holder to consume some good or service offered through a decentralised application (Dapp).

Vending machine (Bitcoin): an internet machine that allows a person to exchange bitcoins and cash. Some Bitcoin ATMs offer bi-directional functionality, enabling both the purchase of Bitcoin as well as the redemption of Bitcoin for cash.

Promoting innovation through education:
The blockchain industry, law enforcement and regulators work towards a common goal

Jason Weinstein & Alan Cohn
The Blockchain Alliance

Criminal use of technology

When many people think of "Bitcoin" or other cryptocurrencies, they often think of crime, because of "Silk Road" and other high-profile examples of people exploiting cryptocurrencies for unlawful purposes.

But for the entrepreneurs, engineers, venture capitalists and bankers who are pouring their time, energy, and money into cryptocurrency- and cryptoasset-related businesses, it is the underlying "blockchain" technology that is the real attraction. And contrary to popular belief, this technology is friendlier to law-enforcers than it is to law-breakers.

Blockchain technology uses cryptography to verify and confirm all transactions and then records those transactions on a searchable public ledger. Bitcoin and other cryptocurrencies represent just the first "app" for blockchain technology. There are endless other possibilities for that technology – from securities and commodities trading, to supply chain, to IP rights, to identity management and security, to real estate to government services, just to name a few – that could transform the way the world does business, much like the internet did over 20 years ago.

It's a fact of life in law enforcement that criminals are always among the first adopters of any novel technology that works. And law enforcement has a long history of adapting in order to pursue criminals who use "new school" technology to commit "old school" crimes. From beepers to email to online chat to Skype to social networking, law enforcement consistently has had to evolve as new technology designed for legitimate purposes is used to facilitate criminal activity. Bitcoin and other cryptocurrencies represent just the latest example.

While there is unquestionably criminal activity taking place via the internet, we don't think of the internet as the "computer network of criminals". That's because the vast majority of commercial activity over the internet is legitimate, whereas illicit activity facilitated by the web represents just a small portion of what happens on the internet every day. Similarly, Bitcoin and other cryptocurrencies should not be thought of as "currencies of criminals," because illicit transactions, while they exist, account for only a minute portion of the activity involving this new technology. Moreover, this technology has as much if not more potential to help root out money laundering and terrorism financing as it does to enable these types of activities.

Proactive engagement by industry

Recognising a shared interest in helping combat criminal exploitation of this revolutionary technology, the blockchain and cryptocurrency industry proactively approached law enforcement and regulatory agencies and offered to help educate these agencies about how cryptocurrencies work, provide technical assistance and an understanding of industry best practices, and foster an open dialogue about issues of common concern. Under the leadership of the Chamber of Digital Commerce and Coin Center, the industry established the Blockchain Alliance, a non-profit organisation that serves as a forum for engagement between the blockchain industry and law enforcement and regulatory agencies. Since its founding in 2015, the Blockchain Alliance has grown to include over 100 blockchain and cryptocurrency companies and law enforcement and regulatory agencies in the U.S. and around the world, including Europol and Interpol and authorities in Europe, Latin America, Africa, Asia, and Australia.

Through the Blockchain Alliance, some of the brightest minds in the industry are working with law enforcement and regulatory agencies to combat criminal activity involving this new technology, in an effort to promote public safety and a pro-innovation regulatory environment. The Blockchain Alliance convenes regular calls to discuss trends in the industry and tools for combating criminal activity. Among other activities, the Alliance has conducted educational programs for nearly 700 law enforcement officers and regulators from more than 35 countries. These educational programs cover a range of topics from the basics of the technology, to tracing tools, to privacy coins.

Tracing the flow of funds

One of the main misconceptions Blockchain Alliance members have worked to correct is that Bitcoin transactions are anonymous. The reality is that the technology has significant benefits for investigators seeking to "follow the (digital) money." Having a public, traceable, immutable, borderless ledger of every Bitcoin transaction ever conducted allows law enforcement to trace the flow of funds involving an investigative target anywhere in the world in a way that would not be possible with cash or many other types of financial instruments. And industry has developed software tools for connecting Bitcoin addresses to a particular user – similar to the challenge law enforcement has faced for years trying to identify anonymous hackers and other cybercriminals – and those tools are continually improving, as well as expanding for use with respect to other cryptocurrencies. Those same types of tools allow cryptocurrency exchanges and others to better identify suspicious actors and transactions as part of their anti-money laundering compliance programs. Under the circumstances, criminals should be running, not walking, away from using Bitcoin and other types of cryptocurrencies.

Impact of regulation

While it is often said that cryptocurrencies and blockchain technology are unregulated, nothing could be further from the truth. Numerous federal and state agencies in the United States, as well as agencies in other countries, regulate applications for this technology in some fashion. But the disparate approaches taken by different countries, or even by different agencies within the U.S., have led to confusion on the part of blockchain companies about the jurisdictions and regulatory regimes to which their products and services will be subject.

An analysis of illicit laundering of Bitcoin found regional differences in volume, part of which may be explained by the different approaches to regulation. CipherTrace, a blockchain forensics and cryptocurrency analytics provider and Blockchain Alliance member, conducted a quantitative analysis of all transactions on the 20 top cryptocurrency exchanges globally, and found that "97% of direct bitcoin payments from identifiable criminal sources were received by unregulated cryptocurrency exchanges" (cryptocurrency exchanges not subject to AML regulation), and that "36 times more criminal bitcoin was received by cryptocurrency exchanges in countries where AML is either lax or lacking." Indeed, the results indicate that "money laundering activity using cryptocurrencies is directly correlated to AML regulations and their enforcement on exchanges."[1]

Many jurisdictions, even within the U.S., regulate cryptocurrency activities like the exchange of cryptocurrency to fiat, or cryptocurrency to cryptocurrency, differently. Europe has now adopted regulation to include cryptocurrency companies like exchanges within the scope of the 5th Anti-Money Laundering Directive. Some exchanges offering services that do not clearly fit in the current regulatory regime have voluntarily developed robust procedures in order to verify their customers' identity and the source of funds. However, clear regulations and guidelines on AML and know-your-customer policies can help reduce the criminal activity flowing through exchanges and other cryptocurrency companies.

Moving forward through continued engagement

In order to ensure the growth of the industry while also protecting consumers and preventing money laundering, a pro-innovation approach to regulation is needed. Positive and proactive engagement by industry with law enforcement and regulators, through the Blockchain Alliance and otherwise, has been critical to the growth of this sector to date. Continued engagement of this type will be equally important going forward, as industry seeks to foster an approach to law-making and rule-making that encourages, rather than stifles, innovation. Only then can the full potential of blockchain technology be realised.

* * *

Endnote

1. CipherTrace, Cryptocurrency Anti-Money Laundering Report, Q3 2018, https://ciphertrace.com/crypto-aml-report-2018q3.pdf.

Jason Weinstein, Director
Tel: +1 202 429 8061 / Email: jweinstein@steptoe.com

Jason Weinstein is Partner at Steptoe & Johnson LLP, co-chair of the firm's Blockchain and Cryptocurrency practice, and Director to the Blockchain Alliance. He has represented just about every type of participant in the blockchain ecosystem and is widely recognised as an authority on legal and regulatory issues involving digital currencies and blockchain technology. Jason previously served as deputy assistant attorney general in the Department of Justice's Criminal Division, where he supervised the computer crime and organised crime sections, and oversaw numerous investigations involving the use of digital currencies. Jason serves on the advisory boards of Coin Center and the Chamber of Digital Commerce. He also serves as an advisor to BitFury, the leading full-service blockchain technology company and one of the largest private infrastructure providers in the industry.

Alan Cohn, Counsel
Tel: +1 202 429 6283 / Email: acohn@steptoe.com

Alan Cohn is Partner at Steptoe & Johnson LLP, co-chair of the firm's Blockchain and Cryptocurrency practice, and counsel to the Blockchain Alliance. Alan counsels companies on cybersecurity, blockchain and distributed ledger technology, and national security issues. Alan is ranked among the top US lawyers in Blockchain and Cryptocurrencies by *Chambers USA* (2019), where he is noted for his "tremendous depth of expertise in regulatory issues facing blockchain platforms and cryptocurrencies." He previously served in senior policy and management positions at the U.S. Department of Homeland Security for almost a decade, most recently as the Assistant Secretary for Strategy, Planning, Analysis & Risk and second-in-charge overall of the DHS Office of Policy. Alan also serves as an advisor to several blockchain companies.

The Blockchain Alliance

1330 Connecticut Avenue, NW, Washington, DC 20036, USA
URL: www.blockchainalliance.org

The loan market, blockchain, and smart contracts: The potential for transformative change

Bridget Marsh, LSTA
Josias N. Dewey, Holland & Knight LLP

Introduction

The Loan Syndications and Trading Association ("LSTA") is the trade association in the United States for the corporate loan market. We promote a fair, orderly, and efficient loan market and actively seek ways in which we can achieve that. During the past couple of years, the LSTA has considered how blockchain (or distributed ledger technology ("DLT")) and related advanced technologies will impact the industry and believes that this new technology can propel the syndicated loan market forward and help address some of its current challenges.

This article provides a brief description of the loan market and its participants to put our conversation in context, sets out the basics of blockchain technology, reviews the concept of "smart contracts", and examines how the primary and secondary loan markets can benefit from these new technologies.

U.S. loan market and loan market participants

There is no single regulatory authority charged with the responsibility of regulating the syndicated loan market in the United States. Of course, most loan market participants are regulated institutions that have one or more regulators overseeing their activities, but the loan market itself is not regulated. The LSTA is, therefore, the entity to which loan market participants turn for standard forms, best practices, and general assistance with primary loan market activities and secondary market loan trades.

The LSTA maintains a suite of documents that can be used by market participants in the origination, servicing, and trading of loans. Since its formation nearly 25 years ago, the LSTA has published standard agreements, forms, and best practices for use in the primary loan market which have been widely adopted by market participants. The LSTA's comprehensive suite of secondary trading documents are used by all loan market participants to evidence their loan trades and then settle those transactions.

At its most basic, in the primary loan market, there are several interested parties involved in the origination of any large syndicated loan, the terms of which are documented in a credit agreement. There must be: (i) a borrower to which the loan is made and which is responsible for principal and interest payments under the terms of the credit agreement; (ii) one or more lenders in the syndicate, each of which owns a portion of the outstanding loan; and (iii) an administrative agent which is responsible for the ongoing administration of the loan until

its maturity date. Although complex deal terms may vary from deal to deal, the basics of each loan will generally operate the same way. In the secondary loan market, each loan trade will, of course, include a selling lender and a legal entity buying the loan, an administrative agent who must acknowledge or consent to the loan assignment, and a borrower whose consent to the loan trade is also typically required. The buyer and seller of the loan execute an LSTA Par/Near Par Trade Confirmation ("LSTA Confirm") to evidence their loan trade, and the relevant form of assignment agreement pursuant to which the loan is then assigned to the buyer. Finally, the administrative agent updates the register of lenders to reflect the loan assignment.

For the trading of performing loans ("par trades") where the borrower is making timely loan payments in accordance with the terms of the credit agreement and neither the borrower nor the applicable industry is in any type of financial distress or experiencing any type of turmoil, most of the steps outlined above have become standard practice in the U.S. loan market, and LSTA trading documentation is used uniformly by all participants. After the relevant consents are obtained, those par trades are typically settled on an electronic platform with little or no lawyer involvement and few, if any, modifications. Instead, market participants expect the LSTA to provide the market with trading documents that are periodically updated to reflect current market practices, legal developments, and the latest deal trends.

Because there is no (or very limited) tailoring of documents in the trading of par loans and with practices being quite streamlined and uniform, distinct elements of this market seem ideally suited for the implementation of blockchain technology.

Blockchain basics

The terms blockchain and DLT are often used interchangeably by those in financial services, and both terms seem to be used as acceptable nomenclature for this technology. Although there is a technical distinction between a blockchain and a DLT, for the purposes of our discussion, the terms will be used interchangeably, although it seems that the term blockchain is the preferred term by those in financial services.

Perhaps surprising to some is that the technology underlying blockchain is actually a collection of technologies none of which is new. Blockchain is a decentralised peer-to-peer network that maintains a ledger of transactions (e.g., a transfer of an asset from one party to another party) that uses cryptographic tools to maintain the integrity of transactions and the integrity of the ledger itself, and a protocol-wide consensus mechanism that verifies the data and determines if, when, and how to update the ledger. The decentralised network makes this technology distinct from a traditional centralised database that has one authoritative database maintained by a trusted third party. For example, central banks around the world serve as that trusted third party for a state's banking system; similarly, for a syndicated loan, the administrative agent is the trusted third party that maintains the register of lenders, administers the loan, and keeps a record of all loan positions, including related interest and principal payments. Lenders in the syndicate must reconcile their own records with those of the administrative agent whose entries in the register are conclusive, absent manifest error. Without a trusted party to maintain a ledger, by contrast, in a blockchain, the cryptographic tools (e.g., a public or private encryption key) keep the information secure, for they are used to control the ownership of and/or the right to access the information on the ledger.

A blockchain is often considered to be immutable or tamper-proof because of the technology used to maintain the integrity of the ledger. Although there have been a few examples of hacking of digital currencies that rely on this technology, the unique way in which the

information is stored and updated does make it incredibly secure so it is most definitely tamper-resistant. For example, to create each "block" in a blockchain, transactions are aggregated together and, using the appropriate protocol (a protocol can be thought of as software or a set of rules for a particular system), subjected to a special mathematical algorithm. The calculation results in an alphanumeric string that is put on the next block, and those two blocks are now inextricably chained together or "cryptographically linked". The process is then repeated for each bundle of transactions that are aggregated together; the number of blocks will increase, and the chain will continue to grow over time. To tamper or attempt to hack into or change some of the stored information would be nearly impossible and incredibly expensive. Because a new entry on a blockchain ledger is verified by a consensus mechanism at the time of entry and updated across all computers simultaneously, the computers rely on and trust this single source of truth. One of the enormous benefits of this technology is the potential for cost savings because separate reconciliation efforts will no longer be needed. (This alone makes it incredibly attractive technology for the loan market.)

Public or permissioned ledger

Distributed ledger technology can be implemented with or without access controls, depending on whether an open, public network is used or a restricted, permissioned network is chosen. The decentralised digital currency, Bitcoin, is likely the most well-known example of an open, public network where anyone can query the ledger and broadcast transactions without any authorisation (assuming, of course, the individual has the proper computer equipment and software). In a public blockchain, ledgers are replicated across many computers referred to as "nodes", which are connected to a common network over the internet. Those operating the nodes are referred to as "miners". In contrast, a closed, permissioned network is restricted to certain individuals who have been given permission and the necessary credentials to access the ledger by a trusted third party.

It is not surprising that the financial services industry is currently favouring the implementation of permissioned networks. Because of anti-money laundering ("AML"), know-your-customer ("KYC"), and privacy considerations (discussed more fully below), public networks are not really feasible in financial services at this time. A Bitcoin miner that is anonymous on a public network should be subject to the requirements of the Bank Secrecy Act and a financial institution's own KYC program as if it were to be involved in a similar function in the financial services industry for a bank. Thus, it is understandable that given current frameworks, a bank's systems cannot be integrated with public networks, but as technology develops this, too, could change.

Each member of a permissioned network knows the identity of the counterparty on the other side of a transaction. Being able to identify a counterparty is important for many reasons in a transaction, including KYC and AML. For financial transactions, in particular, it provides parties with a way to make formal demands against each other in the event of nonperformance by one of them. Similarly, if the nonperforming party fails to cure a default, the other party may file a lawsuit and exercise its rights and remedies under the transaction documents. By contrast, on public networks, people are often transacting anonymously or with those who have not disclosed their true identity.

Smart contracts

The term "smart contracts" can be misleading, especially for lawyers who have a definite

idea of what must be shown for there to be a binding legal agreement between parties. At a minimum, a contract requires there to be an offer by one party, an acceptance by another party, and some form of consideration to exist. When the term is used by software engineers, it means computer code that is self-executing (the type of code will depend on the protocol on which the code is implemented). I think a more useful structure for the loan market is a hybrid legal contract that has certain parts of it coded and other parts that remain in human prose. The term "smart legal agreements" has been used to describe this type of hybrid legal contract, and this combination of a legal agreement with a smart contract would be most useful for financial instruments. One could envision how the LSTA's standard forms and agreements could become smart legal agreements with certain provisions remaining in human prose; for example, the reference to LSTA Arbitration Rules in the LSTA Confirm could remain as text while provisions relating to the calculation of the loan purchase price for the applicable trade could be coded and thus become self-executing.

There is an aspect of utilising smart legal agreements which does increase the risk of error or corruption and should, therefore, be highlighted – the management of information that is drawn from an external source referred to as an "oracle" in the blockchain nomenclature. Because smart contracts are programmed to be self-executing, some information may need to be pulled in from an external source, and therefore it is essential that this information from the oracle be accurate. For example, pursuant to the terms of the LSTA Confirm, if a trade does not timely settle, then upon settlement the buyer is credited for certain interest payments made by the borrower, but it must also pay the seller the interest that would accrue at one month LIBOR for deposits in the applicable currency as set by the ICE Benchmark Administration on the amount equal to the purchase price. If the LIBO Rate, an oracle, is corrupted for any reason, then of course there will be repercussions for trades settling on the blockchain, where the Confirm has been turned into a smart legal agreement with certain elements of it coded and thus self-executing.

Smart contracts build on the innovation of blockchain technology and have the potential to allow parties to structure and effectuate transactions in a more efficient and secure manner than traditional contracts; however, there are still challenges and obstacles that must be overcome before smart legal agreements become commonplace. Although we recognise that the technology remains in its infancy and is not a panacea for all our market's present challenges, we remain confident that smart contracts and blockchain technology will ultimately transform our market.

Blockchain, smart contracts and the loan market

There is enormous potential for the marriage of blockchain technology and smart contracts to result in incredible strides forward for the loan market. Although the typical syndicated loan agreement is a complex instrument that cannot be reduced simply to computer code, there are aspects of it which do lend themselves to becoming coded and, where a legal agreement has been standardised for a particular market or asset, then it can be more easily coded and efficiently implemented.

In the context of the loan market, the origination of a syndicated loan – from the time the credit agreement is drafted and the loan funded – could be made using blockchain technology (as has already been done with syndicated loans in Europe). In today's market, a credit agreement is typically drafted by legal counsel based on deal terms that have been emailed to them. The lawyers then prepare the draft credit documentation based on that information. This approach introduces the risk of manual transcription errors, and validation rules will

not have been applied to the information included in the credit agreement. By using document-automation tools, together with a distributed ledger, the credit agreement can be generated from data stored on the ledger that has already been validated. Although this can, of course, be accomplished without a blockchain; in the absence of one there is no single source of validated data. Having a single source of truth as to the ownership of a syndicated loan ultimately will eliminate the redundant, time-consuming, and costly exercise of multiple parties manually processing and accounting for primary allocations, payments and assignments.

In today's loan market, the closing of primary trades is a time-consuming and slow process. After initial funding of the loan by the administrative agent, each party with a primary market allocation must then fund its portion of the loan and execute an assignment agreement to evidence the settlement of their primary trade. With the disparate systems used by loan market participants today, each party is likely still emailed a PDF or another form of the executed agreement, and from those documents it must then extract the relevant information and manually input that information into its own back office system (with all the human touchpoints, there is a greater risk of error and delay with this type of process).

With a blockchain, the credit agreement and related documents could be digitally signed and delivered electronically at closing, thus allowing the deal terms, including information about loan positions, automatically to populate on the network's ledger – the same ledger accessed by all lenders. Think how a DLT network with the applicable credit agreement, assignment agreement and Confirm, all structured as smart legal agreements, could implement identical functionality in a way similar to today's loan operations – but one where the contracts are self-executing and the database replicated across an entire network of computers. Although the computers in the network (assuming a permissioned network is used) will be controlled by potentially hundreds of lenders in the syndicate, the integrity of the data across the network will be assured by the integration of a protocol-wide consensus mechanism.

A blockchain platform for a syndicated loan could also track a loan's interest rate, interest and principal payment dates, and any other data fields relevant to the life cycle of the loan. In a typical syndicated loan, many different parties, each storing information about a syndicated loan, have to continually reconcile all information they receive against their own internal databases. A blockchain platform could eliminate the need for, or significantly reduce the time spent on, reconciling data across the market. That alone could save the loan market an enormous amount of time and money. In addition, other aspects of a credit agreement could also be coded. For example, when a borrower submits periodic financial reports to the syndicate, certain data from those reports could be extracted, thus allowing financial covenants in the credit agreement automatically to be tested.

Secondary market trades in the loan market are memorialised by the parties executing an LSTA Confirm. Settlement of the trade – when the seller's legal ownership of the loan is transferred to the purchaser, and the purchaser pays the purchase price to the seller – typically occurs days or even weeks after the trade is entered into by the parties. It is easy to imagine how the transfer of this asset could be done far more seamlessly and efficiently on a blockchain, with smart legal agreements self-executing and data being updated on the ledger automatically. In this way, one can imagine lenders in the syndicate on a permissioned ledger using private keys digitally to execute the LSTA Confirm and applicable assignment agreements. When the assigning lender digitally signs the Confirm and relevant assignment agreement (and any other consents have been obtained), the register of lenders (assuming existing nomenclature is retained) will be updated automatically to reflect the assignee's

account being credited by the amount of the loan transferred to it, and a corresponding debit to the assignor's account. No-one will need to reconcile their own positions because they will all have access on the permissioned ledger to the same information.

Although the adoption of blockchain will shorten the settlement times for loan trades, the payment of the loan purchase price will likely occur outside of blockchain networks for some period of time. Although it is not currently possible to transfer U.S. dollars across a distributed ledger, in the future, a central bank-issued digital currency could make settlement on the blockchain seamless. Until then, the payment method of a loan trade purchase price will need to rely on processes external to any blockchain to initiate payment. Reliance on such external processes may be acceptable on a permissioned blockchain network, where the identity of parties are known to each other and regulated financial institutions are involved.

The LSTA recently completed the automation of the LSTA Form of Revolving Credit Facility. Working with OpenLaw, a blockchain-based protocol for the creation and execution of legal agreements, we used Solidity, the language native to the Ethereum platform, to code aspects of the credit agreement and create a smart legal agreement. The entire credit agreement was not turned into a smart contract; provisions relating to the mechanical aspects of the credit agreement were coded, including those relating to borrowing requests, interest and principal payments, and loan transfers. The creation of this prototype demonstrated that: (i) the drafting of syndicated credit agreements can be partly automated using legal technology tools with evidence of the parties' agreement and associated electronic signatures stored on a blockchain; (ii) smart contracts can be used to automate certain aspects of loan administration, particularly responsibilities performed by the agent; (iii) blockchain technology and smart contracts can be used to hard code regulatory compliance, in the form of approved addresses that can help ensure compliance with KYC/AML requirements (see further discussion below); (iv) blockchain technology and smart contracts can be used to hard code disqualified lender lists to help streamline the borrower consent process; and (v) blockchain technology can be used to digitally represent a lender's interest in a syndicated loan, creating opportunities to shorten settlement times for syndicated loan trades. The agreement could still be accessed, viewed, and scrolled through. Importantly, the automated contract still looked like the LSTA's credit agreement from cover page to signature page. Unfortunately, at this time, there remain many practical limitations relating to the implementation of this new technology and smart contracts in the loan market. Because smart contracts can only interact with tokenized assets, unless digital assets quickly gain widespread usage in our industry, blockchain-based applications and services will take time to adopt. Nevertheless, we were greatly encouraged by the results of the creation of this prototype and now plan to embark on the next phase and work on developing a means for our members to receive and work with such a digitised loan position.

AML and KYC issues

An appropriately built blockchain solution for the loan market would meet both KYC and AML requirements, and in so doing, would likely improve both the speed of implementation and accuracy of a financial institution's compliance program while satisfying any legal and regulatory requirements. The LSTA's 2017 Guidelines for the Application of Customer Identification Programs, Foreign Correspondent Account Due Diligence, and Other Considerations ("LSTA CIP Guidelines") serve as a comprehensive report outlining the specific due diligence and other compliance work required to engage in primary and

secondary loan market transactions in the United States. The LSTA CIP Guidelines, which accurately set forth what is required for different primary and secondary loan market transactions and relationships between loan market participants, can be embedded in the smart legal agreement implementing the framework.

Because the KYC and AML requirements would be incorporated in this way, there would no longer be any need to have a separate stream of compliance work to satisfy a bank's KYC requirements and AML diligence in any syndicated loan that is processed through the framework. For example, perhaps checking the sanctions lists on the U.S. Department of the Treasury's Office of Foreign Assets Control website to ensure that a counterparty is not on any of the lists, which is typically the only due diligence required under U.S. law, could be like an "oracle", with the diligence thereby completed seamlessly and without any delays. This would result in huge cost savings for our market and would likely also lead to much shorter loan-trade-settlement times.

Regulators could also benefit greatly from the adoption of blockchain in the loan market. Because blockchains contain a complete history of all transactions that have taken place on the network, including a time stamp for all such transactions, internal auditing would be much simpler, and regulators could be granted access to the ledger to confirm that all related transactions are consistent with the stated intentions and information provided by customers. The ability to see transactions in real time would also be beneficial to regulators, who could monitor the transactions and more easily detect and identify illicit activities.

Competition law issues and corporate governance matters

There are, of course, competition law considerations that must be taken into account when considering the implementation of this new technology, and as a trade association we are acutely aware of these. During the process of selecting the appropriate DLT, there will be collaborative efforts necessary to implement the chosen DLT to the particular use case within the loan market. This collaboration and the development of a technological solution raise intellectual property concerns that the parties should seek to address. Although the task of identifying the correct technology may be challenging, once common ground is reached by market participants on that issue, the focus should then turn to internal governance matters, and the relative rights and obligations of the participants.

These efforts are complicated by the ever-present need to ensure compliance with applicable antitrust law, an issue that requires continuing diligence and vigilance amongst industry participants. We would caution consortium participants about anti-trust issues which may arise in such circumstances, and to seek advice from counsel where appropriate. The exchange of specific data on current and future prices and competitive activities – as opposed to aggregated past information – is likely to attract the greatest antitrust scrutiny. Thus, participants in blockchain consortia should take care to ensure that they are not, or could not be perceived to be, agreeing to eliminate their independent decision-making as to any aspect of the prices they charge or markets they serve.

Conclusion

The LSTA is optimistic about the potential for blockchain, or any type of advanced technology, to have a positive effect on the US loan market. At its simplest, blockchain is an efficient way to transfer any asset, including a loan, and the current systems and practices of the US syndicated loan market could benefit enormously from this technology. The LSTA is well-placed to lead the legal, technological, operational and business efforts to develop a

general framework for implementing solutions that address the lifecycle of a loan from origination to repayment. Our market participants should understand not only the potential benefits of blockchain but the challenges to its adoption. This suggests that a sustained educational initiative targeting all loan market participants is necessary, and the LSTA is committed to offering that. The LSTA has been following developments around blockchain and providing educational resources to its members for a few years and will continue to be a resource as its members navigate many of these challenges and, in some cases, take a leading role in helping to craft standards that facilitate the efficient deployment of the technology. Forging consensus within an entire industry about standards, best practices and other uniform approaches and protocols is challenging, as we know, but the LSTA is well-placed to lead these efforts.

Although blockchain technology will not eliminate all inefficiencies in the loan market, it seems very likely that blockchain technology will eventually bring about fundamental change in how syndicated loans are originated, administered and traded in today's loan market. Yet, there is much work to be done before this can be achieved. Computer software engineers, finance professionals, lawyers, and operational personnel will need to work together to analyse all of the processes used in the loan market, loan administration, and secondary loan trading. Policy, legal, and regulatory issues will need to be addressed thoughtfully, and we must always balance our desire to promote innovation with the need for a strong, stable, and reliable loan market.

Bridget Marsh
Tel: +1 212 880 3004 / Email: bmarsh@lsta.org

Bridget Marsh is Executive Vice President and Deputy General Counsel of the Loan Syndications and Trading Association (LSTA). Bridget heads the LSTA's Primary Market Committee and Trade Practices and Forms Committee and leads the legal projects for the development and standardisation of the LSTA's documentation.

Prior to joining the LSTA, Bridget practised as a corporate finance attorney at Milbank, New York, and as a lawyer in the corporate/M&A department of Simmons & Simmons, London, and completed a judicial clerkship for The Honorable Justice Beaumont of the Federal Court of Australia. She is a Regent of the American College of Commercial Finance Lawyers and a Fellow of the American Bar Foundation.

Bridget Marsh received a B.A. *magna cum laude* from Georgetown University, a law degree with first class honors from Sydney Law School, University of Sydney, and a Masters in Political Science from the University of New South Wales. She is admitted as an attorney in New York, England & Wales, and New South Wales, Australia.

Josias N. Dewey
Tel: +1 305 374 8500 / Email: joe.dewey@hklaw.com

Joe Dewey is a financial services and real estate partner in Holland & Knight's Miami office and is considered a thought leader on blockchain technology. Mr Dewey regularly represents banks and other financial institutions across the entire spectrum as measured by assets and scale, from community to global money center banks. Mr Dewey spends a considerable amount of time at the convergence of human prose legal contracts, as well as computational contracts, based primarily on computer code. This includes smart contracts that can be implemented on Hyperledger Fabric (or IBM's Blockchain service), Ethereum (both public and permissioned versions) and R3's Corda platform. Mr Dewey spends a considerable amount of his practice in this space assisting clients in identifying optimal distributed ledger use cases and developing proof of concept applications. He can assist in the transition from proof of concepts (PoCs) to production systems built by our clients' primary technology solutions providers.

Loan Syndications and Trading Associaton (LSTA)

366 Madison Avenue, 15th Floor, New York, NY 10017, USA
Tel: +1 212 8803000 / Fax: +1 212 880 3040 / URL: www.lsta.org

A year of progress – the Wall Street Blockchain Alliance and the ongoing evolution of blockchain and cryptoassets

Ron Quaranta
Wall Street Blockchain Alliance

In the year since the inaugural publication of "**Global Legal Insights – Blockchain & Cryptocurrency Regulation**", the progression and pace of innovation has, if anything, accelerated. Indeed, since that time one would struggle to enter into a business discussion that in some form did not mention artificial intelligence, machine learning, virtual or augmented reality and much more. Of course, none of these has been more prevalent than blockchain and cryptoassets.

Readers of this latest edition are by now probably familiar with the proposed benefits of blockchain technology; benefits such as decentralization, immutability and transparency, to say nothing of the as-yet-not-fully-realized cost savings possible because of these characteristics. As we noted last year, it is *still* the hope of blockchain and cryptoasset advocates that this innovation will fundamentally reinvent the economic models upon which much of the global economy is built.

Blockchain technology and cryptoasset evolution has of course been a rough and uneven progression. While a significant number of companies, industries, entrepreneurs and governments across the globe have progressed their knowledge and understanding regarding the technology, the pace of actual usage has been below the expectations of many. To be certain, some real use cases have come to light. Using blockchain for supply chain management, best exemplified by the IBM-Maersk Tradelens[1] platform, which leverages blockchain for international trade and includes some of the largest shipping companies in the world, has been a good example.[2] Likewise, the usage of blockchain to track provenance of produce has seen some uptake, notably the Walmart program that requires lettuce and spinach purveyors to contribute to a blockchain database that can rapidly pinpoint contamination.[3] Everything from drug prescription tracing to produce tracking to inventory management are beginning to leverage blockchain technology. This has clearly been helped by the explosion of technology providers large and small all offering blockchain-based platforms to their enterprise customers.

In addition to IBM, the past year has seen major inroads by the likes of Amazon Web Services, Hewlett-Packard, Microsoft, Oracle, SAP and more, who have seized the opportunity to produce blockchain offerings across multiple industries. Learning from past Software-as-a-Service models, these firms have developed *Blockchain-as-a-Service*

platforms. These full-service cloud-based solutions enable programmers, entrepreneurs, and enterprises to develop, test, and deploy blockchain applications and smart contracts that will be hosted on their BaaS platform, and offer a level of comfort to enterprises that may not have existed before. This is not to say that small, nimble contenders have not been able to succeed, and one would be well served to track the coming progress of firms like Symbiont, BlockApps, SafeChain, Filament and more too numerous to list here, which offer the promise of many more blockchain implementations across more industries in the coming years.

No less important has been the advancement of cryptoassets across the globe. What started over a decade ago with the launch of Bitcoin as a way of sending value to others in a secure, peer-to-peer way that requires no intermediary,[4] the cryptoasset ecosystem has had its own Cambrian Explosion with, at the date of this writing, over 2,300 different cryptoassets across the world, with a market capitalization exceeding US$ 319 billion.[5] And this only scratches the surface. Around the world we have seen the emergence of a variety of cryptoassets based on the idea that even real-world assets, such as real estate, art, collectibles and more, can leverage blockchain technology and cryptography to facilitate more liquid, accurate and secure markets. Coupled with the reality of a growing number of financial markets participants in New York, London, Singapore and beyond, all looking to trade cryptoasset-based derivatives, options, futures, ETFs and more, one cannot help but face the realization that financial markets are changing. That we are perhaps truly witnessing the emergence of a brand-new class of assets and derivatives, which proponents claim will unlock trillions of dollars in economic value.

It is in the backdrop of these developments that the *Wall Street Blockchain Alliance* (WSBA) continues to be an integral part of market advances towards a blockchain and cryptoasset future. Since our founding over four years ago, the WSBA continues to grow its member base from an ever-widening pool of professionals and industries. In addition to traders, investors, bankers and financial technology executives, our global membership now encompasses hundreds of attorneys, accountants, digital media executives and more. All of them are determined to have a seat at the table as blockchain technology and cryptoassets continue to seep into their relevant industries. With membership representing almost 300 companies and organizations worldwide, the WSBA continues to be an industry-leading non-profit trade association with a global mission to advocate, guide and promote comprehensive adoption of blockchain technology and cryptoassets across global markets. And our members make all of it possible.

Our mission progresses across many fronts, preeminent of them being our collection of Working Groups (WGs), the machinery by which our members can directly interact with the WSBA itself, with other WSBA members and with industry participants. In addition to our Cryptoassets, Legal, Technology, and Enterprise Working Groups, we also proudly launched a Real Estate Working Group in 2019, tasked with helping the evolution of blockchain and cryptoasset usage for a global, multi-trillion-dollar real estate industry. Coupled with our global partnerships alongside other non-profit trade associations such as the Association of International Certified Professional Accountants (AICPA) and its technology arm, CPA.com, as well as the Blockchain in Transport Alliance (BiTA), the WSBA is well positioned to work with and alongside our members to define and develop the adoption of blockchain technology across the global economic landscape. These partnerships continue to highlight our philosophy of cooperation and engagement that is core to the WSBA, and we believe critical to our organization's success.

What, one might ask, does this have to do with a second edition of a book designed to glean the wisdom of worldwide experts about the current state of blockchain and cryptoasset

regulation? It is an interesting question and one that we believe fits well into the milieu of the WSBA ecosystem. One of our largest Working Groups is our Legal WG, now encompassing more than 100 attorneys representing greater than 55 practices and firms from around world. The mission and goal of this group is to not only keep up with the ever-shifting and growing landscape of regulations and laws popping up worldwide about blockchain and cryptoassets. In addition, it is our goal that this group also educate and guide those selfsame regulators and legislators in the paths that we hope most fully advance innovation while maintaining important tenets such as investor protection and orderly markets. Our Legal WG represents some of the greatest legal minds in the areas of blockchain and cryptoassets, and it is not by accident (in our humble opinion) that many of our members are past and present contributors to this book.

Law and regulation are part of the genetic composition of modern global markets. Given the breakneck speed of innovation, and the potential disruptive nature of blockchain technology and cryptoassets, a guide like this becomes ever more important. The Wall Street Blockchain Alliance is proud once again to be a contributor to this publication. More importantly we are proud of our many members who have done likewise.

* * *

Endnotes

1. https://www.tradelens.com.
2. https://www.coindesk.com/ibm-maersk-shipping-blockchain-gains-steam-with-15-carriers-now-on-board.
3. https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html.
4. https://bitcoin.org/bitcoin.pdf.
5. https://coinmarketcap.com.

* * *

Information about the Wall Street Blockchain Alliance can be found at www.wsba.co, or by email to info@wsba.co.

Ron Quaranta
Tel: +1 908 415 9027 / Email: ron@wsba.co

Ron possesses almost three decades of experience in the global financial services and technology industries. He currently serves as Chairman and Chief Executive Officer of the Wall Street Blockchain Alliance, the world's leading non-profit trade association promoting the comprehensive adoption of blockchain technology and cryptoassets across global financial markets. Prior to this, Ron served as CEO of DerivaTrust Technologies, a pioneering software and technology firm for financial market participants. Ron is the editor and contributing author of the book "*Blockchain in Financial Markets and Beyond: Challenges and Applications*", published by Risk Books, as well as a contributor to "*Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019*", published by Global Legal Group. In addition, he was recently named in the Top 100 Most Influential People in Accounting by Accounting Today in 2018. He is a frequent guest of major media outlets, including Bloomberg Radio, and is a sought-after speaker and writer regarding financial technology and innovation. Ron also serves as an advisor to multiple startups and corporations focused on fintech innovation and blockchain technology.

Wall Street Blockchain Alliance

Tel: +1 908 415 9027
URL: www.wsba.co

Blockchain and intellectual property: A case study

Joshua Krumholz, Ieuan G. Mahony & Brian J. Colandreo
Holland & Knight LLP

Introduction

As discussed elsewhere in this book, blockchain has the potential for transformational change. Like most transformational technologies, its development and adoption is laden with intellectual property ("IP") issues, concerns and strategies. Further, given the potentially wide-ranging impact of blockchain technology, the public and private nature of its application, and the prevalent use of open source software, blockchain raises particularly unique IP issues.

The purpose of this chapter is to help the practitioner identify some of the issues that may affect blockchain development and adoption. We address these issues as they may relate to a company's creation of its own IP, and as they may relate to efforts by others to assert their IP against a company. We discuss the issues in the context of the hypothetical scenario discussed below.

The hypothetical transaction

Although many sectors stand to benefit from the use of blockchain technology, the financial and supply chain management sectors may be among the first to benefit. For purposes of discussion, this chapter focuses on the financial sector, and in particular the following hypothetical:

> A U.S. company is building a new platform using distributed ledger technology for its syndicated loan transactions. Many participants are involved in a typical transaction serviced by the platform, including borrowers, lenders, an administrative agent, credit enhancers and holders of subordinated debt. The platform that the company is building employs smart contracts to effectuate the functionality over a permissioned (private) network with several hundred nodes in the network.

Our hypothetical company, as noted, has chosen to deploy its solution via a permissioned network. A blockchain developer has two broad options in this regard. First, the developer could select a public blockchain network for its platform. In a public network, each node contains all transactions, the nodes are anonymous, and participants are unknown to each other. Second, the developer could select a permissioned network (as our hypothetical company has). In a permissioned network, the network owner vets network members, accepts only those that it trusts, and uses an access control layer to prevent others from accessing the network. Unlike the nodes on a public network, the nodes on a permissioned network are not anonymous. In addition, a permissioned network can be structured so that specified transactions and data reside only on identified nodes, and are not stored on all nodes in the network.[1] In certain commercial transactions, participants must be known to each other in

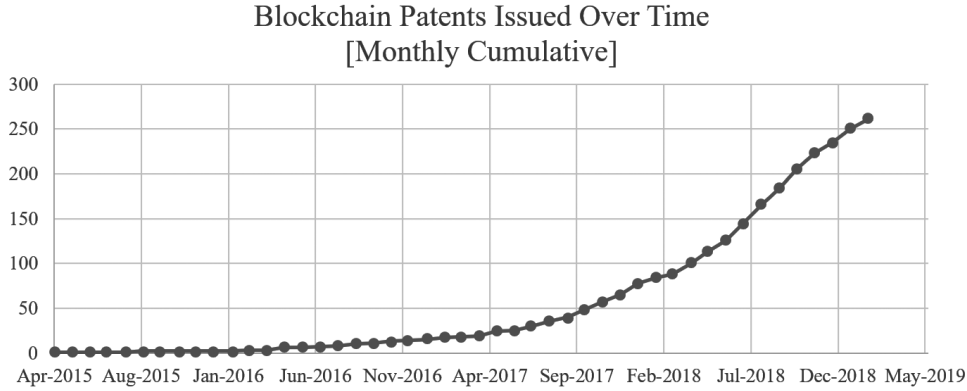
order to meet regulatory requirements, such as those designed to prevent money laundering. In these situations, a network of anonymous nodes would not be compliant.

Our hypothetical company has selected a permissioned network, we can assume, to obtain these benefits. This selection comes with costs, however, and the company will lose the benefit, for example, of validating a transaction over the full multitude of distributed nodes in a public blockchain network, and the assurances of immutability that that provides.

The blockchain patent landscape

Since Satoshi Nakamoto published the Bitcoin whitepaper in 2008,[2,3] the number of blockchain patent applications has steadily risen. In 2016, applicants filed 521 patents related to blockchain technologies in the U.S.[4] and 895 worldwide.[5] In 2017, the number of U.S. filings rose to 602[6] and 1,631 worldwide.[7] In 2018, 4,673 patent applications relating to blockchain were filed worldwide.[8] Notably, Chinese entities filed the greatest number of U.S. blockchain patent applications in 2017, accounting for 56% of all filed applications.[9] Applications for blockchain patents filed by U.S. entities accounted for 22% during that same period.[10]

The number of issued U.S. patents has likewise risen over time. In 2015, the U.S. issued only two patents relating to blockchain. In 2018, there were 170 such patents. As of mid-2019, that figure has risen to 260. The chart below depicts the rapid growth of U.S. blockchain patents:



The largest holders of these U.S. blockchain patents as of early 2018 are shown below:[11]

Entity	Industry	No. of Blockchain Patents
Bank of America	Finance	43
MasterCard	Finance	27
IBM	Technology	27
Fidelity	Finance	14
Coinbase	Finance	13
World Award Foundation / World Award Academy / AMobilePay, Inc.	IP holding	12

Entity	Industry	No. of Blockchain Patents
TD Bank	Finance	11
402 Technologies S.A.	IP holding	10
Accenture	Technology	9
Dell	Technology	8

Because blockchain technology assists in the efficient and secure transfer of assets, it is no surprise that the financial industry currently dominates the blockchain patent space. Technology companies like IBM[12] and Dell[13] also are utilizing blockchains to improve existing technologies and processes, including supply chain and digital rights management. The IP holding companies, meanwhile, presumably seek patents solely to monetize them.

What can be protected?

Only new and novel ideas may be patented

Ideas that are already in the public domain may not be patented, and much of blockchain technology falls into that category. As discussed elsewhere in this book, a blockchain is a distributed ledgering system that allows for the memorializing of transactions in a manner that is not easily counterfeited, is self-authenticating, and is inherently secure. The basic concept of a blockchain may not be patented. A ledgering system that records such transactions, employs multiple identical copies of the ledgers, and maintains them in separate and distinct entities, similarly may not be patented as a new and novel idea. Blockchain technology also uses cryptography. Known cryptography techniques, even if used for the first time with blockchain, also are not likely to be patentable unless the combination resulted from unique insights or efforts to overcome unique technical problems.

Anyone is generally free to use these concepts and, as such, they are not patentable. So what is left that can be protected? Only novel and non-obvious ways to use the above-described blockchain distributed ledger system may be protected. For example, the traditional banking industry utilizes central banks and clearing houses to effectuate the transfer of money between entities, which often results in significant delay to complete the transactions. With access to overnight shipping, real-time, chat-based customer service, and social networks allowing for the live-video conferencing of multiple parties positioned around the globe, it is understandable that today's consumer could be disillusioned with the pace at which financial transactions move through the traditional banking industry.

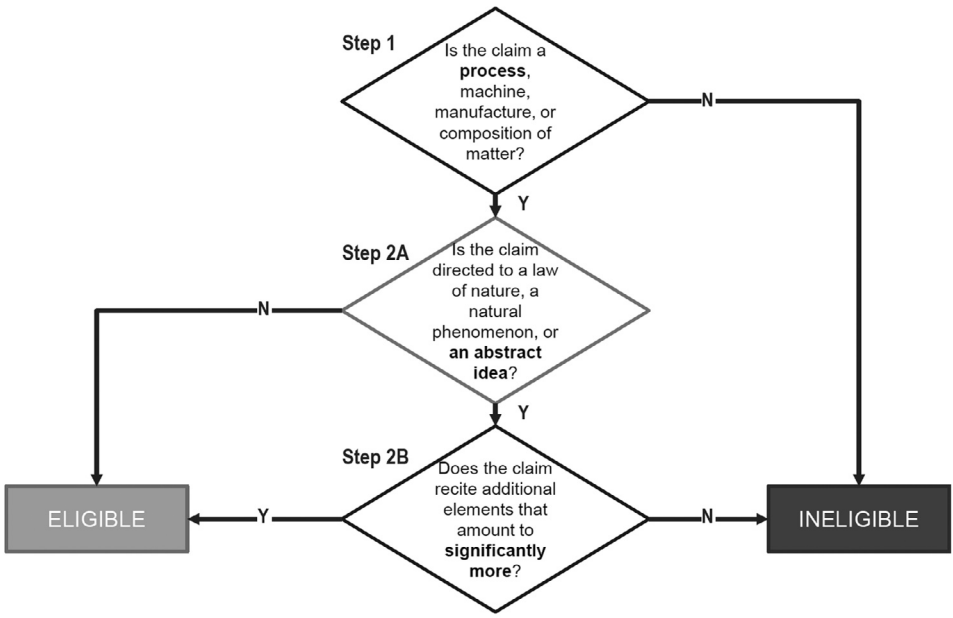
Accordingly, various companies and entities are devoting considerable time and resources to refining and revising the manner in which the traditional banking industry effectuates such monetary transactions. Entrepreneurial companies are inventing unique systems for effectuating asset transfers between banking entities that are memorialized via the above-described blockchain distributed ledgering system, as well as unique systems for expanding the utility of distributed ledgers via remote (and cryptographically secured) content defined within the distributed ledgers. These improvements, as a general proposition, build and improve upon the foundational blockchain technology. Such an improvement could take the form, for example, of an application deployed on the "foundation" of the Hyperledger platform and designed to verify the identity of participants in the hypothetical company's permissioned network, or to create audit trails for transactions on this network. It is these incremental improvements that potentially may be patentable. And it is in this area that our hypothetical company should be focusing its patenting efforts.

The *Alice* decision

Obtaining a patent by our hypothetical company also faces another obstacle. As explained by the Supreme Court in *Alice Corp. v. CLS Bank Int'l*, to be patentable, a claimed invention must be something more than just an abstract idea.[14] Rather, it must involve a technical solution to a specific problem or limitation in the field. In the *Alice* case, for example, a computer system was used as a third-party intermediary between parties to an exchange, wherein the intermediary created "shadow" credit and debit records (*i.e.*, account ledgers) that mirrored the balances in the parties' real-world accounts at "exchange institutions" (*e.g.*, banks). The intermediary updated the shadow records in real time as transactions were entered, thus allowing only those transactions for which the parties' updated shadow records indicated sufficient resources to satisfy their mutual obligations.

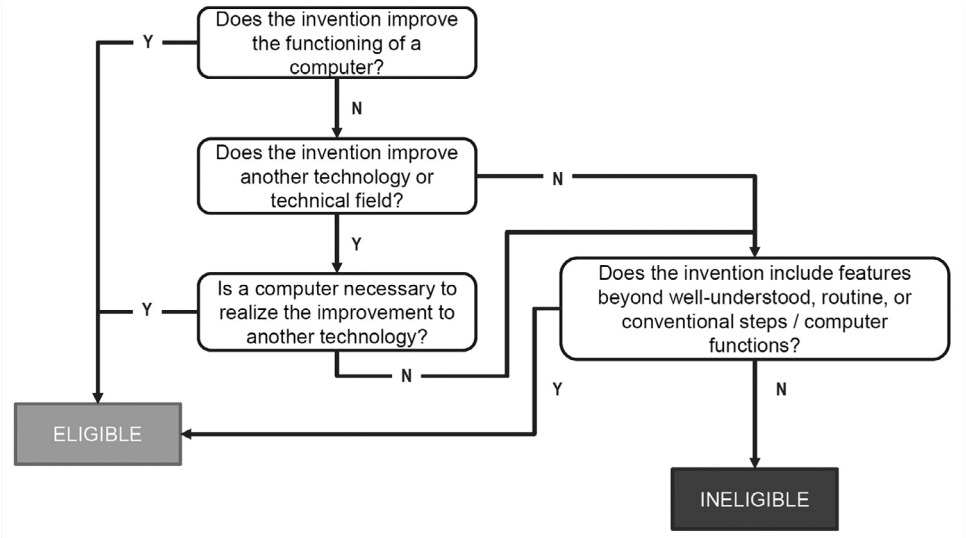
The Supreme Court held that, "on their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk." The Court went on to explain that "the concept of intermediated settlement is a fundamental economic practice long prevalent in our system of commerce." The Court then explained that such basic economic principles could not be patented, even if implemented in software or in some other concrete manner, because abstract ideas are not themselves patentable. Allowing patents on abstract ideas themselves, the Supreme Court explained, would significantly restrict and dampen innovation.

The following flowchart defines the manner in which the patentability of subject matter should be analyzed with respect to the *Alice* decision:



As such, basic concepts, even as they relate to blockchain, may not be patentable. So our hypothetical company must present more than just basic, economic principles in order to get a patent. It must, for example, claim specific improvements to the functioning of a computer, improvements to other, related technology, effect a transformation of a particular article to a different state or thing, add a specific implementation that is not well-understood, routine or conventional, or add unconventional steps that confine the claim to a particular useful application.

The following flowchart may be utilized when assessing the patentability of subject matter with respect to the *Alice* decision:



If the *Alice* decision taught practitioners anything, it is that IP law is continuously changing. Accordingly, just as a sound investment plan requires a diversified securities portfolio, a sound IP strategy requires a diversified IP portfolio. Therefore, companies should not put all of their proverbial eggs into one IP basket. For example, if a company was in the "intermediated settlement" space and all they owned were U.S. utility patents, the *Alice* decision would have been devastating to it.

Accordingly, companies should include utility patents in their IP portfolio. But the prudent company also would include design patents (for protecting, *e.g.*, user interfaces), trade secrets (for protecting, *e.g.*, backend algorithms that are not susceptible to reverse engineering); trademarks (for protecting the goodwill associated with the products produced by the company); service marks (for protecting the goodwill associated with the services provided by the company), copyrights (for protecting software code, and/or the expression of a concept or an idea); and various IP agreements (*e.g.*, employment agreements, development agreements, and licensing agreements). The best IP portfolio for our hypothetical company, therefore, should resemble a quilt that is constructed of various discrete components (utility patents, design patents, trade secrets, trademarks, service marks, copyright, and IP agreements) that are combined to provide the desired level of IP coverage.

The assertion and defense of patent litigation

The threat of patent litigation

Just a few years ago, patent litigation was ubiquitous. Identifying a unique market opportunity, non-practicing entities ("NPEs"), also known as "patent trolls," sprung up, aggregated patents, targeted specific industries, and monetized those patents either through threats of litigation or actual lawsuits. One sector that was the subject of this attack was the telecommunications industry. Beyond a number of competitor versus competitor suits (such as *Apple v. Samsung*), large, sophisticated NPEs also arose that did not make a product or sell a service. Rather, they purchased patents, created portfolios, and engaged in litigation

campaigns to force companies to pay royalties on those patents. Often, if a NPE had a large enough portfolio, then a company would enter into a license agreement to license that portfolio for a defined period of time, often five years.

In the last few years, patent litigation has waned. Due to Congress's creation of *inter partes review* ("IPR") proceedings, stricter requirements on proving damages, member organizations that acquire patents and offer licenses to their members, restrictions on where patent lawsuits may be filed, and new defenses that more easily allow patents to be invalidated at the early stages of litigation, patent litigation is no longer the economic opportunity that it previously had been. While competitors still will engage in patent litigation to preserve (or attack) their relative positions in the marketplace, NPEs have found that this changing landscape has made patent litigation financially less rewarding. To be sure, such patent litigation still exists. Indeed, new lawsuits are filed daily. The number and threat of those lawsuits has greatly diminished, however, and the value of patents generally has diminished as well.

Market changes, of course, can create new incentives for initiating patent litigations, and the increased role of blockchain technology is likely to bring about one of those changes. To the extent blockchain technology becomes prevalent, it is likely to result in substantially increased patent litigation, both between competitors and between NPEs and practicing companies. The reasons for this potential change are several:

- In a competitive landscape, certain companies – specifically those technology companies solely directed toward creating blockchain products – must use their patents to keep competitors out of the marketplace.
- Blockchain is ushering in a new set of patents, based on new technology, that have not been licensed.
- Blockchain technology will be used in lucrative fields which, by association, will make blockchain patents more valuable.
- Blockchain technology likely will be used as fundamental building blocks, making the technology more valuable and damages more lucrative.
- Blockchain startups that hold patents may fail, which could put those patents in the hands of an NPE.

Certainly, NPEs see the opportunity. Eric Spangenburg, a well-known founder of NPEs, has set up IPWE to collect and exploit blockchain patents, and Intellectual Ventures, a well-known and well-financed NPE, similarly is seeking to acquire and exploit patents in this area.[15] And our hypothetical transaction platform reflects this opportunity. If our hypothetical company builds blockchain technology into the basic building blocks of its transactions, and its transactions form the basic building blocks of its business, then it stands to reason that the technology underlying those activities has significant value.

Offensive and defensive uses of patent rights

When entering into this new technical field, therefore, it is critical that our hypothetical company understand the patent landscape. Are there so many patents that they create a barrier to entry? Are other companies actively applying for patents? If so, are they doing so to block others or require licensing fees, or are they doing so merely for defensive purposes? Understanding and properly predicting this landscape may be the difference between a successful and a failed endeavor.

Broadly speaking, the strategic use of patent rights can be categorized as offensive or defensive (or a mix of the two). These strategies are discussed in greater detail below.

Offensive uses of patent rights

From an offensive perspective, the holder of a patent gains the right to exclude others from making, using or selling the invention.[16] An offensive patent holder therefore has the ability to block all others from utilizing its patented inventions. In an emerging technical field like blockchain, patent filers typically have a more open landscape of new solutions to discover and claim. Because of the patent holder's right to exclude, each solution it is able to patent can block competitors from utilizing that solution in their own products or services absent permission.

For our hypothetical company, if the patented technology allows for a more efficient and secure transaction, then our hypothetical company may want to exclude others from using that technology, giving the hypothetical company a competitive advantage in the marketplace. If our hypothetical company does not wish to exclude competitors, it may instead allow other companies to use its patented technology, but demand that they pay reasonable royalties for that use, perhaps to help defray research-and-development costs or to create an alternative revenue stream.

It is not enough, however, for the offensive patent holder to file and receive issued patents. The offensive patent holder must affirmatively enforce its patent rights, and make sure that those patent rights are not encumbered by open source licenses, per our discussion under "The impact of open source software" below, or by FRAND licensing obligations, per our discussion under "The role of industry standards" below. Enforcement requires monitoring for activities that may infringe the patent holder's claims, demanding that others halt infringing activities and, if necessary, instituting litigation to halt the activities and/or receive reasonable compensation for those activities.

Our hypothetical company also may seek to develop income streams from its patent portfolio. By enforcing its patent rights, the offensive patent holder may force competitors to take and pay for licenses. These licenses may provide income to the offensive patent holder as a single lump sum, where the licensee pays for its license upfront, or as a running royalty, where the licensee pays a percentage of the revenue generated by its products in the marketplace.

Defensive uses of patent rights

Rather than affirmatively asserting patents, the defensive patent holder uses them as a hedge against other potential claims against it. Thus, if the hypothetical company is building a platform and cannot have that platform's use interrupted, then the hypothetical company needs to build up as many defenses against a claim of patent infringement as possible. By having its own portfolio, our hypothetical company may be able to deter competitors from a lawsuit against it, because that competitor knows that it may face claims against it if it brings a patent infringement action.

A defensive strategy, if timely performed, also can block others from securing patents that later can be asserted against it. That is, in fact, the precise strategy of Coinbase's patent filings. By filing for as many patents as possible in the blockchain field, Coinbase hopes to take away patent rights from non-practicing entities, which those entities could otherwise assert against Coinbase.[17]

Ultimately, as blockchain matures, players in the field will tend to take several forms. Patent leaders will emerge, and to avoid mutual destruction, they will enter into cross-licenses with each other. Other companies will try to enter the industry without a proper patent portfolio, and may find significant barriers to entry if the existing patent leaders seek to assert their

right to exclude those other companies from using their patented technology. And then there will be companies that simply acquire patents for the purpose of asserting them. Such companies will create transaction costs but should not bar entry into the marketplace.

* * *

Our hypothetical company must then consider a long-term strategy. Is it creating a platform of critical importance, but leaving itself vulnerable to its competitors? Is it fully taking advantage of its hard work and innovation by protecting the original and novel concepts that it created? Will it find itself blocked by aggressive competitors that are aggregating important patents? All of these questions must be addressed at the same time that our hypothetical company is investing in its technological improvements, and seeking to attract entities and (perhaps) developers to join and participate in its newly created blockchain network.

Strategies for limiting patent litigation exposure

The threat of patent litigation in the blockchain field is real. So how can our hypothetical company limit potential liability? There are several steps that it can take:

- **Open source defenses.** At a minimum, if a claim is asserted, our hypothetical company needs to consider whether that claim is blocked or barred by open source restrictions. In addition, our company also should be deliberating carefully on its own open source strategy, and how the use of open source software impacts its potential defenses and assertion rights.
- **Actively enter into cross-license agreements.** If our hypothetical company has acquired a significant patent portfolio, then it may want to approach other major players in the blockchain field and seek to enter into cross-licenses with those companies. This approach allows companies to compete based on the quality of their product or service, rather than engage in a damaging patent war.
- **Join patent pools.** In certain industries, particularly telecommunications, patent pools have arisen to help combat NPEs. These patent pools are membership-based organizations, whereby companies pay a fee for a license to all patents held by the pool. The patent pool's typical approach is to acquire patents, or take licenses on patents, for the benefit of its members. The goal of these organizations is to charge a reasonable fee for a license to a broad-based portfolio.
- **Monitoring patent application and allowed patents.** While there are many blockchain patents and patent applications, they number in the hundreds, not the thousands. As such, if committed, our hypothetical company can review patent applications as they are published (18 months after filing) and when patents issue (on average 3–4 years after filing). Doing so allows a company to identify potentially problematic patents. The downside of such an approach, however, is that such monitoring may become discoverable in a patent litigation, and perhaps can be used as evidence of knowing (willful) infringement.
- **Consider design arounds where available.** To the extent our hypothetical company identifies potentially problematic patents or applications, an option for it is to "design around" the problematic patent. In other words, our hypothetical company can analyze the particular elements that make up the invention, and eliminate one or more of those elements in its product in order to avoid practicing the patent.

- **Be prepared to file IPRs.** If our hypothetical company finds a problematic patent, then one option is to file an IPR with the Patent Office to try to invalidate the patent. Our hypothetical company can take that step even if no lawsuit has been filed against it. Deciding whether to do so requires an assessment of the likelihood that the patent can be invalidated and the cost associated with that process, but that cost will always be substantially less than the cost of patent litigation.
- **Be prepared to attack the patents on *Alice* grounds.** If our hypothetical company ends up in litigation, it still may be able to terminate that litigation early by filing an *Alice* motion, discussed more fully under "Offensive and defensive uses of patent rights" above. The blockchain concept itself is an abstract idea, and not patentable as such. To have a valid blockchain patent, the claimed idea must identify some technical problem in the field and provide some specific technical solution to that problem. Without providing something sufficiently concrete, our hypothetical company may be able to invalidate the asserted patent early in the litigation process.
- **Assert counterclaims.** As discussed above, it is important for our hypothetical company to acquire its own patent portfolio. If successful in doing that, and if sued by a practicing company, then our hypothetical company may be able to assert its own claims of patent infringement. Doing so typically makes it easier to resolve a dispute in its early stages.

The impact of open source software

The term "open source software" refers to software that is distributed in source code form. In source code form, the software can be tested, modified, and improved by entities other than the original developer. The term "proprietary" software refers to software that, in contrast, is distributed in object code form only. The developer of proprietary software protects its source code as a trade secret, and declines to allow others to modify, maintain, or have visibility into its software code base. Proponents of open source software state that the structure fosters the creation of vibrant—and valuable—developer communities, and leads to a common set of well tested, transparent, interoperable software modules upon which the developer community can standardize.

Open source software is ubiquitous in blockchain platforms. The software code bases for Bitcoin,[18] public Ethereum,[19] and Hyperledger,[20] and portions of the software code bases for Enterprise Ethereum[21] and Corda,[22] all consist of open source software. Bitcoin and Ethereum are the leading public blockchain platforms, and Hyperledger, Corda, and Enterprise Ethereum are the "big three" leading commercial, permissioned blockchain platforms.[23] Accordingly, if our hypothetical company wishes to leverage solutions that rely on software from any of these leading platforms, it must consider the impact of the licenses that govern this software.

The open source community has developed a number of licenses, and these range from (a) permissive licenses, that allow licensees royalty-free and essentially unfettered rights to use, modify, and distribute applicable software and source code,[24] to (b) restrictive, so-called "copyleft" licenses, that place significant conditions on modification and distribution of the applicable software and source code. Two open source licenses are particularly relevant to our hypothetical company: the General Public License version 3 ("GPLv3"),[25] because this license (and variants) governs large portions of the Ethereum code base,[26] and the Apache 2.0 license (the "Apache License"),[27] because this license governs open source software provided via the Hyperledger, Corda, and Enterprise Ethereum platforms.[28] Each of these licenses embodies a "reciprocity" concept that our hypothetical company must consider.

GPLv3 is known as a "strong" copyleft license. The license functions as follows: assume a developer is attracted to a software module subject to GPLv3, and incorporate this module into proprietary software that he or she then distributes to others. To the extent the developer's proprietary software is "based on" the GPLv3 code,[29] the developer is required to make his or her proprietary code publicly available in source code form, at no charge, under the terms of GPLv3. This requirement will remove trade secret protection embodied in the proprietary code, as well as the developer's ability under copyright law to control the copying, modification, distribution, and other exploitation of its software.[30] This license, therefore, has a significant impact on the developer's trade secret and copyright portfolios.

GPLv3 also has a significant impact on the developer's patent portfolio. The license obligates the developer to grant to all others a royalty-free license to patents necessary to make, use, or sell the Derivative Code.[31] Finally, simply by distributing GPLv3 code, without modification, the developer agrees to refrain from bringing a patent infringement suit against anyone else using that GPLv3 code.[32] In sum, the structure of GPLv3 reflects a strong "reciprocal" concept: if a developer wishes to incorporate open source software into its code base, it must reciprocate by contributing that code base (and all needed IP rights) back to the community. As noted above, the Ethereum code base is licensed predominantly under GPLv3. Therefore, our hypothetical company should use caution in relying on Ethereum code.

Our hypothetical company should also consider the impact on its IP portfolio of relying on Hyperledger, Corda, and Enterprise Ethereum code. The Apache license (or an equivalent) governs large portions of these code bases. For our hypothetical company, although the Apache license has reciprocal features, it is considerably more flexible than GPLv3. The Apache license impacts a developer's rights to its software under patent, trade secret, and copyright law in a manner similar to GPLv3;[33] however, these impacts only arise where the developer affirmatively contributes its software to the maintainer of the Apache code at issue. The structure functions with respect to patents as follows: if a patent owner contributes software to an Apache project, the Apache license restricts the owner from filing a patent infringement claim against any entity based on that entity's use of the contributed software. If the owner does bring such a suit, the owner's license to the Apache code underlying its contribution terminates.[34] The license thus has a reciprocal structure: a patent owner cannot benefit from Apache-licensed software while suing to enforce patents that read on its contributions to the Apache software community. If the developer, however, decides not to contribute its code to an Apache project, the developer remains free to incorporate Apache code into its proprietary code base, and commercialize this code without obligation to the Apache open source community. The Apache license, therefore, provides developers with considerable flexibility.[35]

This flexibility may present strong value to our hypothetical company. It would permit the company, for example, to leverage existing Apache-licensed software from the Hyperledger, Corda, and Enterprise Ethereum code bases in order to develop its new platform and applications, and would give the company full control over whether and to what extent it wishes to encumber its intellectual property portfolio with open source obligations.

Based on the above, it might appear that our hypothetical company would take extreme steps to avoid GPLv3 code (or other strong copyleft code) and would never contribute code to an Apache project. This, however, has not been the case. A number of entities have contributed code under the Apache license, for example, in order to encourage developers and users to adopt the permissioned commercial network that implements this code.[36] Our hypothetical

company will similarly want to consider the potential benefits of seeking to create a vibrant developer and user community using an "open" approach to its intellectual property portfolio, and potentially contributing code under an appropriate open source software license. In any event, open source software licenses and licensing techniques play a key role in blockchain technology, and our hypothetical company will want to carefully consider these licenses and techniques in its IP strategy.

The role of industry standards

Background

Industry standards refer to a set of technical specifications that a large number of industry players agree upon to use in their products.[37] Industry players collaboratively develop these technical specifications in a Standards Setting Organization (or "SSO"). Periodically, the SSO will hold meetings where participants, often scientists and engineers, who represent industry players will propose and debate differing proposals for how a technology should operate. Decisions regarding proposals, and the final technical specifications that stem from them, are reached by consensus of the participants.

Current efforts to standardize blockchain technology

Several organizations have begun standardizing a variety of blockchain technologies:

- The International Standards Organization ("ISO") has formed Technical Committee 307 ("ISO/TC 307") to consider blockchain and distributed ledger technologies.[38]
- The Institute of Electrical and Electronics Engineers ("IEEE") has formed two blockchain groups: (1) Project 2418 to develop a standard framework for the use of blockchain in Internet-of-Things applications;[39] and (2) Project 825 to develop a guide for interoperability of blockchains for energy transaction applications.[40]
- The Blockchain in Transportation Alliance ("BiTA") is focused on the use of blockchain in freight payments, asset history, chain of custody, smart contracts and other related goals.[41]
- Hyperledger is a blockchain standard project and associated code base hosted by the Linux Foundation that focuses on finance, banking, Internet-of-Things and manufacturing.[42]
- The Enterprise Ethereum Alliance recently released an architecture stack designed to provide the basis for an open-source, standards-based specification to advance the adoption of Ethereum solutions for commercial, permissioned networks (referred to as "Enterprise Ethereum").[43]

Advantages and disadvantages of standards

Advantages of using and contributing to industry standards

There are several advantages to using standards that benefit an industry at-large:

- **Ensures product compatibility** – With a standard in place, any vendor can develop a product that will be compatible with other products in the industry.
- **Stronger technology** – Technical specifications created with the input of many industry players tend to result in stronger overall technologies. In theory, the best ideas should emerge from the process and become industry standards that benefit both vendors and consumers.
- **Shifts competition from the standardized technology to implementation** – Standardization allows industry players to avoid competition with regard to the

standardized technology, and instead shift their focus to developing the best implementation of the remaining technology. Entities that participate in the standard-setting process are obligated to disclose patents that are essential for implementing the standard, and to provide licenses to these patents on fair, reasonable, and non-discriminatory terms (so-called "FRAND" terms). These FRAND obligations ensure that all implementers will bear the same licensing burden as to patents essential to the standard.

- **Greater likelihood of wide adoption** – Approval by many industry players makes the standardized approach a "safer bet" for technology adopters and investors.

Contributing to SSOs also yields several benefits to individual participants. First, a participating company gains visibility into what comes next in their industry. For example, a software vendor for a syndicated loan blockchain platform could observe the emerging form and content of the blockchain's smart contracts and begin to steer its internal development toward efficiently processing those contracts. Second, a participating company has the opportunity to guide the standardization process. For example, steering the SSO toward smart contracts that reference cloud-based digital documents would be advantageous for a vendor with a strong cloud-based solution in place.

Disadvantages of using and contributing to industry standards

There are disadvantages to employing industry standards as well. First, a company loses control over certain aspects of the technology. Instead of developing technology in isolation, our hypothetical company can be at the whim of the industry and its own competitors. Second, a company could develop its own technology that wins over others' in the marketplace. Good faith participation in an SSO implies that a company will contribute its best, most valuable ideas to the SSO instead of applying them solely to its own products. But the prize for developing better technology than the SSO's participants, and not contributing it to the SSO, is alluring: a lucrative monopoly on the best technology. Third, an SSO is less nimble than an individual company because changes to industry standards take consensus of many parties, which, in turn, take time. Finally, by participating in the SSO process, the company will place FRAND obligations on any patents in its portfolio that are essential for purposes of implementing the standard.

Lessons from wireless telecommunications industry standards

Blockchain technology is a relatively new field, and SSOs are only starting to form to develop blockchain standards. Many companies are now deciding whether to join a blockchain SSO or pursue their own solutions. The history of another technical field's, telecommunications, standardization activities provides a good example of the advantages and disadvantages of pursuing industry standards or deciding to go it alone.

In order for a phone to access a carrier's wireless network, it must know how to communicate with the carrier's network. Telecommunications standards dictate how that communication proceeds. By adhering to the telecommunications standard, a manufacturer can ensure that its phone can operate on any carrier's wireless network that also follows that standard.

In the 1980s, the European "first generation" wireless telecommunications market was fractured by a handful of standards marked by national or regional boundaries. Scandinavia used a standard called "NMT"; Great Britain used "TACS"; Italy used "RTMS" and "TACS"; France used "RC2000" and "NMT"; and Germany used "C-Netz."[44] Using this hodgepodge of telecommunications standards meant that a German's phone would not work during her vacation to France, and an Englishman's phone would not work in Scandinavia.[45] Manufacturers for both phones and network infrastructure were likewise geographically constrained. These manufacturers would typically only research and develop products for

specific European regions. What resulted were regional monopolies for those manufacturers, but with low subscriber rates and little opportunity to compete in foreign markets where their technology would be inoperable.[46]

Mindful of these issues with the first-generation wireless telecommunications standards, phone and infrastructure manufacturers from around Europe (and indeed around the world) came together to develop a pan-European, "second generation" standard within the European Telecommunications Standards Institute ("ETSI") SSO. These manufacturers sent their best scientists and engineers to ETSI to ensure that this emerging standard would meet wireless subscribers' and carriers' needs. The result of their work was the Global System for Mobile communications ("GSM"), which was the *de facto* wireless standard throughout Europe and parts of the United States from 1992 through 2002. During that period, manufacturers would compete to develop better phones or network equipment, all the while maintaining compliance with the GSM standard. As a result, equipment developed in Sweden or Finland could be sold throughout Europe. This open market brought the price of wireless technology down, increased subscriber bases and, by adoption of a similar approach in the United States, ushered in today's ubiquitous smartphones and wireless networks.

Analogies can be drawn to current trends in blockchain standardization. Blockchain is based on networks that are large enough—have enough nodes—to create reliability. As such, interoperability and scalability are important. Standardization of blockchain elements can be an important tool in achieving those goals. But the standardization process often involves competing visions. Certain companies will advance one approach, and other companies will advance a different approach. That advocacy typically is based on a good faith belief, but it also arises from investments that companies make in their technology.

A meaningful standardization process contains both risk and opportunity for our hypothetical company. No company wants to be make the wrong bet and become the "Betamax" or "HD DVD" of blockchain technology. Companies therefore need to be thinking hard about the competing standards that are being created and what role they wish to play in that creation. An entirely passive role can result in other thought leaders seizing the marketplace, but too aggressive a role can lead to massive investments that are not adopted by the marketplace as a whole. Ultimately, every company needs to think about the role that they wish to play on that spectrum.

* * *

Endnotes

1. There are a range of other differences between public and permissioned networks as well. For example, a permissioned network can be structured with different consensus rules that reduce the resource requirements (including electricity requirements) needed on a public network such Bitcoin. There are also a range of gradations between fully public and fully private blockchain networks. The Enterprise Ethereum Alliance, for example, is designed to permit operation on a public network, but to restrict the nodes on that public network that receive the data at issue. *See* I. Allison, Enterprise Ethereum Alliance Is Back – And It's Got a Roadmap (May 2, 2018), located at https://www.coindesk.com/enterprise-ethereum-alliance-isnt-dead-got-roadmap-prove/.
2. Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System* (October 31, 2008) (available at https://bitcoin.org/bitcoin.pdf).

3. 2008 is not the earliest disclosure of blockchain-like solutions. *See* Stuart Haber and W. Scott Stornetta (1991) and Bayer, Haber and Stornetta (1992).
4. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
5. https://www.lexology.com/library/detail.aspx?g=6aab712d-2ce9-401f-b37c-bffbe2aadf5f.
6. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
7. https://www.lexology.com/library/detail.aspx?g=6aab712d-2ce9-401f-b37c-bffbe2aadf5f.
8. https://www.lexology.com/library/detail.aspx?g=6aab712d-2ce9-401f-b37c-bffbe2aadf5f.
9. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
10. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
11. http://patentvue.com/2018/01/12/blockchain-patent-filings-dominated-by-financial-services-industry.
12. https://www.ibm.com/blockchain.
13. https://www.delltechnologies.com/en-us/perspectives/tags/blockchain.
14. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014).
15. Certain industry participants have been working to place restrictions on key patents, to prevent them from being acquired by NPEs. *See* Michael del Castilloite, Patent Trolls Beware: 40 Firms Join Fight Against Blockchain IP Abuse (March 16, 2017) located at https://www.coindesk.com/40-blockchain-firms-unite-in-fight-against-patent-trolls/.
16. 35 U.S. Code § 154(a)(1) ("Every patent shall . . . grant to the patentee, his heirs or assigns, of the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States . . .").
17. https://blog.coinbase.com/how-we-think-about-patents-at-coinbase-26d82b68e7db.
18. *See* http://www.bitcoin.org.
19. L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing.
20. "About Hyperledger," located at https://www.hyperledger.org/about.
21. Enterprise Ethereum Alliance Specification Clears the Path to a Global Blockchain Ecosystem (May 16, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-specification-clears-path-global-blockchain-ecosystem/.
22. "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md; Downloads: DemoBench for Corda 3.0, located at https://www.corda.net/downloads/.
23. R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038.
24. Bitcoin software, for example, is licensed under the permissive, MIT License. *See* http://www.Bitcoin.org; https://opensource.org/licenses/MIT.

25. GPLv3 license, located at https://www.gnu.org/licenses/gpl-3.0.en.html.
26. L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing. *See*, *e.g.*, Ethereum-sandbox License, located at https://github.com/ether-camp/ethereum-sandbox/blob/master/LICENSE.txt.
27. Apache 2.0 license, located at https://www.apache.org/licenses/LICENSE-2.0.
28. For Corda, *see* R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038; "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md. For Hyperledger, *see* Brian Behlendorf, "Meet Hyperledger: An 'Umbrella' for Open Source Blockchain & Smart Contract Technologies" (September 13, 2016) located at https://www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies. Code contributed to the Enterprise Ethereum Alliance is generally made available under an open source license that mirrors the Apache 2.0 license, *see* Enterprise Ethereum Alliance Inc. Intellectual Property Rights Policy, available at https://entethalliance.org/join/.
29. In defining the key term "based on," GPLv3 largely relies on copyright law rules governing derivative works. Courts generally rule that two copyrighted works are distinct (and one is not derivative of the other) if "they can live their own copyright life;" in other words, the test focuses on whether each expression "has an independent economic value and is, in itself, viable." *E.g.*, *Columbia Pictures Indus. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1192 (9th Cir. 2001); *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, 964 F.2d 965, 969 (9th Cir. 1992).
30. For convenience, the code the developer is required to open-source in this manner is referred to as "Derivative Code."
31. GPLv3, sec. 11 (Patents).
32. GPLv3, sec. 10 (Automatic Licensing of Downstream Recipients).
33. The maintainer of the relevant Apache code at issue, through the Apache Software Foundation, has the ability to set downstream terms for the contributed software.
34. Apache 2.0, sec. 3 (Grant of Patent License).
35. Our hypothetical company will also need to consider "compatibility" issues between various open source licenses. The Hyperledger platform, for example, was unable to assimilate Ethereum code due to incompatibility between the Apache license and strong copyleft licenses, and the resulting need to obtain permissions from copyright owners to "re-license" the Ethereum code at issue. *See* J. Manning, Hyperledger Fails Ethereum Integration Due To Licensing Conflicts (February 3, 2017), located at https://www.ethnews.com/hyperledger-fails-ethereum-integration-due-to-licensing-conflicts; J. Buntinx, Ethereum app Developers may Face Licensing Issues Later on (December 6, 2017), located at https://www.newsbtc.com/2017/12/06/ethereum-app-developers-may-face-licensing-issues-later/.
36. IBM, for example, has contributed code under the Apache license to the Hyperledger platform, and in turn is providing commercial Blockchain-as-a-Service (BaaS) offerings based on this platform using IBM's cloud infrastructure. *See* IBM Blockchain, The Founder's Handbook: Your guide to getting started with Blockchain (Edition 2.0) located at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=28014128USEN. Microsoft has similar commercial offerings, based on Azure and

the Enterprise Ethereum platform. *See* M. Finley, Getting Started with Ethereum using Azure Blockchain (January 24, 2018), located at https://blogs.msdn.microsoft.com/premier_developer/2018/01/24/getting-started-with-ethereum-using-azure-blockchain/.

37. A simple example is the shape and voltage of a wall power outlet. Because the power outlet is standardized among geographic regions, an appliance maker can ensure that its coffee maker will work (and can be sold) anywhere within a given region.
38. https://www.iso.org/committee/6266604.html.
39. http://standards.ieee.org/develop/project/2418.html.
40. http://standards.ieee.org/develop/project/825.html.
41. https://bita.studio.
42. https://www.hyperledger.org.
43. Enterprise Ethereum Alliance Advances Web 3.0 Era with Public Release of the Enterprise Ethereum Architecture Stack (May 2, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-advances-web-3-0-era-public-release-enterprise-ethereum-architecture-stack/; https://entethalliance.org/wp-content/uploads/2018/05/EEA-TS-0001-0-v1.00-EEA-Enterprise-Ethereum-Specification-R1.pdf.
44. Funk, Jeffrey L., Global Competition Between and Within Standards: The Case of Mobile Phones at 39 (New York, Palgrave, 2002); Garrard, Garry A., Cellular Communications: Worldwide Market Development (Boston, Artech House, 1998).
45. Gruber, Harald, The Economics of Mobile Telecommunications (Cambridge University Press, 2005) at 35.
46. *Id.*

Joshua Krumholz
Tel: +1 617 573 5820 / Email: Joshua.Krumholz@hklaw.com

Josh Krumholz is a partner in Holland & Knight's Boston office. A trial attorney and the national Practice Group Co-Leader for the firm's Intellectual Property Group, Mr Krumholz focuses primarily upon intellectual property litigation, with a particular focus on patent litigation. His practice covers a variety of technologies and jurisdictions. Mr Krumholz has successfully taken cases to jury verdict in the Eastern District of Texas, Illinois, Massachusetts, New York and New Jersey, among other jurisdictions. Technologies that Mr Krumholz handles include telecommunications, software, hardware, electronics and consumer goods. Mr Krumholz represents leading companies across a range of industries, including Ericsson Inc., T-Mobile, Inc., Verizon Corp., Avaya Inc., Acushnet Company and Hasbro, Inc., among others.

Ieuan G. Mahony
Tel: +1 617 573 5835 / Email: Ieuan.Mahony@hklaw.com

Ieuan Mahony is a partner in Holland & Knight's Boston office. He concentrates his practice in intellectual property (IP) licensing and development, data privacy and security, and information technology (IT). Mr Mahony combines his transactional and compliance work with dispute resolution and litigation matters. His substantial background in transactional and litigation practice areas helps clients receive high-quality advice in the dynamics of reaching an agreement as well as the realities of combating an adversary. Mr Mahony is a member of the firm's three-partner Information Technology Governance Committee.

Brian J. Colandreo
Tel: +1 617 305 2143 / Email: Brian.Colandreo@hklaw.com

Brian Colandreo is a partner in Holland & Knight's Boston office. Mr Colandreo serves as the National Patent Practice Leader and is a member of the Intellectual Property Group. A registered patent attorney, Mr Colandreo focuses his practice on client management, general intellectual property prosecution, transactional work, litigation support, due diligence work, and utility and design patent opinion work. Prior to entering law school, Mr Colandreo worked as a systems/software engineer for Johnson Controls.

Holland & Knight LLP

800 17th Street N.W., Suite 1100, Washington, DC 20006, USA
Tel: +1 202 955 3000 / Fax: +1 202 955 5564 / URL: www.hklaw.com

The custody of digital assets – 2020

Jay G. Baris
Shearman & Sterling LLP

Introduction

The growing fascination with digital assets, including cryptocurrencies and tokens, presents legal and operational challenges to investors, entrepreneurs and service providers, not to mention the regulators who oversee them. Perhaps no cryptocurrency issue presents more challenges than custody: how do individuals, broker-dealers, investment advisers, private funds and registered investment companies legally and effectively safeguard digital assets?

On the surface, the answer is simple: individuals can store their cryptocurrencies through a third-party custodian or intermediary, or, alternatively, directly in a "digital wallet" by controlling a "private key." Private funds managed by registered investment advisers can store their cryptocurrencies with "qualified custodians." Registered investment companies can store their cryptocurrencies only with custodians that meet additional requirements.[1]

But, alas, as is often the case with digital assets, a practical solution is not so simple. In reality, the operational and regulatory issues are more complicated, including whether the custody arrangements meet regulatory requirements, and whether they provide adequate safeguards, regardless of regulatory requirements.[2]

This chapter examines the custody requirements that apply to various industry players under U.S. Investment Advisers Act of 1940, as amended (the "Advisers Act")[3] and the Investment Company Act of 1940, as amended (the "1940 Act"),[4] and analyses the challenges that they and the regulators face in evaluating arrangements for safeguarding digital assets.[5]

Terminology

Before we examine the legal requirements for custody, it is helpful to ensure that we use consistent terminology.

For the purposes of this chapter, "cryptocurrencies" refer to digital assets that function as a digital representation of a store of value, such as Bitcoin or Ethereum or similar assets. Cryptocurrencies are not issued or backed by a central government, and thus are not legal tender. Alternatively, we refer to cryptocurrencies as "digital currency" or "virtual currency."

"Utility tokens" refer to coins or tokens that serve a particular (non-incidental) function, or give the holder rights or access to goods, licenses or services. A common form of utility token may give the holder the right to use a computer program that provides a kind of service for a defined period of time. Some refer to utility tokens as "app coins," "app tokens," or "utility coins." Some utility tokens may be securities, others are not. As we will see later, whether or not a utility token is characterized as a security becomes critical in evaluating what custody rules apply.

"Security tokens" or "investment tokens" are tokens or coins that are securities for purposes of the federal securities laws. The status of a token as a securities token may be intentional

or unintentional. Some utility tokens may start out as securities and at some point morph into non-securities, depending on their usage, how they are sold, and the expectations of the holders of those tokens.

Simply labelling a digital asset as a utility token, however, does not mean that the digital asset is not a security.[6] The analysis of whether or not a utility token functions as a security token, or when a security token transforms into a utility token is beyond the scope of this chapter, but, again, the distinction is relevant for purposes of the custody analysis.

Legal requirements for custody of digital assets

Background

Current U.S. federal securities laws impose strict requirements on investment companies and investment advisers to safe-keep their assets and those of their clients. These laws are designed not just to ensure that assets are held securely, but also to enable auditors to verify that the assets exist. Why can't the SEC apply these laws to safekeeping of cryptocurrencies, digital tokens and other digital assets? The simple answer is that these existing laws and regulations do apply to digital assets (maybe, and at least in theory). The real mystery to be solved is precisely *how* they apply.

The safeguarding of client assets has long been a priority of Congress and the Securities and Exchange Commission (the SEC). The legislative history of the 1940 Act, and, by implication, its companion statute, the Advisers Act, shows that Congress was clearly concerned with the potential for abuses or misappropriation of client assets held in investment trusts and investment companies that are managed by investment advisers:[7]

> That investors in investment trusts and investment companies are subject to substantial losses at the hands of unscrupulous persons is obvious from the very nature of the assets of such companies. Their assets consist almost invariably of cash and marketable securities. They are liquid, mobile, and easily negotiable. These assets can be easily misappropriated, 'looted,' or otherwise misused for the selfish purposes of those in control of these enterprises. In the absence of regulating legislation, individuals who lack integrity will continue to be attracted by the opportunity available for personal profit in the control of the liquid assets of investment trusts and investment companies.[8]

The Senate had similar concerns:

> Basically the problems flow from the very nature of the assets of investment companies. The assets of such companies invariably consist of cash and securities, assets which are completely liquid, mobile and readily negotiable. Because of these characteristics, control of such funds offers manifold opportunities for exploitation by the unscrupulous managements of some companies. These assets can and have been easily misappropriated and diverted by such types of managements, and have been employed to foster their personal interests rather than the interests of public security holders. It is obvious that in the absence of regulatory legislation, individuals who lack integrity will continue to be attracted by the opportunities for personal profit available in the control of the liquid assets of investment companies and that deficiencies which have occurred in the past will continue to occur in the future.[9]

These issues made national headlines in December 2008, when Bernard L. Madoff admitted to perpetrating a massive Ponzi scheme in which he convinced his clients that they owned securities that did not exist. For years, he evaded regulatory scrutiny until the scheme began

to unravel. This scandal prompted the SEC to take actions to reduce the chance that a Madoff-style fraud would occur or go undetected in the future.[10] While the SEC took steps to bolster its oversight and enforcement functions, it focused on rules designed to enhance the custody rules for investment advisers and broker-dealers. In December 2009, the SEC amended Advisers Act Rule 206(4)-2 (the "custody rule"),[11] which was designed to provide greater assurance that investors' accounts contain the funds that their account statements say they contain.

Among other things, the rule encouraged advisers to maintain their clients' assets with independent custodians. For investment advisers who can control their clients' assets, the rules require enhanced procedures, such as surprise asset-counts, third-party reviews and audited financial statements. To be sure, when the U.S. Congress enacted the 1940 Act and the Advisers Act, it clearly did not contemplate, or could even dream of, how the law would apply to digital assets such as cryptocurrencies or utility tokens. But the basic concerns of preventing fraud or misappropriation are just as valid today as they were in 1940. The only difference, of course, is that we are now attempting to apply 80-year-old laws designed to protect assets consisting of cash and securities to an entirely new class of digital assets created by a technology that did not exist at the time the laws were written.

What is "custody"?

Rule 206(4)-2 under the Advisers Act defines custody to mean "holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them." The regulation provides that a registered investment adviser has custody of an asset "if a related person holds, directly or indirectly, client funds or securities, or has any authority to obtain possession of them, in connection with advisory services you provide to clients."

Rule 206-4(2) defines custody of an asset to include:

- possession of client funds or securities;
- any arrangement (including a general power of attorney) under which the registered investment adviser is authorized or permitted to withdraw client funds or securities maintained with a custodian upon your instruction to the custodian; and
- any capacity (such as general partner of a limited partnership, managing member of a limited liability company or a comparable position for another type of pooled investment vehicle, or trustee of a trust) that gives the registered investment adviser or its supervised person legal ownership of or access to client funds or securities.

A threshold question is: does the SEC's custody rule apply to digital assets? The answer depends on the facts and circumstances.

The SEC's Division of Investment Management has said that Rule 206(4)-2 does not apply to an adviser to the extent that it manages assets that are "not funds or securities."[12] Does this mean that advisers to clients or funds that invest in Bitcoin are free to hold these assets in personal digital "wallets" without regard to federal regulation? If not, to what standard will an adviser be held?

The answer, of course, depends on whether cryptocurrencies are "funds or securities" for purposes of Rule 206-4(2). In light of the legislative history, which makes the protection of investors' assets a priority, it is possible that most, if not all, digital assets would be considered "funds or securities," at least for purposes of the Advisers Act and the custody rule. The matter, however, is not free from doubt.

What are the legal custody requirements for an investment adviser?

The first step in analyzing the legal requirements for the custody of assets is to determine the nature of the investment adviser. The two threshold questions are:

- What law applies? That is, is the adviser an "investment adviser" as defined in the Advisers Act?
- If yes, is the adviser registered or required to be registered under the Advisers Act?

Next, we examine the nature of the assets and the nature of the entity that holds them.

What law applies?

To determine what law applies, we must look at the nature of the person or entity that holds or proposes to hold a digital asset. The holder of a digital asset can be:

- A natural person, directly or in a managed account.
- A pooled investment vehicle that is not an investment company, such as a hedge fund, private equity fund, or other private fund.
- A pooled investment vehicle that is registered as an investment company.
- A regulated entity such as a broker-dealer, bank or investment adviser.
- An operating company.
- Other pooled investment vehicles that might be commodity pools that otherwise would be investment companies but for an exemption under the 1940 Act.

Our focus here will be investment advisers and their clients, including natural persons, private funds and investment companies. We first discuss investment advisers and then registered investment companies.

What is an investment adviser?

Section 202(a)(11) of the Advisers Act defines an investment adviser as a person or entity that:

- engages in the business of advising others, directly or indirectly,
- as to the value of securities or as to the advisability of investing in securities,
- for compensation.

If you satisfy each of these three elements, you are an investment adviser for purposes of the Advisers Act unless you fall within one of the statutory exemptions.[13] If you fall within the definition of an investment adviser, the next step in the analysis is to determine whether you are required to register under the Advisers Act.

This analysis is important, because a person that falls within the statutory definition of an investment adviser (a) is subject to regulation by the SEC, and (b) meets certain statutory thresholds or otherwise is required to register with the SEC, the person may be subject to the substantive provisions of the Advisers Act and its rules, including Rule 206(4)-2 (the SEC rule that applies to the custody of client assets).

Is the adviser providing advice to anyone about *securities?* For example, an adviser that solely provides investment advice about "commodities" would not be an investment adviser. For purposes of this discussion, we will assume that a "pure cryptocurrency," such as Bitcoin or Ethereum, is a commodity, and not a security.[14] Thus, an investment adviser that only provides advice to persons that invest in Bitcoin or Ethereum would not be an investment adviser, because these cryptocurrencies are not securities.[15]

The answer may be different if the investment adviser is providing advice about a derivative, the reference asset of which is a cryptocurrency. In that case, the advice may relate to a security (e.g., a structured note that links a return to a benchmark reference cryptocurrency or shares of a trust that holds cryptocurrency) or a commodity-related instrument that is regulated under the Commodity Exchange Act (e.g., a forward, future, put, call, straddle, swap, etc. relating to a cryptocurrency).

If the entity is providing advice with respect to securities, the entity may have to register with the SEC, depending on whether the person: (a) meets the statutory thresholds that permit registration; (b) is required to register by the Advisers Act; or (c) is eligible for status as a an "exempt reporting adviser."[16]

Investment advisers not required to register under the Advisers Act

The Advisers Act provides several voluntary exemptions from registration, including, among others:

- intrastate advisers, that is, advisers whose clients all reside in the state in which the adviser maintains its principal place of business;
- advisers whose only clients are insurance companies;
- "foreign private advisers," which generally are advisers that (a) have no place of business in the U.S., (b) have fewer than 15 clients and investors in private funds in the U.S., (c) have less than $25 million in assets under management attributable to those clients and investors, and (d) do not hold themselves out as investment advisers in the U.S.;
- charitable organizations and plans;
- certain commodity trading advisors registered with the Commodities Futures Trading Commission ("CFTC");
- private fund advisers, which generally are advisers solely to private funds that have less than $150 million in assets under management in the U.S.;
- venture capital fund advisers; and
- advisers to small business investment companies (SBICs).

Advisers that rely on the private fund adviser exemption and the venture capital fund exemption are considered "exempt reporting advisers." Exempt reporting advisers must file with the SEC certain disclosures on Form ADV, but generally they are not subject to the substantive rules of the Advisers Act, including the custody rule (discussed below).

Exempt reporting advisers, and investment advisers that fall within the definition but are not required to register are, however, nonetheless subject to the anti-fraud provisions of the Advisers Act, not to mention their fiduciary obligations to those clients under federal law. This includes state-registered investment advisers and investment advisers that are not required to register anywhere. While these investment advisers are not subject to the custody rule, it is reasonable to presume they still must exercise care and prudence in maintaining or arranging for the custody of their clients' digital assets, including a responsibility to disclose related risks.

We discuss some of the challenges that investment advisers face in maintaining custody of digital assets below.

Investment advisers required to register under the Advisers Act

Rule 206(4)-2, the custody rule under the Advisers Act, applies to investment advisers registered, or required to be registered with the SEC ("RIAs") that have "custody" of client funds or securities.

How does a qualified custodian maintain custody of client assets? The custody rule defines what entity can serve as a custodian, and prescribes specific steps that investment advisers with custody of client assets must take. Rule 206-4(2), however, stops short of specifying *how* a custodian must safeguard—or maintain custody of—the client's assets.

As noted, an RIA is deemed to have "custody" of client assets if the RIA (or its related person) directly or indirectly holds client funds or securities, or has any authority to obtain possession of them.[17] This authority can arise out of custodial or advisory arrangements. For example, an adviser that has access to a client's private key to a cryptocurrency holding could be deemed to have access to the client's asset, even if the same key is held by a third-party custodian. Depending on the facts and circumstances, the SEC staff has said, "custodial agreements could impute advisers with custody they otherwise did not intend to have."[18] Other arrangements in which an RIA is presumed to have custody of client assets include when an RIA or an affiliate acts as general partner or managing member to a private fund.

Put another way, it would be difficult for an RIA to avoid having custody of client funds and securities unless an RIA neither holds, nor has authority to obtain possession of, client funds and securities, including digital assets. When an RIA or its related person is deemed to have custody of client funds or assets, it must comply with certain requirements under Rule 206(4)-2(a), unless an exception in Rule 206(4)-2(b) applies. Unless the RIA qualifies for such an exception, an RIA that fails to comply likely violates the anti-fraud provisions of the Advisers Act.[19]

What does the custody rule require of RIAs? Unless an exemption applies, if an RIA or its "related person" has custody of a client's assets (including funds and securities), Rule 206(4)-2(a)(1) requires the RIA to use a "qualified custodian" to maintain those client funds and securities:

- in a separate account for the client under the client's name; or
- in accounts that contain only the client's funds and securities, under the RIA's name as agent or trustee for the client.

Qualified custodian. A "qualified custodian" includes:

- Many federal and state chartered banks.
- Registered broker-dealers holding client assets in customer accounts.
- Registered futures commission merchants holding client assets in customer accounts (but generally only with respect to futures contracts and other securities incidental to transactions in futures and related options).
- Foreign financial institutions that customarily hold financial assets for customers, provided that they keep advisory clients' assets in customer accounts segregated from its proprietary assets.[20]

Notice, Account Statement and Examination Requirement. Rules 206(4)-2(a)(2), (a)(3) and (a)(4) impose certain notice, account statement, and examination requirements on RIAs if RIAs or their "related persons" have custody of client funds or securities, unless an exemption is met. These requirements are relatively burdensome.

Notice to clients requirement. When an adviser opens an account with a qualified custodian on the client's behalf, Rule 206(4)-2(a)(3) requires the RIA to notify the client *in writing* of

the qualified custodian's name, address, and the manner in which the custodian maintains the funds or securities in the account, promptly when the account is opened and following any changes to this information.

Account statement requirement. Rule 206(4)-2(a)(3) requires that the qualified custodian send account statements to each client for which it maintains funds or securities, unless an exemption applies. The statements, which must be sent at least quarterly, must identify the amount of funds and each security in the account at the end of the period, and all transactions during the period. RIAs must "have a reasonable basis, after due inquiry" for believing that the qualified custodian has sent the required account statements. This necessarily entails due diligence. Advisers have the option of sending their own account statements to their clients, in addition to those required to be sent by the qualified custodian. In this event, the notice to clients (summarized above) must include a statement "urging the client to compare the account statements from the custodian with those from the adviser."[21]

When the RIA (or a related person of the RIA) serves as general partner or the equivalent of a pooled investment vehicle, the qualified custodian must send the account statement to each beneficial owner of the fund.[22] This is so unless the audit exception for pooled investment vehicles (described below) applies.

Surprise audit requirement. Under Rule 206(4)-2(a)(4), at least once during each calendar year, RIA and "related person" custodied funds and securities must be verified by actual examination in a "surprise audit," unless an exemption applies. The surprise audit—which is really a securities count and not a traditional "audit" of financial statements—must be conducted by an independent public accountant at a time be chosen by the accountant without prior notice or announcement to the RIA and that is irregular from year to year.

The surprise audit must be subject to a written agreement. The written agreement must provide for an initial surprise examination within six months of becoming subject to the surprise audit, except that if the RIA is a "qualified custodian," then the agreement must provide for the first surprise audit to commence not later than six months after the adviser obtains an "internal control report" as described below.

The written agreement must require the independent public accountant to: (a) file a certificate on Form ADV-E within 120 days of the examination date, stating that it has examined the funds and securities, and describing the nature and extent of the examination; (b) notify the SEC within one business day of any findings of "material discrepancies" during the examination; and (c) notify the SEC by filing Form ADV-E accompanied by certain statements regarding the registration if the independent public accountant resigns, or is dismissed, removed or terminated.[23]

Surprise audits of digital assets may pose significant challenges for independent auditors, who must validate that the private key actually represents ownership of a cryptocurrency without the benefit of traditional ownership indicia supported by securities registrars, control practices associated with regulated securities intermediaries, known and trusted parties to receive verification requests, etc.

Pooled investment vehicles. When the RIA (or a related person of the RIA) serves as general partner (or the equivalent) of a pooled investment vehicle, it can satisfy the notice, account statement and surprise audit requirements described with respect to the fund that is subject to an annual audit:

(a) if at least annually, the fund sends its audited financial statements, prepared in accordance with generally accepted accounting principles, to all limited partners (or members or other beneficial owners) within 120 days of the end of its fiscal year;

(b) by an independent auditor that is registered with and subject to regular inspection as of the commencement of the engagement, and as of each calendar year-end, by the Public Company Accounting Oversight Board ("PCAOB") in accordance with its rules; and

(c) upon liquidation, and distributes its audited financial statements prepared in accordance with generally accepted accounting principles ("GAAP") to all limited partners (or members or other beneficial owners) promptly after the completion of the audit.

Similar asset verification challenges to those described above apply during the audit process.

Independent advisers or related parties acting as qualified custodians. RIAs that maintain custody of client funds or securities, directly or through a related person that has actual rather than deemed custody (i.e., those acting as a qualified custodian) "in connection with" advisory services, must comply with two requirements that require the use of independent public accountants.[24]

First, a PCAOB-registered and inspected independent public accountant must satisfy the surprise audit requirement (discussed above). RIAs must obtain, or receive from their related person, a written internal control report *within six months of becoming subject to such requirement and at least once per calendar year.*

Second, the internal control report must be prepared by an independent public accountant. The internal control report must include an opinion of a PCAOB-registered and inspected independent public accountant "as to whether controls have been placed in operation as of a specific date, and are suitably designed and are operating effectively to meet control objectives relating to custodial services, including the safeguarding of funds and securities held by either the RIA or a related person on behalf of the RIA's advisory clients, during the year." The independent public accountant must verify that the funds and securities are reconciled to a custodian other than the RIA or its related persons. A copy of any internal control report obtained or received is subject to record-keeping requirements.[25]

Non-U.S. advisers. Generally, non-U.S. RIAs with a principal place of business outside of the U.S. are not subject to the custody rule with respect to their non-U.S. clients. This includes a client that is a non-U.S. fund (organized outside the U.S.), whether or not the fund has U.S. investors.[26]

How does a qualified custodian maintain custody of client assets? The custody rule defines what entity can serve as a custodian, and prescribes specific steps that advisers with custody of client assets must take. Rule 206-4(2), however, stops short of specifying *how* a custodian must safeguard—or maintain custody of—the client's assets. The lack of specificity has not been an issue for registered investment advisers that are deemed to have custody of traditional assets, such as stocks, bonds, futures contracts, or derivatives contracts. The custody rule, however, leaves open the question of *how* to provide custody for digital assets.

Registered investment companies

Section 17(f) of the 1940 Act and its regulations govern how registered investment companies must maintain custody of their assets.[27] This section requires a registered fund to maintain its securities and similar investments with certain types of custodians under conditions designed to assure the safety of the fund's assets.[28] While the section addresses custody of fund assets by certain banks, broker-dealers and futures commission merchants ("FCMs"), as well as securities depositories, unsurprisingly it does not specifically address custody of digital assets.

Notably, Section 17(f)(1) refers to "securities and similar investments," which is a broader category of assets than covered by the custody rule under the Advisers Act.

Section 17(f)(1) provides that every registered management company shall place and maintain its securities *and similar investments* in the custody of:

- a bank;
- a company that is a member of a national securities exchange, subject to the SEC's rules; or
- the investment company itself, subject to the SEC's rules.

When Congress enacted Section 17(f), of course, no-one anticipated how it would apply to digital assets. The term "and similar investments," however, can readily be read to include digital assets.

Rule 17f-1 under the 1940 Act governs custody of investment company assets maintained by broker-dealers that are members of a national securities exchange. Among other things, Rule 17f-1 requires that the securities *and similar investments* held in such custody shall at all times be individually segregated from the securities and investments of any other person and marked in such manner as to clearly identify them as the property of such registered management company, both upon physical inspection thereof and upon examination of the books of the custodian. The rule, however, is a bit dated if its terms are to be taken literally: "The physical segregation and marking of such securities and investments may be accomplished by putting them in separate containers bearing the name of such registered management investment company or by attaching tags or labels to such securities and investment."

Rule 17f-2 governs custody by the investment company itself or by a bank.

Rule 17f-2(a) provides that "[t]he securities and similar investments of a registered management investment company may be maintained in the custody of such company only in accordance with the provisions of this section." While the rule is deemed largely unworkable by the industry, it is in any event not clear how an investment company itself could take custody of digital assets without running afoul of the other provisions of the 1940 Act.

This section also addresses custody by banks:

> Except as provided in paragraph (c) of this rule, all such securities and similar investments shall be deposited in the safekeeping of, or in a vault or other depository maintained by, a bank or other company whose functions and physical facilities are supervised by Federal or State authority. Investments so deposited shall be physically segregated at all times from those of any other person and shall be withdrawn only in connection with transactions of the character described in paragraph (c) of this rule.

Rule 17f-4 allows investment companies to maintain custody of assets with a securities depositary or intermediate custodian, subject to certain conditions.

Rule 17f-6[29] generally provides that investment companies may "place and maintain cash, securities, and similar investments with a Futures Commission Merchant in amounts necessary to effect the Fund's transactions in Exchange traded futures contracts and commodity options," subject to certain conditions to safeguard the assets.

In sum, a registered investment company can comply with the requirements of Section 17(f) by placing digital assets in the possession of a bank, a broker-dealer that is a member of a national securities exchange, or a securities depository.

Funds that utilize certain derivatives related to digital assets (e.g., swaps, futures, options) can maintain custody with the futures commission merchant, but the custody arrangements present challenges when the derivative calls for physical settlement of the underlying asset, which we discuss below.

Other custody considerations for registered investment companies include oversight by chief compliance officers and the fund's board of directors.

Funds that invest in digital assets directly or indirectly through derivatives must ensure that their compliance policies and procedures and disclosures address, among other things, the attendant risks.

Legal and practical custody challenges faced by investment advisers and investment companies with respect to digital assets

Custody of "traditional" assets, such as stocks and bonds, is a straightforward matter. Back in days gone by, custodian banks would lock up a paper stock certificate or bond in a concrete-encased steel vault, access to which was restricted. To verify that the assets existed, auditors would enter the vault and literally pick up the certificates and count them. Technological (and legal) innovation led to "uncertificated" or "book-entry" securities, making paper certificates obsolete. Rather than issue paper stock certificates or bonds, issuers only record ownership of securities on their books. These securities are then often held electronically in "street name" through banks and brokers. This technology allows auditors to easily verify that an investor owns a particular security.

Investment advisers, whether or not they are registered with the SEC, and investment companies, face challenges when designing a custody arrangement that meets the regulatory requirements as well as protecting the client's digital assets. Custody of digital assets involves different processes and procedures than custody of physical assets. For example, the risk of cybertheft is greater in the case of a digital asset, or the custodian may lose or misplace a private key. Similarly, if the custodian transfers the digital asset to an unauthorized person in error, it may not have recourse to recover the asset.[30]

Distributed ledger technology ("DLT"), such as blockchain, presents a novel challenge: how can a custodian—and an auditor—be certain that the custodian has actual and exclusive possession of a digital asset?

With these challenges in mind, let us begin by asking: how does an investment adviser maintain custody of a digital asset? To start, a registered investment adviser can satisfy the custody rule by maintaining the digital assets with a "qualified custodian." To be sure, some qualified custodians have begun to accept digital asset custody accounts, and more are expected to enter that business.

Arguably, that is the easy part. Now comes the challenge: how does the qualified custodian maintain custody of digital assets in a way that satisfies regulatory scrutiny and provides adequate safeguards for the client or fund's assets? How much protection against fraud can a qualified custodian of digital assets really provide, and what liability would it be willing to accept by contract?

In theory, the answer is simple: to prove you own or "have possession" of a digital asset, such as one bitcoin, you must have both a *public* key and a corresponding *private* key to prove you own the asset, much the same way access to a safe deposit box is accessible by the bank's key and the depositor's private key. The public key appears as a string of computer-coded entries on a digital ledger, representing a unique transaction that is added

on as a "block" in a chain of other transactions, understood to represent a particular digital asset. In public blockchains, these digital entries are visible to and verifiable by all "nodes" that have access to the internet.

The private key, however, is a string of digits that is intended to be kept secret, a sort of electronic bearer instrument. Whoever has the private key to a particular digital asset can transfer it immutably and potentially anonymously to anyone. The challenge, then, is how to ensure that the digital asset in the safekeeping of a custodian are in fact safe, and cannot be stolen or misappropriated. Moreover, the fact that a custodian holds the private key may not be sufficient to demonstrate that, by itself, the custodian has *exclusive* control of the digital asset, because it may not be possible to prove that some other unauthorized person does not also have access to the private key.[31]

The answer to this riddle may involve a combination of physical and electronic solutions, combined with common sense-procedural safeguards and a measure of creative legal thinking.

Some special purpose banks assert that they have developed tailored platforms and procedures to ensure that they can keep digital assets safe. These procedures may include, among other things, maintaining digital assets in a "cold" or offline digital wallet, rather than on an "exchange," requiring multiple electronic signatures in order to use or obtain access to the private key (sometimes referred to as "multisignature" or "multisig" and keeping the private key on a thumb drive or hard drive on a computer in a physical vault (and to wax metaphorically, encase the vault in concrete and surround it with an alligator-filled moat)). These physical safeguards, combined with layers of cybersecurity (e.g., no access by internet connection) may be reasonably sufficient (but by no means absolutely foolproof) to prevent bad actors from hacking in and stealing the private key.

In the final analysis, however, digital assets are essentially bearer assets. In general, a bad actor who obtains possession of the private key can, in theory, misappropriate the asset, no matter where the private key maintained.

Some industry participants have addressed this risk by proposing to obtain insurance against loss or theft of the digital asset. While insurance may address some of the counterparty and custody risks associated with cryptocurrencies, it may be costly and may not completely cover potential risks.

As already suggested, there also are other practical considerations that apply to the auditors of accounts holding digital assets. For example, how will independent auditors verify ownership of the digital asset? To whom would they send the audit letter requesting confirmation?

Challenges for registered investment companies.[32] Registered funds face additional challenges if they wish to invest in digital assets.

Registered funds must also ensure that that the board of directors has sufficient information to provide meaningful oversight of the fund's custody arrangements. Among other things, fund directors must approve the compliance policies and procedures of the investment company and its investment adviser, and also must approve of contractual arrangements with fund custodians. While some qualified custodians are willing to take custody of digital assets held by registered investment companies, they may face some challenges. For example, will the fund directors be satisfied that the custodian has adequate safeguards in place to protect the assets? Will the custodian's limitations on liability be acceptable to the directors? Will the directors conclude that the cost of cryptocurrency custody is reasonable?

The staff of the SEC staff raised these issues in a letter dated January 18, 2018 by Dalia Blass, Director of the Division of Investment Management.[33]

> The 1940 Act imposes safeguards to ensure that registered funds maintain custody of their holdings. These safeguards include standards regarding who may act as a custodian and when funds must verify their holdings. To the extent a fund plans to hold cryptocurrency directly, how would it satisfy the custody requirements of the 1940 Act and relevant rules? We note, for example, that we are not aware of a custodian currently providing fund custodial services for cryptocurrencies. In addition, how would a fund intend to validate existence, exclusive ownership and software functionality of private cryptocurrency keys and other ownership records? To what extent would cybersecurity threats or the potential for hacks on digital wallets impact the safekeeping of fund assets under the 1940 Act?

These custody issues carry over to settlement of digital asset-related derivatives. That is, when a fund holds certain derivatives that are based on the value of an underlying digital asset, the futures commission merchant, which holds the derivative position for the benefit of the fund, will satisfy the qualified custodian requirements. But a fund that takes a long position in a Bitcoin futures contract may be required to accept Bitcoin when the contract matures, or to deliver Bitcoin to a futures commission merchant upon settlement of a short position. The Blass Cryptocurrency Letter noted the challenges that registered funds will face when taking positions in cryptocurrency-based derivatives:

> While the currently available bitcoin futures contracts are cash settled, we understand that other derivatives related to cryptocurrencies may provide for physical settlement, and physically settled cryptocurrency futures contracts may be developed. To the extent a fund plans to hold cryptocurrency-related derivatives that are physically settled, under what circumstances could the fund have to hold cryptocurrency directly? If the fund may take delivery of cryptocurrencies in settlement, what plans would it have in place to provide for the custody of the cryptocurrency?

The Blass Cryptocurrency Letter notwithstanding, on March 13, 2019, Cipher Technologies Management LP filed a registration statement on Form N-2 to register shares of a closed-end "interval" fund called the Cipher Technologies Bitcoin Fund.[34] This fund would provide total returns available to direct investors in Bitcoin, less operating expenses. The fund would invest substantially all of its assets in a portfolio of Bitcoin or futures contracts or other derivatives providing similar economic exposure, as well as certain liquid securities to satisfy certain requirements of Rule 23c-3 under the 1940 Act (the "interval fund rule"), which requires interval funds to buy back a certain number of their shares at certain periods, or intervals (e.g., quarterly or semi-annually).

In a letter dated May 28, 2019, the staff of the Division of Investment Management asked the sponsor to withdraw the registration statement, because, among other things, "it is unclear whether the proposed fund would meet the definition of an investment company," and therefore whether the fund can be registered under the 1940 Act. The staff asked the fund to provide an analysis of whether and how it would meet the definition of an investment company.[35]

In a letter dated June 14, 2019, the sponsor of the fund asserted that Bitcoin is a security for purposes of the Securities Act of 1933, the Securities Exchange Act of 1934, and yes, 1940 Act. Under the traditional *Howey* definition of a security, the sponsor argued, Bitcoin is a security because, for purposes of this fund, it consists of (i) an investment of money, (ii) in a common enterprise, (iii) with profits, (iv) to come solely from the efforts of others.[36]

The sponsor rejected that the argument articulated by William Hinman, Director of the SEC's Division of Corporation Finance, in June 2018, that certain digital asset transactions do not represent securities offerings when "the network on which the token or coin is to function is sufficiently decentralized…." That is, Hinman said, there may be no investment contract when "purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts."[37]

Moreover, the sponsor of the fund asserted, it is irrelevant whether Bitcoin is a commodity, and by extension, it is irrelevant if the fund must register as a commodity pool operator. The sponsor concluded by stating that it respectfully declines the staff's request that it withdraw its registration statement.

The debate over whether cryptocurrencies are securities for purposes of the federal securities laws is far from over, and in fact may have only just begun. Our summary of the Cipher Technologies registration statement highlights the challenges facing the industry and its regulators as RIAs and registered investment companies begin to invest in digital currencies.

To be sure, however, the current environment of persistent uncertainty cannot last; as the markets for cryptocurrencies and other digital assets mature, so too will custody standards. Custodians, auditors and other trusted parties that comprise the infrastructure for reliable custody in the securities markets will develop a battery of tailored policies, procedures and practices appropriate to this new and growing asset class, reasonably designed to minimize the potential of loss and maximise the protection of client assets.

* * *

Acknowledgments

The author gratefully acknowledges the contributions and insights provided by Nathan J. Greene, Partner, and Andrew J. Donohue, Of Counsel, of Shearman & Sterling LLP.

* * *

Endnotes

1. Broker-dealers, commodity pool operators, commodity trading advisors and advisers to certain retirement plans are subject to separate requirements, which are not the subject of this chapter.
2. For a general discussion of steps that the SEC could consider to address custody of digital assets, see Jay Baris, *SEC Must Solve Its Cryptocurrency Conundrum*, Fin. Times (May 2, 2019), https://www.ft.com/content/6411aaff-dd80-382f-ab1c-80cae225673d.
3. Investment Advisers Act of 1940, 15 U.S.C. §§ 80b–1–80b–21 (1940).
4. Investment Company Act of 1940, 15 U.S.C. §§ 80a–1–80a–64 (1940).
5. For a general discussion of blockchain issues for investment managers, see Jay G. Baris & Joshua Ashley Klayman, *Blockchain Basics for Investment Managers: A Token of Appreciation*, 51 Rev. Sec. & Commodities Reg. 67 (2018), https://www.shearman.com/-/media/Files/Perspectives/2018/03/Blockchain_Basics_for_Investment_Managers_Token_of_Appreciation_March_23_2018_101818.PDF?la=en&hash=A91839D14053E8D16F2136A0BEF71D09DB9654D4.

6. William Hinman, Director, SEC Div. of Corp. Fin., Remarks at the Yahoo Finance All Markets Summit: Crypto, Digital Asset Transactions: When Howey Met Gary (Plastic) (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.
7. The Advisers Act does not specifically address custody of client assets. Rather, the SEC addressed this issue in the Rule 206(4)-2 under the Advisers Act (the "custody rule"). 17 C.F.R. § 275.206(4)-2 (2010).
8. H.R. Rep. No. 76-2639 (1940).
9. S. Rep. No. 76-1744 (1940).
10. SEC, The Securities and Exchange Commission Post-Madoff Reforms (2009), https://www.sec.gov/spotlight/secpostmadoffreforms.htm.
11. Investment Advisers Act Rule 206(4)-2, 17 C.F.R. § 275.206(4)-2 (2010).
12. The SEC staff has taken the position that if an adviser manages client assets that are not funds or securities, the custody rule does not require the adviser to maintain the assets with a qualified custodian. SEC Div. Of Inv. Mgmt., Staff Responses to Questions About the Custody Rule (2010), Question II.3, https://www.sec.gov/divisions/investment/custody_faq_030510.htm. The issue now presented is whether the SEC staff considers cryptocurrencies to be "funds or securities" for purposes of the custody rule.
13. For example, family offices, banks, insurance companies and broker-dealers that provide advice incidental to their brokerage business, among others, are excluded from the definition of an investment adviser under the Advisers Act.
14. We are assuming that at least these two cryptocurrencies are not "securities" for purposes of the federal securities laws. *See, e.g.*, Commodity Futures Trading Comm'n v. McDonnell, 287 F. Supp. 3d 213, 228 (E.D.N.Y. 2018) ("Virtual currencies can be regulated by CFTC as a commodity."), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf. In an April 26, 2018 testimony before the House Appropriations Committee, SEC Chair Jay Clayton confirmed this view. *Testimony before the Financial Services and General Government Subcommittee of the House Committee on Appropriations*, 115th Cong. (2018) (statement of Jay Clayton, Chairman, U.S. Securities and Exchange Commission) ("A pure medium of exchange, the one that's most often cited, is – is Bitcoin. As a replacement for currency, that is – has been determined by most people not to be a security."). We are aware of at least one public filing that challenges this notion.
15. We are aware of at least one public filing asserting that Bitcoin is a security for purposes of the Securities Act of 1933, the Securities Exchange Act of 1934 and Investment Company Act of 1940, challenging "conventional wisdom" and the sparse amount of legal precedent available. *See* Letter from Jacob E. Comer, Head of Regulatory and Compliance, Cipher Technologies Management LP, to Brent J. Fields, Assoc. Dir. of Disclosure Review and Accounting, Division of Investment Management (June 14, 2019), https://www.sec.gov/Archives/edgar/data/1776589/000114420419030981/filename1.htm. If the SEC accepts this argument, which is far from certain, the debate about custody of digital assets could change dramatically. The analysis of whether a particular digital asset is a security, in general or for purposes of custody requirements, is beyond the scope of this chapter and we save that debate for another day.

16. The provisions of the Advisers Act relating to whether an adviser is required to register are beyond the scope of this chapter.
17. Investment Advisers Act Rule 206(4)-2(d)(2), 17 C.F.R. § 275.206(4)-2(d)(2).
18. SEC Div. of Inv. Mgmt., Guidance Update No. 2017-01, Inadvertent Custody: Advisory Contract Versus Custodial Contract Authority (2017), https://www.sec.gov/investment/im-guidance-2017-01.pdf.
19. One notable exemption is that Rule 206(4)-2 does not apply with respect to mutual fund accounts of the RIA. *See* Rule 206(4)-2(b)(5), 17 C.F.R. § 275.206(4)-2(b)(5).
20. Investment Advisers Act Rule 206(4)-2(d)(6), 17 C.F.R. § 275.206(4)-2(d)(6).
21. Investment Advisers Act Rule 206(4)-2(a)(2), 17 C.F.R. § 275.206(4)-2(a)(2).
22. Investment Advisers Act Rule 206(4)-2(a)(5), 17 C.F.R. § 275.206(4)-2(a)(5).
23. Investment Advisers Act Rule 206(4)-2(a)(4)(iii), 17 C.F.R. § 275.206(4)-2(a)(4)(iii).
24. Investment Advisers Act Rule 206(4)-2(a)(6), 17 C.F.R. § 275.206(4)-2(a)(6).
25. Investment Advisers Act Rule 204-2(a)(17)(iii), 17 C.F.R. § 275.204-2(a)(17)(iii).
26. Exemptions for Advisers to Venture Capital Funds, Private Fund Advisers With Less Than $150 Million in Assets Under Management, and Foreign Private Advisers, Advisers Act Release No. IA-3222, 76 Fed. Reg. 39,645, 127 n.515 (June 22, 2011) ("[W]e do not apply most of the substantive provisions of the Advisers Act to the non-U.S. clients of a non-U.S. adviser registered with the Commission."), https://www.sec.gov/rules/final/2011/ia-3222.pdf. *See also* Robert E. Plaze, *Regulation of Investment Advisers by the U.S. Securities and Exchange Commission*, 67 n.374 (June 2018), https://www.proskauer.com/report/regulation-of-investment-advisers-by-the-us-securities-and-exchange-commission-june-2018.
27. Investment Company Act of 1940, 15 U.S.C. § 80a–17 (1958).
28. *See generally* Custody of Investment Company Assets with a Securities Depository, Investment Company Act Release No. IC-25934, 68 Fed. Reg. 8,437 (Feb. 13, 2003), https://www.sec.gov/rules/final/ic-25934.htm.
29. Custody of Investment Company Assets with Futures Commission Merchants and Commodity Clearing Organizations, Investment Company Act Release No. IC-22389, 61 Fed. Reg. 66,207 (Dec. 11, 1996), https://www.sec.gov/rules/final/ic-22389.txt.
30. In a joint statement dated July 8, 2019, the Division of Trading and Markets of the SEC and the Office of General Counsel of the Financial Industry Regulatory Authority summarized the challenges that broker-dealers face when broker-dealers take custody of digital assets for their customers. Although the joint statement applies to broker-dealers, the basic principles and challenges involving custody of digital assets apply equally to investment advisers. SEC Div. of Trading & Mkt. & Office of Gen. Counsel, Fin. Indus. Regulatory Auth., *Joint Statement on Broker-Dealer Custody of Digital Asset Securities* (July 8, 2019) (the "Joint Statement"), https://www.sec. gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.
31. *Joint Statement, supra* note 30.
32. For a discussion about digital asset-related exchange-traded products (ETPs), including exchange-traded funds (EFTs), see Baris & Klayman, *In Pursuit of Perfection? A Primer of Ditigal Asset-Related ETPs,* Blockchain and Virtual

Currencies Briefing, Issue No. 1, June 2019, https://www.shearman.com/-/media/Files/Perspectives/2019/06/Blockchain_06-11-2019_final.pdf?la=en &hash=683AA5F567DAB86DFFB6BDA15E17FFB33B73C204.

33. Investment Company Institute & Securities Industry and Financial Markets Association, SEC Staff Letter, *Engaging on Fund Innovation and Cryptocurrency-Related Holdings* (Jan. 18, 2018), https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm (the "Blass Cryptocurrency Letter").
34. Cipher Technologies Bitcoin Fund, Registration Statement (Form N-2) (May 13, 2019), https://www.sec.gov/Archives/edgar/data/1776589/000114420419025611/tv521304_n2.htm.
35. Letter from Brent J. Fields, Assoc. Dir. of Disclosure Review and Accounting, Division of Investment Management, to Jacob E. Comer, Head of Regulatory and Compliance, Cipher Technologies Management LP (May 28, 2019), https://www.sec.gov/Archives/edgar/data/1776589/999999999719005113/filename1.pdf.
36. Letter from Jacob E. Comer, Head of Regulatory and Compliance, Cipher Technologies Management LP, to Brent J. Fields, Assoc. Dir. of Disclosure Review and Accounting, Division of Investment Management (June 14, 2019), https://www.sec.gov/Archives/edgar/data/1776589/000114420419030981/filename1.htm.
37. Hinman, *supra* note 6.

Jay G. Baris
Tel: +1 212 848 4000 / Email: jay.baris@shearman.com

Jay G. Baris is a partner in the Investment Funds practice and has practiced in the asset management area for more than 35 years.

Jay is widely recognised for his breadth of experience representing registered funds, investment advisers, financial institutions, broker-dealers and independent directors on the full spectrum of financial services regulation, transactions and governance matters. Jay's work with registered funds spans mutual funds, closed-end funds, exchange-traded funds (ETFs) and business development companies (BDCs). He has extensive experience advising on the regulatory aspects of fund and investment advisory operations, and has represented numerous clients on mergers and acquisitions, reorganisations, compliance, exemptive applications and compliance issues. He also advises operating companies on "status" issues that arise under the Investment Company Act of 1940. More recently, he has been advising Fintech clients on cryptocurrency issues.

An active speaker and writer on issues concerning investment management and the regulation of financial institutions, Jay has been published in a variety of trade and general interest publications, *Insights: The Corporate & Securities Law Advisor*, *The New York Times*, *The Wall Street Journal*, *The Review of Securities & Commodities Regulation*, *Fund Action*, *The Review of Banking & Financial Services*, *Fund Directions* and *Fund Board Views*.

Educated at Hofstra University, J.D. and Stony Brook University, B.A., Jay is admitted to the Bars of New York, District of Columbia and New Jersey.

- Chair of the ABA Task Force on Blockchains, Cryptocurrencies and Investment Management of the ABA Subcommittee on Investment Companies and Investment Advisers.
- Co-Chair of the Task Force on Investment Company Use of Derivatives and Leverage of the Committee on Federal Regulation of Securities of the ABA's Business Law Section.
- Previously, vice chair of the Committee on Federal Regulation and chair and vice chair of the Subcommittee on Investment Companies and Investment Advisers of the ABA's Business Law Section.
- Member of the Advisor Panel of Blockchain, Virtual Currencies and ICOs – Navigating the Legal Landscape (Wolters Kluwer 2018).
- Member of the Board of Advisors of The Review of Securities & Commodities Regulation.
- Member of the Advisory Board of the Mutual Fund Directors Forum.
- Member of the Advisory Board of BoardIQ.
- Ranked in "Band 2" in *Chambers USA 2018* for Nationwide: Investment Funds: Registered Funds.
- Recognised as a "Leading Lawyer" and "Hall of Fame" by *The Legal 500* US (2018).
- Listed in *Best Lawyers in America* for his work in corporate law, mutual funds law and financial services regulation law (2008–2019).

Shearman & Sterling LLP

599 Lexington Avenue, New York, NY 10022, USA
Tel: +1 212 848 4000 / URL: www.shearman.com

Cryptocurrency and other digital assets for asset managers

Gregory S. Rowland & Trevor I. Kiviat
Davis Polk & Wardwell LLP

Introduction

In 2008, an unknown author publishing under the name Satoshi Nakamoto released a white paper describing Bitcoin, a peer-to-peer version of electronic cash, and the corresponding software that facilitates online payments directly between counterparties without the need for a financial intermediary. In the decade that has followed, Bitcoin and countless other open-source, decentralised protocols inspired by Bitcoin (for example, Ethereum and Monero) have come to represent a $270 billion-plus market of alternative assets, commonly referred to as "digital assets", which are typically traded over the internet using online exchange platforms.

Digital assets can serve several functions. Although the following categories are not independent legal categories under U.S. law, such distinctions are helpful for understanding and crafting various investment strategies involving these assets. Some digital assets, such as Bitcoin or Litecoin, are widely regarded as decentralised stores of value or mediums of exchange due to certain common economic features that support these functions; these are sometimes referred to as "pure cryptocurrencies". Other digital assets, such as Monero or Zcash, are a subset of pure cryptocurrencies that also possess certain features designed to enhance transaction privacy and confidentiality ("**privacy-focused coins**").

Beyond pure cryptocurrencies and privacy-focused coins, there exists a broad array of general purpose digital assets ("**platform coins**"), such as Ethereum, NEO and Ravencoin, which are designed to facilitate various peer-to-peer activity, from decentralised software applications to "smart" contracts to digital collectibles, such as CryptoKitties. Platform coins also enable the creation of new digital assets called "tokens", which are typically developed for a specific purpose or application – for example, (1) "utility tokens", which generally are designed to have some consumptive utility within a broader platform or service, or (2) "security tokens". The latter are designed to represent more traditional interests like equity, debt and real estate with the added benefit of certain features of the digital asset markets, such as increased liquidity, more cost-effective fractional interest transfers, more efficient cross-border trading, faster and more transparent payment of dividends and other distributions and rapid settlement.

The digital asset market extends beyond the assets themselves. Other participants, including online exchanges, payment processors and mining companies, compose the broader digital asset industry. And as this industry continues to grow, it has captured the attention of retail and institutional investors alike, including asset managers seeking to develop investment strategies and products involving these emerging assets and companies. Some strategies resemble early-stage growth strategies, featuring long-term investments either directly in

certain digital assets or in start-up ventures developing complementary goods and services for the industry. Other strategies include hedge fund strategies, such as long/short funds, which often use derivatives, or arbitrage strategies, which seek to capitalise on the price fragmentation across the hundreds of global online exchanges. Additionally, a recent downturn in the cryptocurrency markets compelled many fund managers to adopt new revenue-generation strategies, such as staking cryptocurrencies,[1] adopting credit-fund type strategies (e.g., distressed debt), engaging in market-making and executing venture capital investments, in order to survive the "crypto winter".[2]

This chapter outlines the current U.S. regulatory framework applicable to cryptocurrency and other digital asset investment funds ("**digital asset funds**") offered to U.S. investors and how those regulatory considerations affect fund structuring decisions.

The U.S. regulatory framework generally

Digital asset funds operated in the United States or offered to U.S. investors must contend and comply with a complex array of statutes and regulations. These include the Securities Act of 1933 (the "**Securities Act**"), which regulates the offer and sale of securities; the Investment Company Act of 1940 (the "**1940 Act**"), which regulates pooled investment vehicles that invest in securities; the Commodity Exchange Act (the "**CEA**"), which regulates funds and advisers that trade in futures contracts, options on futures contracts, commodity options and swaps; and the Investment Advisers Act of 1940 (the "**Advisers Act**"), which governs investment advisers to such funds. Additionally, many fund-structuring decisions are driven by tax considerations. This section sets out the current U.S. regulatory framework applicable to digital asset funds managed in the United States or offered to U.S. investors and explores how those regulatory considerations affect fund structuring decisions.

Offering of fund interests

Interests in investment funds are securities. Under the Securities Act, an offering of securities must be registered with the SEC or made pursuant to an exemption. While there are a few possible exemptions, the most common exemption that private funds rely upon is Regulation D, which provides two alternative exemptions from registration: Rule 504 and Rule 506. Because most private investment funds intend to raise more than $5 million, Rule 506, which provides no limit on the amount of securities that may be sold or offered, is the exemption under Regulation D most commonly relied on by such funds, and consequently, this discussion of Regulation D is limited to offerings made under Rule 506.[3] In order to offer or sell securities in reliance on Rule 506 of Regulation D, an investment fund must:

- limit sales of its securities to no more than 35 non-accredited investors (unless the offering is made pursuant to Rule 506(c), in which case all purchasers must be accredited investors), although securities may be sold to an unlimited number of accredited investors;
- ensure that all non-accredited investors meet a sophistication requirement by having such knowledge and experience in financial and business matters that they are capable of evaluating the merits and risks of the prospective investment;
- refrain from general solicitation or advertising in offering or selling securities (unless the offering is made pursuant to Rule 506(c));
- comply with the information disclosure requirements of Rule 502(b) with respect to any offering to non-accredited investors. There are no specific information requirements for offerings to accredited investors;

- implement offering restrictions to prevent resales of any securities sold in reliance on Regulation D; and
- file a Form D notice of the offering with the SEC within 15 calendar days of the first sale of securities pursuant to Regulation D.

There are also some important limitations on the scope of the Regulation D exemption. For example, Regulation D only exempts the initial transaction itself (i.e., resales of securities acquired in an offering made pursuant to Regulation D must be either registered or resold pursuant to another exemption from registration). Furthermore, Regulation D is not available for any transaction or series of transactions that, while in technical compliance with Regulation D, is deemed to be part of "a plan or scheme to evade the registration provisions of the [Securities] Act".

The regulatory treatment of cryptocurrencies and other digital assets

As discussed above, interests in investment funds themselves are securities; however, these funds may hold a variety of different assets in pursuing their respective strategies – from digital assets (e.g., Bitcoin and Ether) to derivatives instruments (e.g., Bitcoin futures contracts) to securities (e.g., equity in an emerging growth company or interests in another digital asset investment fund). This section provides an overview of the regulatory treatment of such assets, particularly with respect to the definitions of "securities" under the U.S. securities laws and "commodity interests" under the CEA, before explaining how these characterisations impact structuring decisions. Although some generalisations may be inferred about the possible treatment of certain assets based on common features and fact patterns, there is no substitute for a careful case-by-case analysis of each asset, in close consultation with counsel.

In July 2017, in a release commonly referred to the DAO Report,[4] the SEC determined that certain digital assets are securities for purposes of the U.S. federal securities laws. The DAO Report was published in response to a 2016 incident in which promoters of an unincorporated virtual organisation ("**The DAO**") commenced an initial coin offering (an "**ICO**"), a term that generally refers to a sale of tokens to investors in order to fund the development of the platform or network in which such tokens will be used. The DAO was created by a German company called Slock.it, and it was designed to allow holders of DAO tokens to vote on projects that The DAO would fund, with any profits flowing to token-holders. Slock.it marketed The DAO as the first instance of a decentralised autonomous organisation, powered by smart contracts on a blockchain platform. The DAO's ICO raised approximately $150 million (USD) in Ether.

In the DAO Report, the SEC reasoned that The DAO tokens were unregistered securities because they were investment contracts, which is one type of security under the U.S. securities laws. Though it declined to take enforcement action against The DAO, the SEC used this opportunity to warn others engaged in similar ICO activities that an unregistered sale of digital assets can, depending on the facts and circumstances, be an illegal public offering of securities. The SEC has relied on similar reasoning in subsequent actions taken against token issuers that deem certain other digital assets sold in ICOs to be securities (such securities, "**DAO-style tokens**").[5] Many DAO-style tokens are branded by their promoters as utility tokens to convey the idea that such tokens are designed to have some consumptive utility within a broader platform or service. But as noted above, this terminology does not have any legal consequence under the U.S. securities laws. Instead, a proper inquiry must examine the facts and circumstances surrounding the asset's offering and sale, including the economic realities of the transaction.[6] Key factors to consider include: (1) whether a third party – be it a person, entity or coordinated group of actors – drives the expectation of a return; and (2)

whether the digital asset, through contractual or other technical means, functions more like a consumer item and less like a security.[7] Additionally, in April 2019, the SEC staff published new detailed guidance on when a digital asset may be considered a security, in the form of two documents: a framework issued by the SEC's Strategic Hub for Innovation and Financial Technology along with a no-action letter from the SEC's Division of Corporation Finance. The framework reaffirms the staff's position that digital assets sold to investors to raise capital are generally securities, regardless of potential utility, and charts a narrow path for the sorts of digital assets that the staff would not consider a security. Meanwhile, the no-action relief is narrow and unlikely to provide meaningful guidance or practical utility for many types of currently available digital assets or firms considering issuing digital assets.[8]

In addition to DAO-style tokens, some digital assets are explicitly designed to be treated as securities from the outset and are meant to represent traditional interests like equity and debt, with the added benefit of certain features of the digital asset markets, such as 24/7 operations, fractional ownership and rapid settlement. These digital assets are securities by definition, and although they represent an innovation in terms of how securities trade, clear and settle, they are not necessarily a new asset class.

Any cryptocurrencies or other digital assets that are not deemed to be securities under the U.S. securities laws may be considered "commodities" under the CEA, due to the broad definition of the term.[9] For example, the Commodity Futures Trading Commission ("**CFTC**") appears to be treating Bitcoin as an exempt commodity under the CEA, a category that includes metals and energy products,[10] but does not include currencies or securities, which are classified as excluded commodities.[11] In addition, the CFTC recently permitted the self-certification of futures contracts and binary options on Bitcoin by futures exchanges under its rules for listing ordinary futures contracts.[12] And although the SEC has not taken any action with respect to Bitcoin specifically, SEC Chairman Jay Clayton recently acknowledged, and appeared to accept as correct, the CFTC's designation of Bitcoin as a commodity over which the CFTC has anti-fraud jurisdiction.[13] Finally, to the extent that a digital asset is a commodity, any derivatives offered on that commodity – for example, Bitcoin futures contracts and binary options – fall squarely within the definition of commodity interests under the CEA.

Possible obligations of the manager under the Advisers Act or the CEA

The question of whether a digital asset fund manager must comply with additional regulations under either, or both of, the Advisers Act and the CEA turns primarily on the characterisation of the assets its funds hold. First, a manager is deemed an "investment adviser" under Section 202(a)(11) of the Advisers Act, and thus is subject to the rules and regulations thereunder, if it "for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing in, purchasing, or selling securities", or "for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities". So to the extent that a manager of a cryptocurrency or other digital asset fund is advising on "securities" – for example, because its funds hold DAO-style tokens or security tokens – it must register as an investment advisor with the SEC unless such individual or entity qualifies for an exclusion from the definition or an exemption from the registration requirement.[14]

Registration under the Advisers Act subjects advisers to a host of rules and regulations, including those governing advertising, custody, proxy voting, record-keeping, the content of advisory contracts and fees. For example, the Advisers Act custody rule[15] (the "**custody rule**") has detailed provisions applicable to any SEC-registered investment adviser deemed

to have custody, as defined under the rule. Among other things, it requires use of a "qualified custodian" to hold client funds or securities, notices to clients detailing how their assets are being held, account statements for clients detailing their holdings, annual surprise examinations and additional protections when a related qualified custodian is used. For example, investment advisers dealing in digital assets may need to consider whether a bank, registered broker-dealer, or other firm that meets the definition of a qualified custodian, is willing to take custody of the digital assets.

Second, managers of private funds that invest or trade in "commodity interests", whether as an integral part of their investment strategy or only in a limited capacity, for hedging purposes or otherwise, are subject to regulation under the CEA and the rules of the CFTC thereunder ("**CFTC Rules**"). Commodity interests generally include: (1) futures contracts and options on futures contracts; (2) swaps; (3) certain retail foreign currency and commodity transactions; and (4) commodity options and certain leveraged transactions. So to the extent that the activities of a manager of a cryptocurrency or other digital asset fund include trading in commodity interests – for example, because it holds Bitcoin futures contracts or binary options – it will be subject to registration and regulation as a commodity pool operator ("**CPO**") or commodity trading advisor ("**CTA**"), unless it qualifies for an exemption or exclusion under the CEA or the CFTC Rules.

If the activities of an investment fund bring it within the definition of a "commodity pool" under the CEA, the manager is required to register as a CPO with the CFTC, unless such person otherwise qualifies for an exclusion from the definition of CPO or an exemption from the registration requirement. The CEA also provides for the registration of CTAs, which is in some respects analogous to the treatment of investment advisers under the Advisers Act. It should be noted, however, that numerous requirements under the CEA and the CFTC Rules apply to all CPOs and CTAs, even those that are exempt from registration.

Possible obligations of the fund under the 1940 Act or CEA

Similarly, the fund itself may be subject to additional regulations under either, or both of, the 1940 Act and the CEA, an analysis that, again, turns primarily on the assets the fund holds. An investment company is defined under Section 3(a)(1)(A) of the 1940 Act as any issuer that "is or holds itself out as being engaged primarily, or proposes to engage primarily, in the business of investing, reinvesting or trading in securities". This subjective test is based generally on how a company holds itself out to the public and the manner in which it pursues its business goals, and is designed to capture traditional investment companies that are deliberately acting in that capacity. Additionally, Section 3(a)(1)(C) of the 1940 Act sets forth an objective, numerical test that applies to companies that hold a significant portion of their assets in investment securities, even if they do not hold themselves out as traditional investment companies.

Companies that fall within one of these definitions of an investment company must either satisfy an exemption from the 1940 Act or register under it. The 1940 Act is a comprehensive statutory regime that imposes strict requirements on registered investment companies' governance, leverage, capital structure and operations. Consequently, most private equity funds, hedge funds and other alternative investment vehicles, which fall squarely within the definition of "investment company", are structured to satisfy an exemption from the 1940 Act.

The 1940 Act provides specific exemptions from the definition of "investment company" for privately offered investment funds and certain other types of companies. For example, Section 3(c)(1) exempts a private investment fund from registration if the outstanding

securities of such fund (other than short-term paper) are beneficially owned by not more than 100 persons and such fund does not presently propose to make a public offering of its securities. Further, Section 3(c)(7) excludes an entity from registration as an investment company if all of the beneficial owners of its outstanding securities are "qualified purchasers" and the entity does not make or propose to make a public offering of its securities, and it does not limit the number of beneficial owners.

The CEA defines "commodity pool" as any investment trust, syndicate or similar form of enterprise operated for the purpose of trading in commodity interests. The CFTC interprets "for the purpose" broadly and has rejected suggestions that trading commodity interests must be a vehicle's principal or primary purpose. As a result, any trading by a private fund in swaps, futures contracts or other commodity interests, no matter how limited in scope, and regardless of whether undertaken for hedging or speculative purposes, generally will bring a private fund within the commodity pool definition.

According to the CFTC, a fund that does not trade commodity interests directly but invests in another fund that trades commodity interests would itself be a commodity pool. Thus, in a master-feeder fund structure, a feeder fund will be considered a commodity pool if the master fund is a commodity pool. Similarly, a fund of funds that invests in commodity pools may itself be considered a commodity pool.

Finally, an investment vehicle can be both an "investment company" under the 1940 Act and a "commodity pool" under the CEA, and an exception from the registration requirements of the 1940 Act does not generally imply an exception from CPO registration under the Commodity Exchange Act (or vice versa). Similarly, an exception from registration under the Advisers Act does not generally imply an exception from CTA registration (or vice versa). Furthermore, interests in commodity pools are "securities" under the Securities Act, and therefore the Securities Act applies to the offer and sale of interests in a commodity pool to the same extent as it applies to any other type of security. Accordingly, offering of interests in a private fund that is a commodity pool generally will be structured to meet the requirements of a Securities Act exemption (e.g., Regulation D, as discussed above).

Applying this framework to digital asset funds

Given the regulatory minefield laid out above, managers face a multitude of structuring decisions in conceiving and launching digital asset funds aimed at U.S. investors. These decisions will often influence, and be influenced by, the manager's investment strategy – particularly as it relates to the types of assets the fund should be permitted to hold. This section explores some common structures and the strategies they support. In each of these cases, one should keep in mind that interests in the digital asset fund itself are securities, as noted above, that must be offered and sold pursuant to an exemption, such as Regulation D, except in the case of registered (i.e., public) funds, which are offered and sold in fully registered securities offerings.

First, the manager may decide that the fund should have flexibility to invest in securities. It may want to invest in "traditional" securities like equity or debt in a company within the digital asset industry (including through tokenised securities), or DAO-style tokens and other digital assets at risk of being deemed investment contracts. In this case, the adviser will likely need to register under the Advisers Act and comply with the host of rules and regulations thereunder, including those governing advertising, custody, proxy voting, record-keeping, the content of advisory contracts, and fees. Non-U.S. advisers, however, can potentially rely on Advisers Act Rule 203(m)-1 (the "**private fund adviser rule**").[16]

Custody poses unique questions in the digital asset context, and it is not clear in all cases whether digital assets would be viewed as funds or securities, such that the custody rule would apply. Currently, most qualified custodians do not offer custody services for digital assets. In any case, the manager should familiarise itself with the operational considerations of digital asset custody. First, what does it mean to have custody of an asset that is not physical and even in digital form, does not exist on a centralised database, but instead on one that is universal and distributed? For example, one cannot physically move units of Bitcoin off of the Bitcoin blockchain and store them elsewhere. However, in order to exercise control over one's Bitcoins, one needs a private and a public key. These keys are a series of hexadecimal characters (e.g., 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa), which must be stored carefully. The public key is the identity of the address on the network that has ownership and control of those Bitcoins – this key can be shared with anyone, and in fact, it must be shared in order to receive Bitcoins. The private key is essentially a password, and Bitcoins can be transferred out of a particular address by anyone with possession of that address's corresponding private key. So in the case of a blockchain-based asset like Bitcoin, control of the private key may be tantamount to custody. As there is simply no recourse to retrieve Bitcoins when a private key is lost or stolen, a critical operational point for managers is safe and secure private key storage; for example, through "deep cold" storage.[17]

If the manager believes the digital asset fund may invest in securities, the fund itself would likely be structured so as to meet one of the various registration exemptions for entities that would otherwise be classified as "investment companies" under the 1940 Act.[18] For offshore funds, the requirements of Sections 3(c)(1) and 3(c)(7), which are discussed above, generally only apply to U.S. investors.

Alternatively, the manager may consider structuring the fund as a registered investment company, although as of the date of this article, the SEC has not approved any such funds. As the authors discuss in "The Current State of U.S. Public Cryptocurrency Funds", there have been a number of requests to list on national securities exchanges the shares of such funds.[19] The SEC has repeatedly denied such requests, and in January 2018, the SEC's Division of Investment Management outlined several questions that sponsors would be expected to address before it would consider granting approval for funds holding "substantial amounts" of cryptocurrencies or "cryptocurrency-related products".[20] The questions, which focus on specific requirements of the 1940 Act, generally fall into one of five key areas: valuation; liquidity; custody; arbitrage; and potential manipulation. And although such funds alternatively could potentially be offered to the public as non-investment companies (to the extent they do not hold significant amounts of securities) under the Securities Act, the SEC has indicated that significant, similar questions exist there also.[21]

Second, the manager may decide that the fund should have flexibility to invest in commodity interests, such as futures contracts or binary options, either for hedging or speculative purposes. Any such trading by a private fund, no matter how limited in scope, and regardless of the purpose, would generally make such fund a "commodity pool", as discussed above. In this case, the manager may be required to register as a CPO or CTA with the CFTC, although certain exemptions exist for non-U.S. managers and for funds that invest in only limited amounts of commodity interests. Even if the manager decides that such fund should only invest in commodity interests and not securities, interests in commodity pools are "securities" under the Securities Act, and therefore, the fund would generally be structured to meet the requirements of a Securities Act exemption (e.g., Regulation D, as discussed above).

Finally, the manager may decide that the fund should hold neither securities nor commodity interests – in other words, a fund that holds only commodities, or "pure cryptocurrencies", such as Bitcoin, and no commodity interests. Because this category does not have independent legal significance under U.S. law, such determinations regarding the risk that a given digital asset could be deemed a "security" for U.S. securities laws purposes should be made carefully and together with legal counsel. In this case, the fund would not be governed by the 1940 Act, and the manager's activities with respect to the fund would not be governed by the Advisers Act, as both of these regimes are premised upon the fund holding securities, as discussed above. Further, because the fund does not hold commodities interests, it would likely not be considered a "commodity pool", and the manager would likely not be required to register as a CPO or CTA with the CFTC. However, the fund and the manager in this case would not be entirely unregulated. As noted above, interests in the fund are securities (regardless of the underlying assets that the fund invests in), the offer and sale of which must comply with U.S. securities laws. Additionally, the CFTC has some, albeit limited, jurisdiction over the spot market for commodities pursuant to its anti-fraud and manipulation authority.[22] Moreover, the manager of such a fund would likely be considered a common law fiduciary to such a fund and thus subject to fiduciary duties in its management of the fund.

While beyond the scope of this paper, many fund-structuring decisions are driven by U.S. federal income tax considerations. For example, many private investment fund structures typically consist of at least two investment vehicles: a vehicle that is organised in the United States and is treated as a partnership for U.S. federal income tax purposes (the "Onshore Fund"); and a vehicle that is organised in a tax haven jurisdiction, such as the Cayman Islands or the British Virgin Islands, and is treated as a corporation for U.S. federal income tax purposes (the "Offshore Fund"). U.S. taxable investors generally invest in the Onshore Fund. Because of the transparency of partnerships for U.S. federal income tax purposes, the U.S. investors are generally treated as if they directly derived their shares of the Onshore Fund's items of income, gains, losses, and deductions. The Offshore Fund is a passive foreign investment company ("PFIC"), for U.S. federal income tax purposes.

Conclusion

Over the past decade, digital assets have come a long way – from Satoshi's original Bitcoin white paper to today's broad universe of 2,200-plus digital assets trading across hundreds of online trading platforms. As this market and the surrounding industry matures, asset managers will likely continue to identify opportunities to either deploy novel investment strategies or adapt their tried-and-true strategies in this new context. As set out above, such managers face a complex array of statutes and regulations in offering digital asset funds to U.S. investors. These considerations, together with the investment strategies that the manager desires to pursue, affect fund structuring decisions, and accordingly, are best addressed together with counsel.

* * *

Endnotes

1. Frank Chaparro, Crypto hedge funds are getting creative as the bear market tightens its grip, The Block (2018), https://www.theblockcrypto.com/2018/12/04/crypto-hedge-funds-are-getting-creative-as-the-bear-market-continues-to-grip-crypto/ (last visited May 31, 2019).

2. Proof of Stake – Bitcoin Wiki, https://en.bitcoin.it/wiki/Proof_of_Stake (last visited Jun. 3, 2019) (staking involves users locking tokens in a wallet that is then used to secure the network, validate transactions and produce new blocks, thereby allowing users to earn a passive income return). These additional activities, such as market making, may raise additional U.S. regulatory issues that are beyond the scope of this article.
3. Historically, issuers and any persons acting on their behalf were prohibited from engaging in any form of general solicitation or general advertising in Rule 506 offerings. However, in July 2013, the SEC adopted final rules to permit general solicitation and general advertising in Rule 506 offerings under new Rule 506(c). Additional requirements apply to Rule 506(c) offerings, including the requirement to take reasonable steps to verify an investor's accredited investor status. Under Rule 506(b), an investment fund may offer securities pursuant to Rule 506 without complying with these additional requirements if it does not use general solicitation. Currently, most private funds offered in the United States choose not to use general solicitation.
4. SEC Release No. 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Jul. 25, 2017).
5. *See, e.g.*, SEC Release No. 10445, *In the matter of Munchee, Inc.* (Dec. 11, 2017).
6. This includes, for example, (1) whether the investor's fortunes are interwoven with those of other investors or the efforts of the promoter of the investment, and (2) whether the investor's expectation of profits are based predominantly upon the entrepreneurial or managerial efforts of the promoter or other third parties. *See SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).
7. Director William Hinman, Remarks at the Yahoo Finance All Markets Summit, *Asset Transactions: When Howey Met Gary (Plastic)* (Jun. 14, 2018), *available at* https://www.sec.gov/news/speech/speech-hinman-061418. Further, the speech indicates that a digital asset that was originally offered in a securities offering may later be sold in a manner that does not constitute an offering of a security, in limited circumstances, where: (i) there is no longer a central enterprise being invested in; and (ii) the asset is only being sold to end users who will purchase a good or service available through a network. This also raises a counterfactual question – that is, whether a token network that was once decentralised could "centralise", such that it would fall within the scope of the securities laws.
8. SEC, Staff Guidance: Framework for "Investment Contract" Analysis of Digital Assets (Apr. 3, 2019), available at https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets (the "**Framework**"). SEC, No-Action Letter: Response of the Division of Corporate Finance Re: TurnKey Jet, Inc. (Apr. 3, 2019), available at https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm (the "**No-Action Letter**").
9. *See* 7 U.S.C. § 1a(9).
10. *See* 7 U.S.C. § 1a(20) (defining exempt commodity to mean any commodity that is not an agricultural commodity or an excluded commodity; excluded commodity is defined in Section 1a(19) of the CEA to include any "interest rate, exchange rate, currency, security, security index" and other financial rates and assets).

11. *See In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015). In this order, the CFTC found that Coinflip's Bitcoin options were offered in violation of CFTC regulation 32.2, which governs commodity option transactions. The CFTC noted that the options "were not conducted pursuant to [CFTC] Regulation 32.3", the so-called "trade option exemption", which permits trading of commodity options on exempt and agricultural commodities, but not on excluded commodities such as securities, currencies, interest rates and financial indices. The CFTC, in describing why the trade option exemption was not available for Coinflip's options, focused on requirements under CFTC regulation that the options must be offered by eligible contract participants to commercial users of the underlying commodity, and not on the classification of Bitcoin as an excluded commodity.
12. *See* CFTC Release pr7654-17, CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange (Dec. 1, 2017). *See also* CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets (Jan. 4, 2018) (describing the CFTC's authority with respect to virtual currency and the "heightened review" employed during the Bitcoin futures self-certification process).
13. SEC Chairman Jay Clayton, Statement on Cryptocurrencies and Initial Coin Offerings, at n. 2 (Dec. 11, 2017) ("The CFTC has designated Bitcoin as a commodity. Fraud and manipulation involving Bitcoin traded in interstate commerce are appropriately within the purview of the CFTC, as is the regulation of commodity futures tied directly to [B]itcoin."); *see also* CNBC, *SEC Chief Says Agency Won't Change Securities Laws to Cater to Cryptocurrencies* (Jun. 6, 2018) ("'Cryptocurrencies: These are replacements for sovereign currencies, replace the dollar, the euro, the yen with [B]itcoin,' Clayton said. 'That type of currency is not a security.'").
14. Investment advisers not registered with the SEC may be subject to registration with U.S. states.
15. 17 U.S.C. § 206(4)-2.
16. For an adviser that has its principal office and place of business outside of the United States, an Advisers Act registration exemption is available under the private fund adviser rule, so long as: (i) the adviser has no client that is a U.S. person (generally as defined in Regulation S under the Securities Act) except for "qualifying private funds" (as defined in the rule); and (ii) all assets managed by the adviser at a place of business in the United States are solely attributable to private fund assets with a value of less than $150 million. Advisers relying on this exemption are still required to file certain information with the SEC.
17. Cold storage refers to the process of storing digital assets, such as bitcoins, offline (i.e., storing the private keys on a device not connected to the internet). However, the private keys associated with this process may have been exposed to the internet at some time during the generation of the signing process. Deep cold storage, however, is a type of cold storage where not only are the digital assets stored offline, but also the private keys associated with those assets are generated in offline systems, and the signing process of the transactions is also made in offline systems. The systems used in this type of storage never touch the internet; they are created offline, they are stored offline, and they are offline when signing transactions.
18. *See* 1940 Act § 3(c)(1)-(7).

19. Trevor Kiviat & Gregory Rowland, The Current State of U.S. Public Cryptocurrency Funds, International Comparative Legal Guide to Public Investment Funds (2019 ed.), https://iclg.com/practice-areas/public-investment-funds-laws-and-regulations/1-the-current-state-of-u-s-public-cryptocurrency-funds (last visited June 3, 2019).
20. SEC, Staff Letter: Engaging on Fund Innovation and Cryptocurrency-related Holdings (Jan. 18, 2018), available at https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm (the "**Letter**").
21. On March 23, 2018, the SEC issued an order instituting proceedings to determine whether it will approve a proposal by NYSE Arca to list two ProShares-sponsored Bitcoin futures-backed exchange-traded funds ("**ETFs**"). On April 5, 2018, the SEC published a second order instituting proceedings relating to a rule-change proposal by Cboe BZX Exchange, Inc. that would allow for the listing of two GraniteShares-sponsored ETFs that invest in Bitcoin futures contracts (both orders together, the "**Orders**"). The Orders ask for comments on many of the same issues raised in the Letter and institute a new period of review for such products, including a request for public comment on 12 areas of interest. These areas include concerns relating to: (1) such ETFs' investment practices; (2) the underlying spot and futures markets for Bitcoin; and (3) how such markets may in turn affect ETFs that invest in Bitcoin futures. For example, the SEC requests comments on the ETFs' valuation policies (e.g., how would such policies account for the possibility of a hard fork), including how such policies relate to the underlying Bitcoin spot markets, their potential for manipulation and what, if any, effect these factors could have on the ETFs' net asset value. On July 26, 2018, the SEC issued an order disapproving a rule-change proposal by Bats BZX Exchange, Inc. that would have allowed for the listing of the Winklevoss Bitcoin Trust.
22. *See* CFTC Rule 180.1.

Gregory S. Rowland
Tel: +1 212 450 4930 / Email: gregory.rowland@davispolk.com

Gregory S. Rowland is a partner in Davis Polk's Corporate Department, practising in the Investment Management Group. He focuses on providing transactional, regulatory and compliance advice relating to investment advisers, mutual funds, closed-end funds, business development companies, private equity funds and hedge funds. He devotes a large portion of his practice to the structuring, launch and operation of registered investment companies and hedge funds and to the sales, acquisitions and restructurings of asset management firms.

Mr Rowland advises financial institutions, technology companies and asset managers in connection with transactional, regulatory and compliance issues concerning digital currency and blockchain activities, including digital currency fund formation. In addition, he advises financial institutions, fund sponsors, corporations, employees' securities companies, and other entities regarding exemptions under the Investment Company Act and Investment Advisers Act.

Trevor I. Kiviat
Tel: +1 212 450 3448 / Email: trevor.kiviat@davispolk.com

Trevor I. Kiviat is an associate in Davis Polk's Investment Management Group. His practice focuses on advising clients on the formation and operation of private investment funds, including private equity funds and hedge funds. He also regularly provides regulatory and compliance advice to his private fund clients.

In addition, Mr Kiviat wrote the first widely read and cited academic paper distinguishing Bitcoin from blockchain technology. He advises clients on the novel strategic, operational and regulatory issues relating to digital currency-based businesses. He also has been cited in the media for his extensive knowledge of blockchain technology and has lectured on related topics at the International Monetary Fund and Duke University.

Davis Polk & Wardwell LLP

450 Lexington Avenue, New York, NY 10017, USA
Tel: +1 212 450 4000 / Fax: +1 212 701 5800 / URL: www.davispolk.com

The yellow brick road for consumer tokens: The path to SEC and CFTC compliance *An update*

David L. Concannon, Yvette D. Valdez & Stephen P. Wink
Latham & Watkins LLP

Developing a framework for consumer tokens

With the rapid growth in the development of blockchain technology, virtual currencies and token sales (sometimes referred to as initial coin offerings, or ICOs), token offerings came under increased regulatory scrutiny, particularly in the United States. Since the US Securities and Exchange Commission (the SEC) first started taking action with respect to token offerings, the question on the minds of many entrepreneurs and their counsel has been whether the issuance and sale of "consumer" or "utility" tokens – those designed for use by consumers on a distributed platform and not intended to constitute securities – is possible in the United States.[1] While there appears to be a viable regulatory path to the issuance of consumer tokens that would not necessarily be viewed as "securities" subject to SEC oversight, the framework remains unclear. In this chapter, we discuss the legal issues surrounding such issuances under the US federal commodities and securities laws.

This chapter serves as an update to the previous edition and reflects our most current and up-to-date thinking and analysis regarding the development of consumer token sales.

Existing frameworks

The securities law framework

The SEC's approach to whether a digital asset sold in a token sale would be a security derives from its application of the test set forth in *SEC v. W.J. Howey Co.* (the *Howey* Test).[2] The *Howey* Test determines whether an asset constitutes an "investment contract," one of the enumerated types of instruments defined in the securities laws.[3] The test states that an investment contract involves (i) an investment of money, (ii) in a common enterprise, (iii) in which the investor is led to expect profits, (iv) derived from the entrepreneurial or managerial efforts of one or more third parties.[4] If the test is satisfied, it is immaterial whether the enterprise is speculative or non-speculative, or whether there is a sale of property with or without intrinsic value.[5] In short, the heart of the analysis is to focus on the economic reality of the arrangement in question.

In July 2017, the SEC applied the *Howey* Test to digital assets for the first time, and arrived at the conclusion that the sale of Decentralized Autonomous Organization tokens (DAO tokens), a digital asset, was an unregistered securities offering undertaken without a valid

exemption from Section 5 of the Securities Act of 1933 (the Securities Act). The SEC made clear that to the extent instruments have the indicia of investment contracts, they should be offered and sold in compliance with the securities laws.

In its first enforcement action relating to the sale of digital assets, on December 11, 2017, the SEC issued an order instituting cease-and-desist proceedings to halt Munchee Inc.'s sale of tokens (the *Munchee* Order), having concluded the sale was an unregistered securities offering. A key lesson of the *Munchee* Order was that despite the utility design features of the MUN Tokens, the manner in which the digital assets were offered to prospective investors, and the presence of investment intent on the part of participating investors constituted material factors for the SEC in determining that the offering was a securities offering subject to the US federal securities laws.[6]

Following the *Munchee* Order, in a June 2018 speech, William Hinman, Director of the SEC's Division of Corporation Finance, emphasized that digital assets need not always be securities. Rather, in addition to the underlying rights associated with such assets, he reiterated that the manner of sale and the reasonable expectations of the purchasers help determine whether a particular digital asset is a security. This is underscored by Director Hinman's reference to *Gary Plastic Packaging v. Merrill Lynch, Pierce, Fenner, & Smith Inc.*,[7] in which the court found an offering of a certificate of deposit, which in and of itself is not a security, was subject to US federal securities laws because the issuer's marketing efforts centered on the establishment of a secondary market and the opportunity for purchasers to profit from the enterprise. In the case of nascent token platforms and networks, digital tokens sold in an offering by promoters to "develop the enterprise" will most often constitute securities because the value of the token will primarily derive from the entrepreneurial efforts of the enterprise's promoters. Nevertheless, Director Hinman noted that transactions involving digital assets on a sufficiently decentralized network do not otherwise have the indicia of securities transactions and do not give rise to the public policy concern of informational asymmetries between an investor and issuer, and thus may not trigger the application of US federal securities laws. Recently, Director Hinman reiterated these ideas in a May 2019 speech, stating that a potential pathway exists for a token that was once a security to transmute into a non-security.

In April 2019, the SEC staff issued a "Framework for 'Investment Contract' Analysis of Digital Assets" (the Framework) to assist market participants to assess whether a digital asset constitutes an investment contract. In addition, the SEC staff also released a no-action letter in response to a proposed token offering by TurnKey Jet, Inc. (Turnkey Jet), an air carrier and air taxi service (the Turnkey Letter). Together, the Turnkey Letter and Framework emphasize that the analysis of whether a digital asset constitutes an investment contract hinges on the third and fourth prongs of the *Howey* Test; in particular, whether the investors have an expectation of profits that will be derived from the managerial efforts of others. The Framework now serves as the principle source of guidance for analyzing whether a digital asset falls within the definition of a security.

To evaluate "reliance on the efforts of others," the Framework introduces the concept of an Active Participant (AP), defined as "a promoter, sponsor, or other third party … [that] provides essential managerial efforts that affect the success of the enterprise, and investors reasonably expect to derive profit from those efforts." Determining the existence of an AP necessarily requires an analysis of each party's role in developing, maintaining or governing the network. The presence of an AP means it is more likely that profits are being derived from the efforts of others.

To analyze "reasonable expectation of profit," the Framework bases its evaluation on whether an asset conveys the "right[] to share in [an] enterprise's income." This factor should be unsurprising to issuers, as it derives from the reasoning in the *DAO Report*, which pointed to the dividend-like feature of DAO tokens in classifying them as securities. Continuing in the vein of the SEC's prior pronouncements, the guidance also looks to how the digital asset is marketed, whether "the digital asset is offered broadly" (e.g. via secondary markets) "to potential purchasers as compared to being targeted to expected users of the goods or services or those who have a need for the functionality of the network," and whether "[t]he AP continues to expend funds from proceeds or operations to enhance the functionality or value of the network or digital asset." Such factors appear to focus on the more speculative aspects of issuances, such as where the use and value of the digital asset is connected to an undeveloped network, the success of which may likely be tied to the capital raised through the issuance itself. In addition, the Framework looks to whether the AP will receive or retain any of the digital assets, and the nature of purchasers' expectations with respect to the role of the AP and the ongoing viability of the digital asset itself.

In June 2019, the SEC sued Kik Interactive Inc. (Kik) for allegedly conducting an illegal US$100 million securities offering of Kik's digital token, Kin.[8] In its complaint, the SEC alleged that Kik marketed Kin to investors as an investment opportunity, offered and sold Kin before it had any utility, retained a proportion of the tokens for Kik and promised investors that Kin would be listed on secondary markets. For the SEC, such features meant the Kin offering was a securities transaction and should have complied with registration requirements as prescribed by the securities laws.[9] In a press release,[10] Kik responded to the SEC's suit, citing similar arguments as those raised in its Wells submission[11] in December 2018. Specifically, Kik argued that the SEC's complaint is based on "flawed legal theory" and expands the *Howey* test beyond its proscribed limits. In support of this position, Kik claimed that "the complaint assumes, incorrectly, that any discussion of a potential increase in value of an asset is the same as offering or promising profits solely from the efforts of another; that having aligned incentives is the same as creating a 'common enterprise'; and that any contributions by a seller or promoter are necessarily the ['']essential['] managerial or entrepreneurial efforts required to create an investment contract."[12] Of course, in addition to proving instructive, the resolution of this case and these issues could provide useful judicial precedent.

The commodities law framework

The US Commodity Futures Trading Commission (the CFTC) regulates the swaps (*i.e.*, the CFTC's term for derivatives) and futures markets and retains general enforcement authority to police fraud and manipulation in cash or "spot" commodities markets.[13] In 2014, then-CFTC Chairman Timothy Massad observed that what the CFTC has referred to as virtual currencies are "commodities" subject to provisions of the Commodity Exchange Act, as amended (the CEA).[14] Since 2015, the CFTC has been active in bringing enforcement actions when virtual currency enterprises run afoul of regulatory requirements[15] and in the enforcement against fraud and manipulation in the virtual currency "spot" markets.[16]

Pre-functional consumer token sales[17]

Sales of tokens to fund an AP's development of a token-based network have long been considered to constitute investment contracts, regardless of the form of instrument evidencing the sale. That is, the efforts of the AP remain central to the value of the instrument being sold, thus satisfying the *Howey* Test as an investment contract. As a result, in an effort

to separate the pre-functional sale and the underlying consumer token, new financing instruments – including the Simple Agreement for Future Tokens (the SAFT)[18] and other similar token presale instruments – were designed. While such instruments attempted to solve the securities law issues with presales, they raised significant other concerns.[19]

Securities law issues

Token presale instruments commonly fail to address the status of the underlying tokens and the impact of the presale offering on the marketing of the underlying tokens. That is, by marketing the token presale as an investment opportunity, these instruments were implicitly marketing the investment value of the underlying token. As a general matter, such instruments have been and continue to be marketed to purchasers with investment intent, such as hedge funds, venture capital funds and others, and, in at least some cases, purchasers are required to represent that they are purchasing for investment purposes.[20] In addition, settlement of these instruments contemplates delivery of the token at network launch,[21] and thus, at least with respect to the initial iteration of these instruments, the delivery of tokens for consumptive use will occur contemporaneously, or at least nearly so, with the delivery of tokens to purchasers who were investors. This would seem to argue in favor of the proposition that a token launch with delivery of tokens in settlement of these instruments is not directed solely to consumers, and, under the logic of *Gary Plastic* and the *Munchee* Order, is a securities transaction, not a consumer token launch.[22]

While recent iterations of these instruments have begun to acknowledge that issuances of the underlying tokens could be securities transactions, they continue to subject issuers and purchasers to significant risks by potentially increasing the likelihood that the underlying tokens will be deemed to be securities. This does not represent a viable outcome for many token-based networks, which require the free transfer of tokens on the network as part of their necessary function, because the US securities laws often require the existence and registration of an intermediary in securities transactions (*i.e.,* the transfer of tokens deemed to be securities). Accordingly, an issuer or platform may be required to register as a broker-dealer or exchange (or alternative trading system)[23] to permit the functioning of its token-based network,[24] which would render many token-based networks unusable. Although recent statements indicate an acceptance of the notion that a digital asset originally issued as a security could subsequently cease to be a security once the network is sufficiently decentralized,[25] the uncertainty that remains regarding the viability and timing of the consumer token sale raises challenges for appropriate disclosures to investors and potential liability for issuers. This is particularly the case when the entire investment decision is based on the availability and functionality of the underlying token, and it would seem to be challenging to craft sufficient disclosure in such a circumstance where the entire investment proposition is subject to this level of uncertainty.

A recent example of the unintended consequences of using token presale instruments can be seen in the SEC's current action against Kik.[26] Kik offered and sold Kin to accredited investors using a token presale agreement. The SEC's complaint noted that although Kik had filed a Form D for the Kin offered and sold via its token presale instrument to accredited investors, this offer and sale of Kin was not exempt from registration under Regulation D.[27] Either the Kin offered under the presale instrument was part of the same offering of Kin to the public or alternatively, it was integrated with the subsequent offering of Kin to the public. Given that the SEC viewed the public offering of Kin as non-exempt, it would follow that, if viewed as part of the same offering, the private nature of the sale of Kin under the token presale instrument was vitiated. In support of the claim that there had only been one offering

of Kin, the SEC noted that "Kik sold the Kin as part of a single plan of financing, for the same general purpose, at about the same time, without creating different classes of Kin, and for dollars or assets that were immediately convertible to dollars."[28] Furthermore, given that Kik's token presale instrument promised to deliver tokens to investors in return for their investments, from the SEC's perspective, this makes it difficult for Kik to argue that the token distribution event to the public was intended to supply tokens to users and thus not a securities offering.

Commodities law issues

Beyond the securities law concerns, the SAFT, and other similar token presale instruments, also raise commodities laws concerns. Because cryptocurrencies are commodities,[29] a presale of consumer tokens through an instrument that provides the right to receive tokens in the future, or confers the right to exchange or convert such instrument into tokens that are not securities, may be a forward contract for the sale of a commodity or a commodity option, and subject to regulation by the CFTC as a swap, if an exemption is not available.

(a) Commodity forward contracts

Forward sales of commodities fall within the CEA's broad definition of "swap," which encompasses numerous types of derivatives, and are subject to regulation by the CFTC absent an applicable exclusion.[30] Notably, the sale of a non-financial commodity for deferred shipment or delivery is excluded from the swap definition, so long as it is intended to be physically delivered,[31] but provided such forward contract also qualifies as a commercial merchandising transaction (Non-Financial Forward Contract Exclusion).[32] If such instruments are purchased by investors or speculators, they will not satisfy the requirement of the Non-Financial Forward Contract Exclusion because the purchasers are not "commercial market participants."[33] The CFTC has expressly stated that hedge funds, acting in their capacity as investors, are not commercial market participants.[34] As such, token presale instruments are effectively a prepaid forward contract of a commodity whereby parties have agreed a price or percentage discount on the token to be delivered at a later date. As discussed above, the many token presale agreements are (and continue to be) largely marketed to investors and not commercial market participants;[35] such investors would not be eligible for the Non-Financial Forward Contract Exclusion.

(b) Commodity options

More recent versions of token presale instruments have also included convertible features, which provide investors or the issuer, as applicable, a call or put right to deliver tokens upon the consummation of a token sale at an agreed price or discount. Such an instrument may constitute a commodity option and would be subject to CFTC regulation as a swap,[36] unless an exemption applies. Trade options are generally exempt from regulation by the CFTC, other than certain large trader reporting requirements and the CFTC's general anti-fraud and anti-manipulation enforcement authority (the Trade Option Exemption).[37] In order to qualify as a trade option and benefit from the Trade Option Exemption,[38] the commodity option in question must be: (i) intended to be physically settled if exercised; (ii) entered into with an offeror who is either an ECP[39] or a producer, processor or commercial user of, or merchant handling, the commodity (or products or by-products thereof) that is the subject of the option, and such offeror is offering to enter into such option solely for the purposes related to its business as such; and (iii) entered into with an offeree who is either a producer, processor or commercial user of, or merchant handling, the commodity (or

products or by-products thereof) that is the subject of the option, and such offeree is entering into such option solely for the purposes related to its business as such.

Unfortunately (as stated above in connection with the Non-Financial Forward Contract Exclusion), many of the token presale instruments are not offered to commercial market participants who would satisfy the "offeree" prong, even if the issuer of the instrument could satisfy the "offeror" prong. Additionally, even if such instruments are offered to "consumers" they would not necessarily satisfy the "offeree" prong of the Trade Option Exemption, unless such consumer could establish a nexus to a business activity. Accordingly, token presale investors are unlikely to qualify for the Trade Option Exemption.

(c) Hybrid instrument exemption

Furthermore, since token presale instruments may constitute or contain a commodity forward contract or commodity option and may not otherwise qualify for the Trade Option Exemption or the Non-Financial Forward Contract Exclusion, we also consider whether such instruments would meet the Hybrid Instrument Exemption (defined below) and, as a result, be exempt from commodities law regulation. Under CFTC Rule 34.2(a), a "hybrid instrument" is defined to include an equity or debt security with "one or more commodity-dependent components that have payment features similar to commodity futures or commodity options contracts or combinations thereof."[40] Under Section 2(f) of the CEA, a hybrid instrument that is "predominantly a security" is exempt from the provisions of the CEA if, among other things, the instrument is not marketed as a contract of sale of a commodity for future delivery (or option on such a contract) subject to the CEA (the Marketing Condition) (such exemption being the Hybrid Instrument Exemption).[41]

While token presale instruments may, in theory, be capable of qualifying for the Hybrid Instrument Exemption, because they are often primarily marketed to investors who themselves are solely or in large part motivated to purchase such instruments in order to receive the underlying commodity (i.e., the token), such instruments will often fail to satisfy the requirements of the Marketing Condition of the Hybrid Instrument Exemption.[42]

(d) Consequences of CFTC regulation

Because such presale instruments may have an embedded swap, which does not qualify for an exemption from regulation by the CFTC (as discussed above), such presale instrument would be subject to the full swaps regulatory framework applicable to such instruments. In particular, in order to trade over-the-counter, swaps must be entered into between eligible contract participants (ECPs).[43] While some investors may qualify as ECPs, token issuers typically are early stage companies that may not have at least $10 million gross assets, and as a result, would not satisfy the ECP test. A swap entered into by parties who are not ECPs would be in violation of the CEA and CFTC regulation. As a result, the contract could be rescinded and both parties could face penalties and sanctions for such actions.

Potential solutions available through traditional financing instruments

Traditional early-stage financing structures, such as preferred stock and convertible promissory notes,[44] are "tried and true" structures that generally exhibit the necessary flexibility to address the needs of early stage companies/token issuers and token platforms. We believe these structures can be augmented to address investor demand for exposure to

consumer tokens, while enabling the parties to comply with applicable securities and commodities laws. This can be achieved by providing investors with various combinations of token-related purchase, economic and voting rights.

First, the conversion and exchange rights featured in currently popular token presale instruments could be replaced with appropriately limited token sale participation and economic rights that reduce the regulatory risks associated with consumer token sales discussed above. For instance, the purchase right would not represent a conversion or exchange of the security, but would include these rights in addition to the rights granted to the holder of the securities. The exercise of such token sale participation rights could be limited to sales or distributions of the consumer tokens that would not be deemed to be securities transactions, such as when the network had achieved sufficient decentralization (although the challenges in defining an objective standard for this trigger may reduce the practicality of this option). The participation rights could also be limited to purchases for actual use, or limit the consumer tokens reserved for distribution or sale to investors, and require that any distributions or sales thereof occur in a manner that supports the broader consumer token-based network.

Instead of the inclusion of pre-negotiated token prices in such instruments, which – from a commodities law point of view – may increase the risk of being considered a commodity option because such pre-agreed price could be seen as a strike price, the participation rights could be coupled with "most favored nation" (MFN) pricing provisions, guaranteeing certain investors the best token sale and distribution terms offered by the issuer to any other third party. These rights could also be supplemented with token economic rights that could be triggered in lieu of participation in the consumer token sale. For example, preferred stock could be issued with various rights tied to consumer token sales, such as pre-negotiated dividend or redemption rights, or a convertible promissory note under which the issuer pays a multiple of the note's aggregate principal amount or the note converts into preferred stock with dividend or redemption rights. Such token economic rights would have the goal of providing the investor with a similar economic outcome of participating in the consumer token sale. As a result, the careful balancing of such token sale participation and economic rights could provide issuers the flexibility to allow for the participation of investors eager to receive token economics while protecting the development of the underlying network and consumer tokens from the application of the securities laws.

Second, because consumer tokens and the corresponding network protocol often represent a significant portion of the value proposition associated with investing in such platforms, investors can reasonably expect to receive voting rights with respect to the creation and distribution of tokens by the issuer, including the right to approve the initiation of any offerings or distributions.[45] Eventually, as the pathway for consumer token sales becomes more clear, voting rights grants may be more narrowly tailored to only apply when such a sale does not meet certain specifications. In addition, investors may seek additional protections to prevent potential uses of the issuer's token-based network that circumvent their consumer token-related economic and participation rights.

Finally, these preferred stock and convertible promissory note structures may also be preferred from a commodities law perspective for several reasons. First, conferring future participation rights on an investor to participate in a token sale, or conferring economic rights to an investor in respect of future distributions, is not clearly a swap under the CEA and subject to CFTC regulation. Currently no regulatory certainty exists as to the treatment of preferred stock and convertible promissory note structures with token participation rights,

and it is unclear whether such participation rights would constitute swaps (or not) subject to CFTC jurisdiction. There is no strike price or final price differential that creates market risk that the CFTC would necessarily be incentivized to regulate in the commodity options market. Such token participation rights seek to reduce economic risk and loss attributable to other token presale agreements. They afford the investor an MFN pricing provision to purchase the token at spot, which is likely to reduce an investor's risk of loss. Accordingly, for the reasons set forth above, we believe such structures reduce regulatory risk of CFTC intervention which is inherent in predecessor token presale instruments.

Second, if a swap were deemed to exist, in such structures where the conditions of the Hybrid Instrument Exemption other than the Marketing Condition are satisfied, one could argue that – despite the associated consumer token rights – such instruments are "predominantly securities" and unlikely to run afoul of the Marketing Condition, because the commodity forward or option would be a small portion of the value of the instrument. Accordingly, it would be much harder to argue that such instrument was marketed as a swap or purchased by investors solely for the purpose of receiving the value provided by the swap component. That is, because the predominant value of the instrument is a traditional security providing specific rights with respect to the issuer – such as traditional preferred stock rights (*e.g.,* liquidation preference, dividends, anti-dilution protection) or traditional promissory note rights (*e.g.*, returns of principal, potential conversion into equity) – such consumer token presales could arguably fall outside some (if not all) of the CFTC regulatory regime by qualifying for the Hybrid Instrument Exemption or being excluded entirely from the swap definition.[46]

Of course, while each instrument would need to be analyzed on its own merits, we believe these alternate structures have great promise for addressing commodities law issues. At minimum, they significantly mitigate the regulatory risks of the SAFT and other similar presale token structures; and at best may offer a clear path to avoid characterization as a swap subject to CFTC jurisdiction.

Importantly, even if these preferred stock and promissory note structures are not completely exempt from regulation as a swap, certain token projects and network participants may qualify for the Trade Option Exemption, giving further relief from CFTC regulatory requirements.

These structures are also preferred from a securities law perspective for many similar reasons – because the investor is receiving a more traditional security, the various rights they are purchasing are far less ambiguous, and appropriate disclosures regarding the material aspects of the investment are more easily crafted.

Please note that in collaboration with ConsenSys, we have offered up a convertible note tool which we believe addresses the concerns raised in this paper.[47]

Enabling true consumer token sales

Once a platform and token protocol has been developed, the question remains whether a viable consumer token sale may be accomplished. The Framework identifies a number of factors centering around two main inquiries to help distinguish when digital assets transactions may be characterized as securities transactions.[48] First, the Framework emphasizes the necessity of the AP for the continued success of the enterprise. Second, the Framework emphasizes the expectations held by network participants with regard to the AP and the token. Critical in this inquiry is the nature of the marketing of the consumer token and its platform, and the nature of the purchasers.

We believe we can draw three concrete takeaways from the Framework that bear upon this analysis. First, tokens offered in a manner intended to appeal to an investor's investment intent will trigger the application of the securities laws. Second, when the token-based network has developed to an extent that the value of the tokens is no longer dependent upon the entrepreneurial or managerial efforts of such network's APs, token trading on that network will not be considered securities transactions. Third, offerings of tokens with utility on a functioning token-based network that are specifically directed solely to users of that network may be conducted in a manner that renders the securities laws inapplicable.

Features of established non-security virtual currencies

Two of the most widely held and well-known digital assets – Bitcoin and Ether – provide good examples of digital assets that Director Hinman expressly posited no longer constitute securities primarily due to the decentralized nature of their use.[49] The "efforts of others" prong of the *Howey* Test requires that such efforts must be "undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise."[50] Two seminal cases provide guidance on this prong for instruments traded in well-developed markets such as Bitcoin and Ether.[51] In both *Noa v. Key Futures* and *SEC v. Belmont Reid & Co*., the Ninth Circuit applied the *Howey* Test to the sale of precious metals, finding that the *Howey* Test is not satisfied if the expectation of economic return is based on market forces, and not on the efforts of an AP. Thus, the applicability of these cases to the analysis of Bitcoin and Ether within this prong of the *Howey* Test (and therefore the analysis of whether either Bitcoin or Ether is a security) depends on the existence of an established, decentralized market where the spot price is determined by ordinary market forces.

What is the role of the AP? Decentralized networks

As discussed above, the SEC's emerging regulatory framework for consumer tokens appears to be focused on a threshold question derived from the fourth prong of the *Howey* Test: is the token-based network sufficiently decentralized/independent of the entrepreneurial efforts of the AP? There are several factors underlying this inquiry and each case requires careful analysis, and, without further guidance from the SEC, it is difficult to predict the appropriate weighting of such factors.

(a) *Ongoing development and maintenance of the network*

For a token-based network to be truly decentralized, no AP should have the ability to significantly and directly influence the value of the consumer tokens exchanged on the network. This implicitly includes ongoing efforts to develop and maintain the network. The Framework states it is more likely that a token purchaser is relying on the efforts of others if "[a]n AP is responsible for the development, improvement (or enhancement), operation, or promotion of the network, particularly if purchasers of the digital asset expect an AP to be performing or overseeing tasks that are necessary for the network or digital asset to achieve or retain its intended purpose or functionality." Open source projects, where a variety of parties may contribute to the ongoing development of the network, clearly have a greater chance of meeting this requirement.

(b) *Use of token sale proceeds*

Similarly, the expected use of proceeds from a related token sale can impact whether a related token-based network is sufficiently decentralized. For example, a use of proceeds that involves further development and maintenance of the network could lead to a conclusion that the efforts of the issuer remain central to the value of the token. The Framework states that reasonable expectation of profits is more likely to be

present if "[t]he AP continues to expend funds from proceeds or operations to enhance the functionality or value of the network or digital asset." This further supports the use of traditional financing instruments, coupled with economic rights in future token offerings. Issuers utilizing such instruments would be able to fund the development of their network from the investments received pursuant to such instruments and would, subsequently, be able to use the proceeds from token sales to deliver a return of capital to investors, thereby clearly distinguishing early stage investments from token purchases and supporting the position that the tokens themselves should not be deemed to be securities.

(c) Network governance

The Framework also indicated that a token-based network's governance structure will be considered when determining whether such network is decentralized.[52] In its most simple form, a decentralized governance structure would provide token holders the ability to directly determine matters relevant to the network's development. Reliance on the efforts of others is more likely to be deemed present if an AP has a continuing managerial role in network governance, including exercising judgment concerning the network or the characteristics and rights that the digital asset represents. The sufficient decentralization argument is strengthened if the AP can avoid playing a lead role in making decisions regarding governance issues, code and protocol updates, and how third parties participate in the validation of transactions that occur with respect to the digital asset.

(d) Robust token economy

The value of tokens on certain token-based networks is driven by a robust token economy pitting a number of different forces with different operating incentives against each other. These competing elements will be ascendant, and have a corresponding impact on the token value, at differing times. Courts have reasoned that this sort of market valuation mechanism is critical to distinguish a commodity from a security, as the value in the instrument is created by these broad market forces rather than the efforts of others.[53] The Framework also recognizes principle, noting that token "[p]rice appreciation resulting solely from external market forces impacting the supply and demand for an underlying asset generally is not considered "profit" under the *Howey* test." Filecoin[54] is an apt example of a robust economic structure that helps ensure market forces drive token values independent of the AP's efforts. The Filecoin network involves three network participants: (i) clients, who pay to store and retrieve data; (ii) storage miners, who provide data storage to the network; and (iii) retrieval miners, who provide data retrieval to the network.[55] As a result, the competing activities of these three groups create the value of a Filecoin token through the creation of supply and demand economics. This also means the success of the Filecoin network hinges upon a sufficient number of market participants contributing to the network simultaneously, which is a premise reflected in the high proportion of Filecoin tokens allocated to miners in exchange for storage and retrieval services.[56]

There are numerous token-based networks and token economy models that similarly promote the development of a robust economic structure. The success of most decentralized token-based marketplaces, whether for data storage, artificial intelligence, real estate or intellectual property, is dependent on market participants driving the value of the networks and its corresponding tokens. As a result, these marketplaces, like those for Bitcoin and Ether (which rely on market participants to

record transactions on their respective blockchains), have a market valuation mechanism that is helpful in distinguishing a commodity from a security.

Is the asset designed for consumptive purposes? Consumer tokens and consumer token sales

Numerous consumer token and consumer token sale features warrant consideration in furthering the consumer token analysis to determine whether the securities laws may apply.

(a) Functioning network

A factor closely related to the role of the AP, though distinct, is the question of whether the token-based network is "fully functioning or in the early stages of development."[57] A common feature of many early token sales was that they were commenced before the consumer could actually utilize the token. While some consumer goods are purchased in this manner (*e.g.,* concert tickets or a new Tesla car), consumer token presales complicate the analysis of whether "the primary motivation for purchasing the digital asset is for personal use or consumption."[58] Although it remains difficult to assign weighting to the factors presented in the Framework, network functionality appears to be factor that has significant bearing. As such, issuers should, to the extent possible, launch their token-based network prior to initiating consumer token sales.

(b) Secondary markets and transferability

In February 2018, SEC Chairman Jay Clayton testified before the US Senate Committee on Banking, Housing and Urban Affairs, in part sharing his particular concern for token issuers and emphasizing the secondary market trading potential of the tokens offered for sale.[59] This line of thinking clearly follows the *Gary Plastic* case, where the marketing of a non-security investment (*i.e.,* bank certificates of deposit) that included the promise of a secondary market transmutes the certificates of deposit into investment contracts.[60] Accordingly, the Framework states that if the AP promises to arrange trading of the digital asset on a secondary market, this means the token purchasers reasonably rely on the AP for liquidity, strongly supporting the view that such token is a security. However, the mere availability of a secondary market developing following a token sale arguably should not be dispositive and, perhaps, should not matter at all. Again, *Gary Plastic* stands for the notion that it is the *marketing* of the "investment" based on the potential of the secondary market that is what makes the instrument a security. Of course, there are many everyday commodities for which secondary markets regularly develop – in fact, eBay has built a robust business on this basis – and the mere existence of such markets do not transmute the instruments into securities.

For example, a large number of active market participants is critical to the success of Filecoin's network. It is difficult to imagine a scenario where it could achieve the critical mass of network participants necessary if such network participants were restricted from exchanging in some way their Filecoin tokens with other participants for other digital assets or tokens as part of continually broadening the universe of token holders. In order for a network to work under isolated conditions, where such transfers were not permitted, not only would suppliers have to consume the resources created by the network, but maintaining a balance among suppliers and producers would be exceedingly difficult. The secondary market transactions accordingly act to balance the various economic demands without any one actor having to play all roles. Otherwise, for Filecoin, a miner would need to both provide and consume storage and retrieval services, because consumption would be the only way to realize the economic gain in exchange for providing such services. As a result, there would be little

incentive for the miner to participate on such a network. A similar case can be made for any network that includes both suppliers/producers of goods or services and consumers of goods or services. Furthermore, supply on any such market would decrease rapidly if the inputs required to produce the supply of goods and services were not principally derived from the tokens received upon sale, or if an insufficient number of other goods and services were available to enable suppliers to consume all of the tokens they earn within such marketplace. Given the negative effect on network participation that limiting secondary market activity would have, it is likely that overly broad restrictions would impede competition and that only the largest and most established marketplaces would succeed.

Because of the foregoing, a measured approach to addressing secondary market activity and transferability is advisable. Fortunately, the flexibility available with second and third generation blockchain technologies provide companies with several options. First, purchasers of consumer tokens in a consumer token sale could be required to agree to a lockup mechanism, whereby a smart contract prevents the purchaser from selling their tokens for a certain period of time or until they participate on the network in the required manner. That is, they could be unlocked initially only in the event they were utilized on the platform itself first, and thereafter could be traded in the secondary market. Second, a tiered transfer fee or other incentive structure could be implemented, whereby the fees (or other similar incentives) for tokens transferred in connection with participation on the token-based network could be lower than the fees for transfers to non-network participants. In each of these cases, initial purchasers would not have the same profit motive in seeking secondary market for token sales as they may have in a typical token offering.

Director Hinman appears to have suggested as much in his enumerated factors.[61]

(c) Inflationary issuances

Another aspect of consumer token sale structures that warrants discussion is the impact of inflationary/deflationary pressures in token economies. Depending on the token structure, there are a number of scenarios in which subsequent issuances of tokens in exchange for contributions to the economy of the network can simultaneously facilitate network growth while limiting the immediate speculative potential of the token. For example, Filecoin's token allocation design made 70% of the total Filecoin tokens available for miners in exchange for data storage and retrieval services. As those tokens will be subsequently distributed and "earned" by miners, the Filecoin token purchasers are "diluted" in an inflationary sense. However, unlike in the context of an equity security where dilution is significant because the valuation of the interest is always proportionate to the relative interest in the enterprise value, here the value of the token is based on the value of the goods and services that may be received in exchange, and the market supply and demand for such goods and services. Thus, the impact of dilution on a true consumer token is quite different and the value of the token should correspond more directly to the value to the consumer of the applicable goods and services. As a result, consideration should be given to the supply dynamics of a token economy.[62] Ultimate control over dilutive issuances is also a factor in network governance, which may impact the analysis above regarding the decentralization of a given network.

(d) Token retention

To date, a common feature of token offerings has been the retention of the tokens by issuers for distribution to founders, employees, advisors and investors. In instances

where there are reasonable and justifiable grounds to believe that these individuals can and will consume these tokens through their own market participation and will thus assist in the seeding of the network, then consumer token issuers should not be dissuaded from including the retention of consumer tokens in their allotment strategy. However, issuers should exercise caution in doing so, particularly in cases where the products and services offered on an issuer's network or the number of tokens retained could not reasonably be consumed by its founders, employees, advisors and investors. In such instances, it would be difficult to make a credible argument to the SEC that such tokens are not being held for investment purposes.[63] The Framework states that token retention by an AP cuts towards reliance on the efforts of others given that token "[p]urchasers would reasonably expect the AP to undertake efforts to promote its own interests" by taking actions that enhance the value of the digital asset. In addition, such retention of tokens also makes it more difficult for the token issuer to demonstrate that the tokens are "[d]ispersed across a diverse user base[,]" rather than being "[c]oncentrated in the hands of a few that can exert influence[.]"[64]

As a result, companies who wish to reward their teams for the successful development of a token-based network giving rise to a consumer token sale should look to traditional equity compensation methods, which can be augmented by consumer tokens to the extent a viable use case can be established. Additionally, selling restrictions with respect to both timing and price of tokens by such holders could be adopted to bolster the argument that such grants were not made to persons with an investment intent.

(e) Virtual Currency Peg / Stablecoins

Another means of limiting the speculative potential in the purchase and sale of consumer tokens could be the adoption of token structures that initially peg the value of the consumer token to fiat or virtual currency, also known as a "stablecoin." The Framework highlights that tokens designed and marketed as virtual currencies are less likely to be considered securities under the *Howey* test if the token can be used to pay for goods or services without first having to convert it to fiat currency or another token. In addition, the token must operate as a store of value that can be saved, retrieved, and exchanged for something of value at a later time. In the Turnkey Jet matter, the company alerted the Commission of its intent to issue "tokenized jet cards" (tokens) on a user-platform facilitating the procurement of chartered airline flights. In its letter to the Commission, Turnkey Jet made clear that consumers of these tokens would be "motivated . . . by a desire to obtain on-demand air charter services" not by an expectation of future profits. Accordingly, Turnkey Jet maintained that these tokens would not be securities under the *Howey* framework. The Commission agreed, and identified several key attributes of the Turnkey Jet tokens that highlighted their consumptive utility and non-speculative nature. Specifically, the Turnkey Letter noted that Turnkey Jet's tokens would be immediately usable, have a fixed value of one USD per token and would be marketed in a manner that emphasized their functionality and not the potential for an increase in their market value.

As an alternative, in the case of an early-stage marketplace, an issuer could incentivize sellers to advertise their products or services in both the network's native virtual currency/token, as well as, for example, Ether, with the price of the goods or services being determined by the market price of Ether. The transaction could then be consummated in the native token of the network. This structure could have the effect of deterring speculative purchases at the time of an issuer's consumer token sale

because the price of the token would presumably face downward pressure to remain in-line with the exchange rate with the virtual currency peg. As a result, a virtual currency peg could result in the price of a given consumer token being primarily influenced by individuals or events beyond the token issuer's control and may therefore be viewed favorably by the SEC.[65] Once a larger and more functional network was operational with active participants, these incentivizing schemes could be removed to allow for free market activity.

We would note that stablecoins may be swaps subject to CFTC regulation. Such structure would need to be carefully considered under commodities laws.

(f) Token sale legal documentation

Another means of discouraging purchasers of consumer tokens from an expectation of profit could be found in the documentation used in sales of tokens by issuers. Such agreements could include representations and warranties requiring purchasers to state that their intention is to use such consumer tokens on the issuer's network. As discussed above, such documentation could also include lockup mechanisms, whereby the purchaser's tokens could be "locked" using a smart contract for a specified period. Furthermore, instruments could grant issuers a first refusal with respect to any purchaser's tokens, whereby the issuer would be entitled to repurchase the tokens held by a user if the user had determined not to use them on the issuer's network. In many respects, this could be functionally similar to rights of return that are commonly provided by retailers with respect to tangible consumer goods, and issuers may be well advised to allocate a small percentage of any consumer token sales for such repurchases. While on most networks the issuer will only ever have privity of contract with the initial purchasers of consumer tokens, utilization of these mechanisms could substantially reduce the risk of such purchasers having an expectation of requiring the protection of securities laws. However, establishment of valuation protocols and resale price, as well as the potential of a withdrawal of cash from an issuer, may detract from the attractiveness of this alternative.

Seeding network activity and achieving decentralization

Based on the foregoing considerations, issuers who both operate decentralized networks featuring tokens designed for consumption, and sell such tokens in a manner designed to dissuade purchases for investment, should be capable of avoiding the application of securities laws to such token sales under the *Howey* Test. However, this current paradigm appears to create a paradox, given that the process of creating a decentralized and functional network on which consumer tokens can be utilized necessitates that issuers first seed network activity by issuing consumer tokens in transactions that do not trigger the application of the securities laws.

As a result, issuers may seek to seed their network through the distribution of consumer tokens via "airdrops" and other distributions to affiliates, vendors and community members. Such distributions promote network activity, facilitate the implementation governance procedures and enable network testing prior to full launch. The information garnered from this process enables developers to resolve potential issues and simultaneously enhances the credibility of the project both within and outside its community. Furthermore, such activity can help consumers better understand the value of the overall network and each consumer token, which ultimately promotes market efficiency. The benefits of such seed activity extend to consumer token issuances targeting strategic partners, who may also assist with

the development of the network prior to launch. In addition, this seed activity permits the nascent token economy of the platform to grow, allowing forces beyond those of the initial AP to begin to determine the value of the token. As a result, this activity directly addresses several of the factors identified by Director Hinman and can strengthen the case that a particular token is a consumer token.[66]

Nonetheless, issuers need to be aware that the SEC takes the view that the securities laws apply to airdrops of tokens, even though no money or digital currency funds is given by airdrop recipients. For example, in the early days of the internet, some issuers sought to issue free shares of common stock to registered website users, as part of a broader promotion to attract traffic to the website and promote brand awareness and loyalty. The SEC took the view that the free distribution of shares was a "sale" of securities.[67] Similarly, the SEC has taken the view that the spin-off of shares of a subsidiary as a free stock dividend to an issuer's shareholders can be a sale of securities.[68] As a result, unless and until the SEC gives more lenient guidance, airdrops should be considered and conducted in the same manner as token offerings, generally, as discussed above.

Although sufficient decentralization is difficult to define precisely, there are potential steps that the SEC can take to provide market participants with greater clarity. The SEC has highlighted a number of factors to consider when inquiring whether a token-based network is sufficiently decentralized. Of course, as noted by Commissioner Peirce,[69] it would be helpful if the SEC could provide clarity as to the appropriate weighting of such factors. One of the primary goals of securities law is to protect investors through the mitigation of information asymmetries that exist between issuers and investors. We propose that this principle should inform the weighting of the factors used to measure the sufficient decentralization of a network. As a result, there should be less emphasis on factors that penalize tokens simply because they bear similarity to securities in their marketing, and greater emphasis on factors that have a clear nexus to the reduction of information asymmetries. For example, the decentralization of network development and maintenance as well as network governance should be factors that are amongst the most heavily weighted. If such activity is truly decentralized, the less likely it is for there to be information asymmetries between network users and a powerful central group that manages the network.

On the other hand, the SEC should give less weight to factors such as a token's transferability or the existence of secondary markets for it. As discussed, a commodity does not become a security simply because there are secondary markets on which it is traded. It is critical to the success of certain token-based networks to have a large number of active market participants. If users on such networks were restricted from exchanging in some way their tokens with other potential participants, it is unlikely that the network could reach the necessary critical mass.

Furthermore, the SEC should provide clear guidance regarding potential pathways for achieving sufficient decentralization. Under the current regulatory framework, developers need to be wary that the seeding of their network via token "airdrops" and other distributions to affiliates, strategic partners, vendors and community members could be deemed to be a securities offering given that the issuer may receive a direct benefit from such distributions. However, these parties are unlikely to require protection from the information asymmetries securities laws are designed to guard against and these distributions are a vital step for many networks to be able to achieve decentralization. Such distributions often promote network activity, facilitate the implementation of governance procedures, enable network testing prior to full launch and incentivize third-party development work. In addition, this seed activity

permits the nascent token economy of a network to grow, allowing forces beyond those of the initial promoter to begin to determine the network's value. As a result, this activity directly addresses several of the factors identified in the Framework and can strengthen the case that a particular network is decentralized.

Conclusion

Much has been made of the need for certainty, and perhaps even innovation, in the application of various laws, including the US securities and commodities laws, to commercial activities relating to blockchain, cryptocurrencies and related technologies. After all, the applicable federal securities statute is over 85 years old, and the seminal case, *Howey*, is more than 70 years old. That said, the SEC has not retreated from the application of existing precedent when examining token transactions. Nevertheless, given the underlying principles, and the SEC's public statements, there is some reason for optimism that the existing framework will permit at least some transactions in tokens – consumer token launches – to be executed without the application of the federal securities laws. We suggest, however, that it continues to be prudent for interested parties to seek guidance directly from the SEC staff before proceeding.

* * *

Acknowledgments

In addition to the co-authors listed below, the authors gratefully acknowledge the invaluable contributions of Naim Culhaci, Cameron Kates, Shaun Musuka and J. Ashley Weeks.

Paul M. Dudek

Tel: +1 202 637 2377 / Email: paul.dudek@lw.com

Paul Dudek is a counsel in the Washington, D.C. office of Latham & Watkins. From 1993 to 2016, he was Chief of the Office of International Corporate Finance in the US Securities Exchange Commission's (SEC) Division of Corporation Finance. Mr. Dudek has deep experience in SEC registrations, and his practice covers all aspects of cross-border capital market transactions involving non-US companies and sovereigns, as well as related regulatory matters. In his previous role, Mr. Dudek oversaw the Office's efforts to develop and implement rulemaking initiatives and interpretive policies pertaining to US public and private offerings, listings and other transactions and periodic reporting by foreign private issuers in the US and multinational offerings by foreign and domestic issuers.

Miles P. Jennings

Tel: +1 650 463 3063 / Email: miles.jennings@lw.com

Miles Jennings is an associate in the Silicon Valley office of Latham & Watkins. Mr. Jennings represents public and private technology, life science, cryptocurrency and other growth companies, as well as the entities that finance them. His practice focuses on general corporate counseling, venture capital financings, cryptocurrency offerings, mergers and acquisitions, and public offerings. Mr. Jennings' general company representation includes assistance with formation issues, employment matters, equity incentives, securities law compliance, negotiation of license agreements, and advising boards of directors regarding corporate governance matters.

Endnotes

1. The Digital Asset Taxonomy published by ConsenSys, a leader in the blockchain field, defined "consumer tokens" as "inherently consumptive in nature, which means that their intrinsic features and primary use are to represent, or facilitate the exchange of or access to, a limited set of goods, services, or content. The term "consumer" here refers to the consumptive nature of the relevant goods, services, or content, which businesses as well as individual users may ultimately use or consume[.]" DIGITAL ASSET TAXONOMY: FROM THE PERSPECTIVE OF GLOBAL FRAMEWORKS FOR SECURITIES AND FINANCIAL INSTRUMENTS, https://thebkp.com/token-taxonomy/ (last visited July 26, 2018).
2. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
3. 15 U.S.C. §§ 77b(a)(1), 78c(a)(10).
4. *See Howey* at 301.
5. *See id.*
6. *See* Latham & Watkins, SEC Takes Enforcement Action against Utility Token ICO, Client Alert No. 2257 (Dec. 20, 2017), https://www.lw.com/thoughtLeadership/SEC-vigorously-police-utility-token-ICO.
7. *Gary Plastic Packaging v. Merrill Lynch, Pierce, Fenner, & Smith Inc.*, 756 F.2d 230 (2d Cir. 1985).
8. *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4 2019).
9. *Id.*
10. *Kik Responds to SEC Complaint*, PR NEWSWIRE (June 4, 2019), https://www.prnewswire.com/news-releases/kik-responds-to-sec-complaint-300862114.html [hereinafter Kik Response Article].
11. Wells Submission of Kik Interactive, Inc. and the Kin Ecosystem Foundation at 17 (Dec. 10. 2018), https://www.kin.org/wells_response.pdf.
12. Kik Response Article.
13. *See, e.g.,* 7 U.S.C. §§ 6c(a), 9, 12(a)(5), 15; 17 C.F.R. § 180.1; *see also* Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41398 (July 14, 2011), https://www.gpo.gov/fdsys/pkg/FR-2011-07-14/pdf/2011-17549.pdf.
14. Timothy Massad, Chairman, Commodity Futures Trading Comm'n, Testimony of Chairman Timothy Massad before the U.S. Senate Committee on Agriculture, Nutrition & Forestry (Dec. 10, 2014), http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6 [hereinafter 2014 Massad Senate Testimony].
15. During this time, the CFTC has settled enforcement actions with exchanges, stressing a distinct aspect of its jurisdictional oversight in each: from establishing that virtual currencies are "commodities," to applying the retail commodity rules to leveraged virtual currency transactions, to asserting jurisdiction over virtual currency derivatives. *See* Latham & Watkins, CFTC Brings Significant Enforcement Action Against Online Cryptocurrency Exchange, Client Alert No. 1980 (June 20, 2016), https://www.lw.com/thoughtLeadership/CFTC-brings-significant-enforcement-action-against-online-cryptocurrency-exchange; Latham & Watkins, Enforcement Trends in Cryptocurrency, Client Alert No. 1904 (Dec. 9, 2015), https://www.lw.com/thoughtLeadership/lw-enforcement-trends-cryptocurrency; Latham & Watkins, Cryptocurrencies Are

Commodities: CFTC's First Bitcoin Enforcement Action, Client Alert No. 1874 (Sept. 21, 2015), https://www.lw.com/thoughtLeadership/LW-CFTC-first-bitcoin-enforcement-action.

16. *See, e.g.*, CFTC Release PR7938-19, CFTC Charges Company and its Principal in $147 Million Fraudulent Bitcoin Trading Scheme (June 18, 2019), https://www.cftc.gov/PressRoom/PressReleases/7938-19; CFTC Release PR7839-18, CFTC Orders Former Virtual Currency Trader to Pay More than $1.1 Million for Fraudulent Bitcoin and Litecoin Scheme (Nov. 9, 2018), https://www.cftc.gov/PressRoom/PressReleases/7839-18; CFTC Release PR7813-18, CFTC Charges Two Defendants with Fraudulent Solicitation, Impersonation of a CFTC Investigator, and Forging CFTC Documents, All in Attempt to Steal Bitcoin (Sept. 28, 2018), https://www.cftc.gov/PressRoom/PressReleases/7813-18; CFTC Release PR7714-18, CFTC Charges Multiple Individuals and Companies with Operating a Fraudulent Scheme Involving Binary Options and a Virtual Currency Known as ATM Coin (April 18, 2018), https://www.cftc.gov/PressRoom/PressReleases/7714-18; CFTC Release PR7614-17, CFTC Charges Nicholas Gelfman and Gelfman Blueprint, Inc. with Fraudulent Solicitation, Misappropriation, and Issuing False Account Statements in Bitcoin Ponzi Scheme (Sept. 21, 2017), http://www.cftc.gov/PressRoom/PressReleases/pr7614-17.
17. The following discussion of consumer token presales only seeks to address fundraising instruments utilized for pure consumer token issuances and not instruments utilized for pure security token issuances, which often have similar terms. We note that the presale of a token designed to be a security is a far easier analysis, as each of the instruments should be offered and sold in compliance with securities law requirements and ordinary corporate finance practices.
18. *See, e.g.,* Juan Batiz-Benet, Jesse Clayburgh & Marco Santori, THE SAFT PROJECT: TOWARD A COMPLIANT TOKEN SALE FRAMEWORK (Oct. 2, 2017), https://saftproject.com/static/SAFT-Project-Whitepaper.pdf [hereinafter SAFT Whitepaper].
19. In addition to the securities law issues and commodities law issues discussed below, the SAFT and similar presale instruments can raise tax concerns in light of the uncertainty regarding their treatment for US federal income tax purposes. It is possible that an issuer could be subject to US federal income tax on proceeds from SAFT sales on a current basis, particularly where the underlying tokens are consumer tokens.
20. *Id.* (Section 5(c) of the SAFT, which is included as Exhibit 1 to the SAFT Whitepaper):

    "(c) The Purchaser has no intent to use or consume any or all Tokens on the corresponding blockchain network for the Tokens after Network Launch. The Purchaser enters into this security instrument purely to realise profits that accrue from purchasing Tokens at the Discount Price."
21. Defined in the SAFT as "a *bona fide* transaction or series of transactions, pursuant to which the [issuer] will sell the Tokens to the general public in a publicized product launch." Simple Agreement for Future Token, https://saftproject.com/static/Form-of-SAFT-for-token-pre-sale.docx (last visited July 29, 2018).
22. We note that some practitioners have proposed that if the network launch occurs more than six months after the SAFT sale, they should constitute two distinct plans of financing and thus would not be integrated in accordance with the safe harbor of Rule

502 under the Securities Act. In this regard, we would consider the concurrent settlement to negate this proposition. Similarly, the SAFT itself may constitute an offering of the underlying token that is continuous until delivery. In any event, we would expect that the tokens received by SAFT investors would nevertheless constitute securities on the date of delivery given the nature of the SAFT offering and the delivery of tokens to investors, unless the network has become sufficiently decentralized in the interim such that the "efforts" prong of the *Howey* Test was no longer satisfied.

23. It is worth noting, however, that the US House of Representatives recently passed several bills aimed at improving capital formation for smaller companies. For example, the Main Street Growth Act would amend the Securities Exchange Act of 1934, as amended, to allow registration of venture exchanges that would provide trading venues tailored for smaller companies, such as blockchain-based start-ups, whose securities are considered less liquid than those of larger companies. Main Street Growth Act, H.R. 5877, 115th Congress (as passed by House, July 10, 2018), https://www.congress.gov/bill/115th-congress/house-bill/5877; *see* Tom Zanki, *House Passes Bill to Allow Venture Exchanges,* LAW360 (July 11, 2018), https://www.law360.com/articles/1062096/house-passes-bill-to-allow-venture-exchanges.
24. *See* 15 U.S.C. § 78c(a)(4)(A) (defining "broker" as "any person engaged in the business of effecting transactions in securities for the account of others"); 15 U.S.C. § 78c(a) (5)(A) (defining "dealer" as "any person engaged in the business of buying and selling securities . . . for such person's own account"); 15 U.S.C. § 78c(a)(1) (defining "exchange" as "any organization, association or group of persons, whether incorporated or unincorporated, which constitutes, maintains or provides a marketplace or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange as that term is generally understood, and includes the market place and the market facilities maintained by such exchange").
25. *See* William Hinman, Dir., Div. Corp. Fin., Sec. & Exch. Comm'n, *Digital Asset Transactions: When Howey Met Gary (Plastic)* (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418 [hereinafter Hinman Speech].
26. *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4, 2019).
27. *Id.*
28. *Id.*
29. *See, e.g.,* 2014 Massad Senate Testimony.
30. *See* 7 U.S.C. § 1a(47)(A)(ii) ("the term 'swap' means any agreement, contract, or transaction . . . that provides for any purchase, sale, payment, or delivery . . . that is dependent on the occurrence, nonoccurrence, or the extent of the occurrence of an event or contingency associated with a potential financial, economic, or commercial consequence"). Swap contracts are subject to a myriad of CFTC regulations under the CEA, as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the Dodd-Frank Act), including the requirement that over-the-counter (OTC) swap counterparties be "eligible contract participants." *Id.* § 1a(18) (defining eligible contract participants (ECPs)). An individual can only qualify as an ECP if such person has amounts invested on a discretionary basis, the aggregate of which is in excess of US$10 million; or US$5 million and enters into swaps in order to manage the risk associated with an asset owned or liability incurred (or reasonably likely to be

owned or incurred) by such person. *Id*. § 1a(18)(A)(xi). If one or both of the parties to a swap transaction are non-ECPs, the swap must be executed on a CFTC-registered designated contract market. *Id*. § 2(e).

31. Both the CEA and CFTC regulations thereunder have long recognized a forward contract exclusion from futures contracts. *See* 7 U.S.C. § 1a(27) ("The term 'future delivery' does not include any sale of any cash commodity for deferred shipment or delivery."). Following enactment of the Dodd-Frank Act in 2010, the sale of a non-financial commodity for deferred shipment or delivery was also excluded from the definition of "swap" in Section 1a(47) of the CEA under the Non-Financial Forward Contract Exclusion. *Id.* § 1a(47)(B)(ii).
32. *See* Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement"; Mixed Swaps; Security-Based Swap Agreement Recordkeeping, 77 Fed. Reg. 48208, 48228 (Aug. 13, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-08-13/pdf/2012-18003.pdf [hereinafter *Products Release*].
33. As the CFTC has noted, "the underlying postulate of the [forward] exclusion is that the [CEA's] regulatory scheme for futures trading simply should not apply to private commercial merchandising transactions which create enforceable obligations to deliver but in which delivery is deferred for reasons of commercial convenience or necessity." *Id.* at 48228.
34. The CFTC drew a clear distinction between commercial market participants and investors in the Products Release, stating that "[a] hedge fund's investment activity is not commercial activity within the CFTC's longstanding view of the Brent Interpretation." *Id.* at 48229. The "Brent Interpretation" refers to the CFTC's 1990 interpretation of the application of the forward contract exclusion from the definition of "future delivery" in the context of "book-outs" transactions, which the CFTC extended in the Products Release to apply to the forward contract exclusion from the swap definition for non-financial commodities. Statutory Interpretation Concerning Forward Transactions, 55 Fed. Reg. 39188 (Sept. 25, 1990), https://cdn.loc.gov/service/ll/fedreg/fr055/fr055186/fr055186.pdf.

    Moreover, the CFTC continued to elaborate on its discerning view of "commercial" in the Products Release, stating that "an investment vehicle taking delivery of gold as part of its investment strategy would not be engaging in a commercial activity within the meaning of the Brent Interpretation." Products Release at 48229. However, if the investment vehicle were to own a chain of jewelry stores and would purchase gold on a forward basis to provide raw materials for the jewelry store, the CFTC would consider such activity to fall within the forward contract exclusion under the Brent Interpretation. *Id*. Notably, the CFTC stated in the Products Release that, for purposes of the "swap" definition, the Non-Financial Forward Contract Exclusion will be interpreted in a manner consistent with the CFTC's historical interpretation of the existing forward exclusion with respect to futures. As a result, the Brent Interpretation analysis is applicable for purposes of evaluating the Non-Financial Forward Contract Exclusion as it pertains to the "swap" definition. *Id*. at 48227-48228.
35. *See id.*; *supra* text accompanying note 20.
36. 7 U.S.C. § 1a(47)(A)(i) ("the term 'swap' means any agreement, contract, or transaction . . . that is a put, call, cap, floor, collar, or similar option of any kind that is for the purchase or sale, or based on the value, of 1 or more . . . commodities").

37. *See* 17 C.F.R. § 32.3(c).
38. *See* 17 C.F.R. § 32.3(a).
39. *See supra* text accompanying note 27.
40. 17 C.F.R. § 34.3(a).
41. Under Section 2(f) of the CEA, a hybrid instrument is "predominantly a security" and exempt from the provisions of the CEA if:
    1. the hybrid instrument issuer receives payment in full of the hybrid instrument's purchase price, substantially contemporaneously with delivery of the hybrid instrument;
    2. the hybrid instrument purchaser/holder is not required to make any payment to the issuer in addition to the purchase price described above, whether as margin, settlement payment or otherwise, during the life of the hybrid instrument or at maturity;
    3. the hybrid instrument issuer is not subject by the instrument's terms to mark-to-market margining requirements; and
    4. the hybrid instrument is not marketed as a contract of sale of a commodity for future delivery (or option on such a contract) subject to the CEA.

    7 U.S.C. § 2(f)(2).
42. This discussion assumes that prongs (i) – (iii) of the Hybrid Instrument Exemption are met with respect to any such presale instrument. Any such presale instrument must meet all four prongs of the exemption.
43. *See supra* text accompanying note 27; 7 U.S.C. § 2(e).
44. Such securities offerings are almost exclusively accomplished through the use of an exemption from registration, such as in a private placement that is limited to participants who are "accredited investors," as defined in 17 C.F.R. § 230.501, either under the more traditional style private placement of Regulation D, Rule 506(b), or the crowdfunding compatible, Regulation D, Rule 506(c). Issuers may also consider utilizing Regulation CF or Regulation A, which permit sales to non-accredited investors after making certain filings with the SEC. For additional information, see Latham & Watkins, SEC Adopts Final Crowdfunding Rules, Client Alert No. 1893 (Nov. 10, 2015), https://www.lw.com/thoughtLeadership/lw-sec-adopts-crowdfunding-rules; Stephen P. Wink and Brett M. Ackerman, Crowdfunding Under the SEC's New Rules, 49 REV. OF SEC. & COMMODITIES REG. 267 (Dec. 21, 2016), https://www.lw.com/thoughtLeadership/crowdfunding-SEC-new-rules-2016.
45. While issuers should be cautious when granting such rights, generally the enterprise and its investors are best served when their interests align. In consumer token sales, the parties share a direct interest in ensuring the offering or distribution complies with applicable securities and commodities laws. In addition, all participants should share a similar interest in the maturing of the market for token presales, as in the traditional venture capital space, to attract capital from investors that have yet to approach the sector due to regulatory risks.
46. A discussion of the types of structures that may so qualify and the nature of the availability of the possible exemptions is beyond the scope of this chapter.
47. *See* Latham & Watkins, Token Presale Agreements and the ConsenSys Automated Convertible Note (May 22, 2019), https://www.lw.com/thoughtLeadership/token-presale-agreements-consensys-automated-convertible-note.

48. *See* Hinman Speech; *see also* Latham & Watkins, A Path Forward for Consumer Tokens, Client Alert No. 2336 (June 27, 2018), https://www.lw.com/thoughtLeadership/lw-a-path-forward-for-consumer-tokens.

49. *See* Hinman Speech.

50. *SEC v. Glenn W. Turner Enterprises Inc*., 474 F.2d 476, 482 (9th Cir. 1973) ("[T]he fact that the investors here were required to exert some efforts if a return were to be achieved should not automatically preclude a finding that the Plan or Adventure is an investment contract. To do so would not serve the purpose of the legislation. Rather we adopt a more realistic test, whether the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise."); *see United Housing Found., Inc. v. Forman*, 421 U.S. 837, 855 (1975) (the "efforts of others" prong of the *Howey* Test requires that investors have a reasonable expectation of profit derived from the efforts of others).

51. In *Noa v. Key Futures, Inc*., the Ninth Circuit held that if the expectation of economic return from an instrument is based solely on market forces, and not on the efforts of a promoter, then the instrument does not satisfy this prong of the *Howey* Test. *Noa v. Key Futures, Inc*., 638 F.2d. 77 (9th Cir. 1980). The scheme in *Noa* involved the sale of silver bars through high-pressure sales efforts, and the Ninth Circuit's decision rested primarily on the existence of a separate market for the instrument that the investor could sell into, such that the economic return was driven by the market price and not the efforts of the promoter: "Once the purchase of silver bars was made, the profits to the investor depended upon the fluctuations of the silver market, not the managerial efforts of Key Futures. The decision to buy or sell was made by the owner of the silver." *Id*. at 79.

    SEC v. Belmont Reid & Co. involved a promoter that was involved in a gold mining operation who obtained prepayments from investors for the purchase of gold coins that would be obtained as a result of the mining operation. *SEC v. Belmont Reid & Co,* 794 F.2d 1388 (9th Cir. 1986). While the purchaser's return was highly dependent on the ability of the promoter to successfully mine and deliver the gold coins, the Ninth Circuit reasoned that the same non-performance risk exists in the context of any sale-of-goods contract in which the buyer pays in advance, and therefore that such a dependence on the promoter's efforts could not itself satisfy the *Howey* Test without making any such sale-of-goods contract a security. Instead, the Ninth Circuit held that the *Howey* Test was not satisfied in *Belmont Reid & Co*., because the purchasers who prepaid for the gold coins: "[H]ad as their primary purpose to profit from the anticipated increase in the world price of gold . . . In short, the purchaser[s] were speculating in the world gold market . . . To the extent the purchasers relied on the managerial skill of [the promoters] they did so as an ordinary buyer, having advanced the purchase price, relies on an ordinary seller." *Id.* at 1391.

52. *See id.*

53. *See supra* text accompanying note 47.

54. Please note that we have chosen Filecoin in this example in part because we have no connection to its activities.

55. Protocol Labs, FILECOIN: A DECENTRALIZED STORAGE NETWORK (Aug. 14, 2017), https://filecoin.io/filecoin.pdf.

56. CoinList, FILECOIN TOKEN SALE ECONOMICS, https://coinlist.co/assets/index/filecoin_index/Filecoin-Sale-Economics-e3f703f8cd5f644aecd7ae3860ce932064ce014dd60de 115d67ff1e9047ffa8e.pdf (last visited July 26, 2018).
57. Hinman Speech; *see* Munchee Order; Jay Clayton, Chairman, Sec. & Exch. Comm'n, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.
58. Hinman Speech.
59. Jay Clayton, Chairman, Sec. & Exch. Comm'n, Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC, (Feb. 6, 2018), https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission. ("In short, prospective purchasers are being sold on the potential for tokens to increase in value with the ability to lock in those increases by reselling the tokens on a secondary market or to otherwise profit from the tokens based on the efforts of others. These are key hallmarks of a security and a securities offering.")
60. *See Gary Plastic* at 240–241.
61. *See* Hinman Speech ("Are the tokens distributed in ways to meet users' needs? For example, can the tokens be held or transferred only in amounts that correspond to a purchaser's expected use? Are there built-in incentives that compel using the tokens promptly on the network, such as having the tokens degrade in value over time, or can the tokens be held for extended periods for investment?").
62. *See id.* ("Is token creation commensurate with meeting the needs of users or, rather, with feeding speculation?").
63. *See id.* ("Has this person or group retained a stake or other interest in the digital asset such that it would be motivated to expend efforts to cause an increase in value in the digital asset?").
64. *Id.*
65. *See* Hinman Speech ("Are independent actors setting the price or is the promoter supporting the secondary market for the asset or otherwise influencing trading?").
66. *See id.* ("Are the assets dispersed across a diverse user base or concentrated in the hands of a few that can exert influence over the application?").
67. Simplystocks.com, SEC No-Action Letter (Feb 4, 1999).
68. SEC Staff Legal Bulletin No. 4 (Sept 16, 1997), https://www.sec.gov/interps/legal/slbcf4.txt.
69. Hester M. Peirce, How We Howey (May 9, 2019), https://www.sec.gov/news/speech/peirce-how-we-howey-050919.

David L. Concannon
Tel: +1 212 906 1389 / Email: david.concannon@lw.com

David Concannon is a partner in the New York office of Latham & Watkins where he is a member of the firm's Emerging Companies Practice. Mr Concannon is among a select few lawyers in New York whose practices focus exclusively on emerging companies, representing both clients as company counsel and venture capital firms as investor counsel. He advises emerging companies through their entire lifecycle, from formation through growth stages and exits. Mr Concannon spends substantial time advising market participants regarding cryptocurrencies and initial coin offerings, and serves as a Co-Chair of the firm's Blockchain and Cryptocurrency Task Force.

Yvette D. Valdez
Tel: +1 212 906 1797 / Email: yvette.valdez@lw.com

Yvette Valdez is a partner in the New York office of Latham & Watkins and a member of the Derivatives Practice, Financial Institutions Group, and FinTech Industry Group. Ms Valdez advises emerging companies, financial institutions, and investment managers on complex regulatory challenges in the development of bespoke financial crypto-asset and cryptocurrency technologies, including token sales, market infrastructure, trading, clearing, and settlement solutions on distributed ledger technology. She also advises clients on domestic and cross-border fintech initiatives in the derivatives markets. Ms Valdez also has significant experience representing dealers, intermediaries, and end-users in connection with derivatives (swaps and futures) legal and regulatory matters under the Dodd-Frank Act, the Commodity Exchange Act, as well as related CFTC, SEC, and prudential regulation.

Stephen P. Wink
Tel: +1 212 906 1229 / Email: stephen.wink@lw.com

Stephen Wink is a partner in the New York office of Latham & Watkins and a member of the Financial Institutions Group and FinTech Industry Group. Mr Wink is Co-Chair of the firm's Blockchain and Cryptocurrency Task Force. His practice focuses on advising a wide range of market players, including fintech companies, cryptocurrency issuers and platforms, investment banks, hedge funds, private equity firms, trading platforms, and other financial institutions. Mr Wink has in-depth knowledge and broad experience advising institutions on regulatory and related matters, gained in part from a decade as general counsel of a full-service investment bank.

Latham & Watkins LLP

885 Third Avenue, New York, New York 10022, USA
Tel: +1 212 906 1200 / Fax: +1 212 751 4864 / URL: www.lw.com

Custody and transfer of digital assets: Key U.S. legal considerations

Michael H. Krimminger, Colin Lloyd & Sandra Rocks
Cleary Gottlieb Steen & Hamilton LLP

Particularly since 2017, cryptocurrencies, initial coin offering ("ICO") tokens, and other similar financial assets ("Digital Assets") have drawn increased interest and participation from institutional investors. As with other financial assets, investors in Digital Assets face the risk of theft or loss of their holdings. This risk can be especially pronounced in connection with Digital Assets because transfers may not be easily reversible, intermediaries can be lightly capitalized, and other market participants are frequently anonymous or pseudonymous. These market characteristics underscore the importance of effective practices for the custody and transfer of Digital Assets. Unfortunately, the legal framework for such custody and transfer is evolving and not always well-understood.

This chapter summarizes that legal framework as it currently stands within the United States ("U.S.").[1] First, it describes certain aspects of how distributed ledgers operate, which are relevant to the mechanics for holding or transferring Digital Assets. It then describes the U.S. commercial and insolvency law considerations relevant to custodial relationships and transfers involving Digital Assets. Next, it summarizes the key U.S. regulatory frameworks currently applicable to Digital Asset custodians. Finally, it describes the proposed Uniform Regulation of Virtual-Currency Businesses Act (the "URVCBA"), which would make certain reforms in these areas.

Operation of distributed ledgers

The ownership and transfer of a Digital Asset is commonly recorded on a "blockchain" or other distributed ledger. Typically, distributed ledgers operate through the use of public and private keys.[2] The distributed ledger shows which public key owns each Digital Asset. To effect a transfer of a Digital Asset, the transferor needs to enter the private key that corresponds to the public key that the ledger shows as the owner of the Digital Asset. Private keys are created in mathematical relation to their public key pair and are unmodifiable. Participants in the distributed ledger validate transactions by confirming that the transfer has been authorized by the private key associated with the relevant public key.

Through the possession and use of a private key to validate Digital Asset transfers, every asset recorded on a specified distributed ledger may be transferred between different public keys. Without a public key's private key match, however, no assets held in connection with a public key may be transferred at all. As a result, Digital Asset investors must be able to effectively retain and protect such private key information, and thus control over all attached Digital Assets to protect their investments. Without security and control over all private key

information, investors are susceptible to both malicious attacks intended to obtain access to their private key—resulting in a malicious actor gaining the ability to transfer their Digital Assets and often leaving investors without recourse—and to losing possession of the private key and the ability to transfer their Digital Assets to or from any other person's public key in the future.

On a rudimentary level, Digital Asset investors have often looked to solve this problem with what are referred to as "wallets," which hold a private key for those investors and often require the use of a "passphrase" to subsequently access their private keys to transfer any Digital Assets. If investors choose to store their private keys in a "hot" wallet that is connected to the Internet, they face an increased risk of cyber-attack but may more quickly transfer Digital Assets to other parties. By contrast, maintaining private keys in an off-line, hardware-based "cold" wallet protects against cyber-hacking risks, but requires an investor's continued maintenance and possession of the hardware. Given some of the difficulties that investors may face in sufficiently managing all of these risks on their own, Digital Asset investors have frequently looked to some form of a centralized custodian to hold their assets.

Many investors have stored Digital Assets directly with the exchanges through which they trade. Many exchanges often maintain those assets in pooled, hot wallets that always remain connected to the Internet. While such storage solutions provide for faster access when an investor is looking to execute Digital Asset transactions on the exchange, hackers have increasingly succeeded at capitalizing on exchanges' vulnerabilities, including hot wallets' connections to the Internet, to steal large quantities of pooled Digital Assets from such exchanges. In those instances, investors have faced challenges in recouping their assets from the exchanges or otherwise. Other exchanges maintain both hot wallets for immediate transactions and cold wallets for longer-term custody. The cold wallets are usually wholly disconnected from the Internet and provide for far superior security.

Market participants have attempted to address these issues by providing Digital Asset custody services.[3] Such services often primarily or exclusively use cold storage wallets, holding all Digital Asset private keys in pooled accounts that are entirely offline until an individual investor wishes to withdraw or transfer their Digital Assets. This model provides investors with increased assurances in the safety of their private keys and Digital Assets, while also removing the additional work required of investors if they were to protect this information themselves.

Key U.S. commercial and insolvency law considerations

Custodial relationships

The characterization of the relationship between a holder of a Digital Asset and its custodian is a question of state law. Some key factors that may affect the characterization of the relationship include:

- What service is the custodian providing?
  - Is the custodian holding the holder's private key or the Digital Asset itself?
  - Has the custodian established a "multi sig" arrangement (i.e., an arrangement in which more than one key is required to authorize a Digital Asset transaction)? If so, does the custodian have all of the keys that are needed to allow the Digital Asset transaction to take place?
- How does the parties' agreement (if any) describe the relationship?
  - Does it call the relationship a bailment or another similar relationship such as some form of an agency?

- Does the documentation transfer any ownership of the private key or Digital Asset to the custodian or does the customer retain all right, title, and interest in the private key or Digital Asset?
- Does the custodian have the right to reuse the custodial assets?
- Is there an agreement to treat the private key or Digital Asset as a "financial asset"?

A custodial relationship could take many different forms, and the questions to consider will depend on the facts at hand. While the documentation will likely be crucial, it is not necessarily determinative.

Bailment or Similar Relationship. One possible way to frame the relationship between an owner of a Digital Asset and its custodian is as a bailment or similar relationship such as some form of an agency. A number of Digital Asset market participants have characterized their relationship as a bailment or similar agency relationship in order to ensure application of certain rights and duties discussed in greater detail below. A written or express agreement, however, is not necessarily required for a bailment or agency to be created. A court may conclude that the facts and circumstances demonstrate that a bailment or agency relationship was created. Such characterizations are more likely when the owner does not transfer to the custodian its rights in the private key or Digital Asset.

If the custodian is recognized as the bailee or agent of the customer, then the custodian would owe certain duties to the bailor or principal. Such duties include, if the custodian is recognized as a bailee, a duty to exercise ordinary care in keeping and safeguarding property of the bailor and if instead the custodian is recognized as the customer's agent, then the duties of obedience, loyalty, and care.

Although the rules governing the distribution of custodial assets upon the custodian's insolvency will depend on the applicable insolvency regime, many U.S. regimes, including the U.S. Bankruptcy Code, look to state law in the first instance to see whether the property is considered property of the custodian or instead property of the customer. If the latter, the assets will generally not be subject to claims of the custodian's general creditors. The way state law views property held subject to a bailment or similar relationship will depend on whether the property is fungible or not. For non-fungible property, the assets would be considered property of the customer and therefore, as long as the customer can substantiate the bailment or similar relationship and identify the relevant assets, its claim for the return of the asset will not be subject to the claims of the custodian's general creditors. State law also provides that fungible property held subject to a bailment or similar relationship is the property of the bailor, but that if there is a shortfall in the amount of a particular fungible asset relative to the claims of all bailors, the bailors will share *pro rata*.

While it appears unlikely that private keys would be considered fungible assets, the analysis is less clear for the Digital Assets themselves. For example, Digital Assets carried on particular blocks that make them sufficiently non-interchangeable may be non-fungible. However, if a custodian were to hold the Digital Assets in bulk with each customer owning a portion thereof, such Digital Assets could be considered fungible.

Securities Intermediary-Entitlement Holder Relationship. Another possible way to describe the customer-custodian relationship is as one between an entitlement holder and its securities intermediary within the purview of Article 8 of the Uniform Commercial Code as in effect in the applicable state ("UCC").

In the United States, the relationship between securities broker-dealers and their customers in respect of the customers' securities is generally subject to Article 8 of the UCC. However,

a broader range of relationships can fall within the scope of Article 8 if the asset being maintained is a "financial asset." An ICO token would likely be a financial asset by virtue of its status as a security.[4] Article 8 also allows parties to agree to treat an asset that is not a security as a financial asset so long as it "makes sense to apply the [duties in Part 5 of Article 8 of the UCC ("Part 5 duties")] to the relationship."[5] It is likely appropriate to apply the Part 5 duties to the custody of cryptocurrencies. For other assets recorded on a distributed ledger, one would have to analyze whether it would make sense to apply the Part 5 duties to the relationship based on the nature and properties of the asset, including whether the asset is transferable, generates payments or distributions, or provides holders with certain rights such as voting rights.

Overall, the benefit of electing to treat custodial assets as "financial assets" and thereby subject to Article 8 is that parties would then be able to have their relationship governed by a well-established legal regime that governs a very large market.

If the custodial relationship is subject to Article 8, then Part 5 of Article 8 imposes certain duties on the custodian as the securities intermediary, including a duty to maintain a sufficient quantity of the custodial assets to satisfy customer entitlements, a duty to comply with a customer's instructions, and a prohibition on granting security interests in the custodial assets without consent. In the absence of an agreement between the custodian and its customer as to which standard applies to the custodian in the exercise of its Part 5 duties, the custodian must exercise "due care in accordance with reasonable commercial standards."[6]

As in the context of a bailment or similar relationship, the rights of a customer in the event of the custodian's insolvency will depend on the applicable insolvency regime.[7] As mentioned above, most U.S. insolvency regimes look to state law to determine who has an interest in certain assets. However, the Securities Investor Protection Act ("SIPA"), which will likely govern the insolvency of a securities broker-dealer, provides that a securities customer will have a claim against the debtor based on its "net equity," which generally reflects all of the customer's securities positions and associated customer cash. To the extent this distribution rule applies, which it may in the case of ICO tokens held with a broker-dealer, a Digital Asset customer's claim for the return of its securities will share ratably with the claims of other securities customers and in priority to the broker-dealer's general creditors.

In the event the SIPA distribution rules do not apply and the insolvency regime points to state law, Section 8-503 of the UCC provides that financial assets held by a securities intermediary are not property of the securities intermediary and Section 8-511 of the UCC provides that the claims of entitlement holders would have priority over creditors except when the creditors have "control" over the financial asset. Section 8-503(b) further provides that each entitlement holder's property interest is a *pro rata* property interest in all interests of the securities intermediary in the particular type of financial asset that is being held for the entitlement holder by the securities intermediary.

Other Relationship Characterizations. If there is no bailee-bailor or similar relationship and no securities intermediary-entitlement holder relationship, then there might only be a contractual relationship. In the context of such other relationships, the custodian may not have any special duties, and if it enters into insolvency proceedings, the customer might only have an unsecured monetary claim (and not a claim to the actual custodial assets). However, this does not exclude the possibility that there are other relationships with legal import that might exist between the custodian and its customer.

Transfers of digital assets to third parties

In addition to determining the rights and obligations of a custodian of a Digital Asset and the Digital Asset owner, how a Digital Asset is held and the agreement governing the Digital Asset may have significant implications for the rights of any transferee of the Digital Asset. This is because the UCC's rules concerning perfection and priority differ for different asset categories and the nature and documentation of the custodial relationship may dictate which category a Digital Asset falls into. Most notably, while many Digital Assets would, absent an agreement to the contrary, likely be considered "general intangibles" for purposes of Article 9 of the UCC, an effective agreement between a custodian and customer to treat a Digital Asset as a financial asset would cause such asset to be "investment property" under Article 9, which is subject to very different priority and perfection rules.

Pledging. Perfecting a security interest in a general intangible requires filing a UCC financing statement, and the pledgee must be the first to file in order for its security interest in the Virtual Asset to have priority over the rights or interests of most third parties. In contrast, a security interest in investment property can be perfected by "control," and control affords enhanced priority. A secured party can obtain control by: (1) becoming the entitlement holder; (2) being the securities intermediary; or (3) entering into a control agreement.[8]

Sales. Whereas there are no commercial rules that provide for adverse claim cutoff protection for general intangibles in the context of sales, UCC Sections 8-502 and 8-510 provide that if a transferee of a financial asset gives value, acquires its interest without notice of any adverse claims and obtains "control," it will acquire its interest free of adverse claims.

Key U.S. regulatory considerations

Analyzing the regulatory status of a Digital Asset custodian begins with a categorization of the underlying Digital Asset. Generally speaking, as a matter of U.S. federal law, Digital Assets are viewed as either "securities" (as appears to be the case with most ICO tokens),[9] and thus subject to regulation by the Securities and Exchange Commission ("SEC"), or non-security "commodities" (as appears to be the case with Bitcoin and certain other cryptocurrencies),[10] and thus subject to regulation by the Commodity Futures Trading Commission ("CFTC"). In addition, certain state laws can apply to Digital Asset custodial activities.

Federal securities law considerations

The Securities Exchange Act of 1934 (the "Exchange Act") generally requires any person engaged in the business of effecting transactions in securities for the account of others (a "broker") to register with the SEC as a broker-dealer.[11] The SEC views handling customer funds or securities as a type of brokerage activity.[12] Accordingly, a person acting as a custodian for Digital Assets that are securities typically must register with the SEC as a broker-dealer. Among other regulations, registered broker-dealers are subject to extensive requirements related to the handling of customer funds and securities (which would include these Digital Assets), maintenance of minimum net capital, creation and maintenance of books and records, and anti-money laundering requirements.[13]

An exception from broker-dealer registration exists, however, for certain federal or state chartered or licensed banks engaged in custody or safekeeping activities.[14] These custodians are instead subject to banking law regulation of their custodial activities. Banking regulation for custodial or fiduciary activities by state and federal banks and trust companies, whether

insured by the Federal Deposit Insurance Corporation ("FDIC") or not, is designed to preserve the customer's interest in the property held by the bank or trust company for safekeeping. The trust departments of banks and trust companies are examined by the appropriate supervisory agency in order to require segregation and recordkeeping for trust assets, and those assets are treated exclusively as customer assets even in a failure of the bank or trust company.

In addition, federal securities law regulation of investors can obligate them to use certain regulated institutions as custodians for client assets. For example, Rule 206(4)-2 (the "Custody Rule") under the Investment Advisers Act of 1940 (the "Advisers Act") generally requires SEC-registered investment advisers that have custody[15] of client funds or securities[16] to maintain such funds or securities with a "qualified custodian," such as a bank or broker-dealer.[17] The qualified custodian must maintain an adviser's client funds and securities either in a separate account for each client in the client's name, or in one or more accounts containing only funds and securities of the client in the name of the investment adviser as agent or trustee for the client. Also, as investment advisers must have a "reasonable basis, after due inquiry, for believing that the qualified custodian sends an account statement, at least quarterly"[18] to each of the adviser's clients, such account statements are implicitly demanded of qualified custodians as well.[19]

Market participants have faced challenges complying with custodial requirements with respect to Digital Assets. For example, the limited availability of "qualified custodians" such as banks and broker-dealers that have the technological ability to custody Digital Assets may require SEC-registered investment advisers to consider issues not fully addressed by the Custody Rule.[20] Relatedly, SEC-registered broker-dealers with custody of client assets (including those who many consider offering custodial services to SEC-registered investment advisers) are required by Rule 15c3-3 under the Exchange Act to maintain "physical possession or control" of client securities. Staff of the SEC and the Financial Industry Regulatory Authority have noted several challenges that a broker-dealer may face in satisfying this requirement in connection with custody of Digital Asset securities, but suggested that they may, following an application to the SEC under Rule 15c3-3(c)(7), consider an issuer or transfer agent who publishes a distributed ledger to serve as a good "control location," so long as the authoritative record of ownership is established through a traditional master security list maintained by an issuer or a transfer agent, not by a distributed ledger.[21]

The Custody Rule does not apply to accounts of SEC-registered investment companies.[22] Rather, a separate set of requirements under Section 17(f) of the Investment Company Act of 1940 (the "Investment Company Act") and related rules govern how assets of SEC-registered investment companies must be held. Like the Advisers Act, the Investment Company Act requires either that registered investment companies use a regulated intermediary as a custodian or that they self-custody assets. Self-custody subjects registered investment companies to significant additional regulatory burdens, including surprise physical inspections by an independent public accountant and procedures that must be followed for the deposit and withdrawal of securities,[23] as well as recordkeeping requirements and the need to develop systems to facilitate trading. Section 17(f) of the Investment Company Act and the related rules allow registered investment companies to use, among other custodians, U.S. banks,[24] certain foreign banks,[25] and members of national securities exchanges.[26]

Federal commodities law considerations

Unlike the federal securities laws, the Commodity Exchange Act ("CEA") generally does not impose registration or licensing requirements on intermediaries, including custodians, providing services in connection with cash commodities, including Digital Assets traded on a spot or forward basis. Instead, substantive regulation under the CEA and CFTC rules thereunder typically extends solely to parties transacting in commodity-related derivatives, with CFTC jurisdiction over cash commodity market participants mostly limited to the enforcement of anti-fraud and anti-manipulation provisions of the CEA.[27]

Aspects of a custodial arrangement for Digital Assets can affect whether the CFTC views transactions in the Digital Asset to be cash market transactions or derivatives. For example, in the retail context, the CFTC has proposed to treat certain leveraged or margined transactions as a type of derivative if certain liens or transfer restrictions apply to the Digital Asset.[28] The CFTC has not finalized this interpretation, however, and a recent court decision (currently on appeal) casts doubt on it.[29] The CFTC has also not yet addressed how its other precedents distinguishing cash market transactions from derivatives apply to Digital Asset transactions.[30]

CFTC regulations can also apply to the custody of Digital Assets if they serve as collateral for CFTC-regulated derivatives. In particular, a party accepting customer funds or other property (such as Digital Assets) to secure a CFTC-regulated derivatives (other than an uncleared swap) typically must register with the CFTC as a futures commission merchant and satisfy CFTC customer segregation rules.[31] These segregation rules, in turn, require the futures commission merchant to deposit its customer's funds or other property in a segregated account held by a permissible depository, such as a bank, trust company, another futures commission merchant, or a derivatives clearing organization.[32]

State law considerations

At the state level, many jurisdictions similarly require that custodial services for customers' financial assets can only be provided by certain regulated persons. Many states similarly require some form of a bank, trust company, or other fiduciary charter to act as a fiduciary in performing such custodial duties. Additionally, many state laws limit such fiduciary powers either to federally-chartered entities or to entities chartered or regulated by that state. While reciprocity may be provided to out-of-state trust companies for certain activities, in some states the regular conduct of custodial and fiduciary activities may require separate licensing by the state where the customers reside.

In addition, New York requires licensing and oversight for custodial activities through the relatively extensive "BitLicense" framework introduced in 2015 or through its oversight of banks and trust companies. Persons who are "storing, holding, or maintaining custody of virtual currency on behalf of others" within the New York market are conducting "virtual currency business activity" within the jurisdiction,[33] and must either obtain a BitLicense from the New York Department of Financial Services ("NYDFS"), or otherwise fit an exemption by being chartered under New York Banking Law and approved by NYDFS to engage in such activity.[34] Persons operating as BitLicensees (as opposed to exempt, chartered institutions) are required to maintain a trust account with a "qualified custodian"—defined to extend only to a broad number of federal and New York banking entities in the state's relevant regulations—and must also hold Digital Assets of the same type and amount as any "owed or obligated" to another person for whom it is providing such custodial services. Thus, for any person seeking to provide Digital Asset custodial services of any kind involving New York markets, this additional regulatory hurdle is imposed.

In addition to state laws governing custodial relationships, it is important to note the central role played to date by state money transmitter laws in governing transactions in Digital Assets. State money transmitter licensing is frequently required for many Digital Asset activities, particularly for serving as an intermediary in fiat currency, virtual currency, and related transactions. While custodial activities may not be subject to the money transmitter laws, it is important to carefully consider the applicable statutory and regulatory language as well as any interpretative rulings by individual state regulators to define what is within the ambit of that state's money transmitter law.

Looking ahead: the URVCBA and Uniform Supplemental Commercial Law for the URVCBA and other state law initiatives

The URVCBA and the Uniform Supplemental Commercial Law for the URVCBA (the "Supplemental Act") are an initiative of the Uniform Law Commission intended to provide a state-level regulatory framework similar to that created by state money transmitter laws for entities that offer virtual currency[35] transfer, exchange, or storage services. The URVCBA has not yet been enacted by any state, although it has been introduced in California, Hawaii, Nevada, Oklahoma, and Rhode Island.[36] The Supplemental Act has also been introduced in each of these states except for Rhode Island.

The URVCBA

In order for a person to exchange, transfer, or store a virtual currency for purposes of the URVCBA, such person must have "control" over that virtual currency, which means the "power to execute unilaterally or prevent indefinitely a virtual-currency transaction."[37] In the context of a "multi sig" arrangement, a custodian may only have one of several private keys that are needed to effectuate a transaction in the relevant virtual currency, in which case such custodian would not have "control" over such virtual currency for the purposes of the URVCBA. However, certain entities are exempt from the URVCBA's requirements, including (1) federally- or state-chartered depository institutions; (2) broker-dealers or futures commission merchants provided that their virtual currency activities are ancillary to their securities or commodities business and they provide protections comparable to those contained in Section 502 of the URVCBA (discussed below); and (3) governments.

A person within the scope of the URVCBA needs to obtain a license from state authorities if the value of such person's virtual currency business activities exceeds a $5,000 *de minimis* threshold. The URVCBA, however, also creates an "on-ramp" or "lite" regime for entities whose virtual currency business activity is below a $35,000 threshold. Such persons still need to register with the relevant authorities and comply with certain requirements that are less onerous than those imposed on fully licensed persons.

Obligations applicable to licensees and registrants are similar to those imposed under money transmitter laws and include recordkeeping, disclosure, and business continuity planning obligations. Unlike money transmitter laws, however, Section 502 of the URVCBA requires licensees and registrants that have "control" over customers' virtual currencies to maintain "an amount of each type of virtual currency sufficient to satisfy the aggregate entitlements of the persons to the type of virtual currency." While this obligation is similar to that imposed on securities intermediaries under Part 5 of Article 8 of the UCC, Part 5 permits a securities intermediary and its customer to agree that a different rule will apply and also provides that this obligation will be displaced to the extent addressed by another statute or regulation. Section 502 also provides that virtual currency held by a licensee or registrant for a customer is not property of the licensee or registrant and will not be available to satisfy the claims of

such licensee's or registrant's creditors. Customers will share *pro rata* in the virtual currencies to which they are entitled.

The Supplemental Act

The Supplemental Act requires entities subject to the URVCBA to agree with their customers that virtual currencies controlled by such entities for such customers are to be treated as financial assets, which would mean that the commercial law rules for financial assets discussed above would apply to such virtual currencies. Notably, the Supplemental Act also provides that the agreement between a licensee or registrant and their customers cannot provide for a standard for the licensee or registrant to comply with its Part 5 duties that is less protective of the customer than the standard that applies under Part 5 when there is no agreement between the parties as to which standard applies (i.e., "due care in accordance with reasonable commercial standards"). The Supplemental Act further requires that the agreement between a licensee or registrant and its customer must state that the licensee or registrant will not grant a security interest in the virtual currency it is maintaining on behalf of its customer.

Other state law initiatives

Certain states have taken a different approach to address the commercial law treatment of Digital Assets. In particular, Wyoming enacted a statute[38] and Missouri has proposed a bill[39] that treat certain Digital Assets as "money" and others as "securities" for purposes of the UCC. It appears that one of the impetuses for these laws is to allow transferees to benefit from adverse claims cutoff rules without requiring the assets to be maintained with an intermediary. There are, however, concerns that these laws may conflict with existing UCC structures and engender difficult choice-of-law issues.

Conclusion

As with many issues involving Digital Assets, the laws and interpretations governing their custody and transfer continue to evolve. Current law generally was not designed to address Digital Assets and, as a result, is being adapted to fit this new asset class that, in some areas, fits imperfectly within existing legal frameworks and interpretations. Perhaps the only sure prediction is that the law will continue to evolve and, less certainly, continue to develop to promote greater certainty as Digital Assets themselves continue to evolve and play an increasingly significant role in the markets.

* * *

This chapter was prepared by Michael Krimminger, Colin Lloyd and Sandra Rocks, with the assistance of Marc Rotter, Brandon Hammer, Reshama Patel, Jim Wintering and Zachary Baum. The views expressed in this paper are solely those of the authors and do not necessarily represent the policies or views of Cleary Gottlieb or any of its partners. © 2019 Cleary Gottlieb Steen & Hamilton.

* * *

Endnotes

1. This chapter reflects legal developments as of July 9, 2019.
2. This chapter describes the typical operation of publicly accessible distributed ledgers, such as the blockchain used for Bitcoin. Other distributed ledger technologies,

especially permissioned (*i.e.*, "private") blockchains, can involve different mechanics for recording the ownership and transfer of Digital Assets.

3. *See, e.g.,* Olga Kharif and Sonali Basak, *Regulated Crypto Custody Is (Almost) Here. It's a Game Changer*, Bloomberg (June 18, 2018), https://www.bloomberg.com/news/articles/2018-06-18/regulated-crypto-custody-is-almost-here-it-s-a-game-changer.
4. UCC § 8-102(a)(9) defines a "financial asset" as, in relevant part, "(i) a security; or (ii) an obligation of a person or a share, participation, or other interest in a person or in property or an enterprise of a person, which is, or is of a type, dealt in or traded on financial markets, or which is recognized in any area in which it is issued or dealt in as a medium for investment."
5. *See* UCC § 8-102 cmt. 9.
6. *See* UCC §§ 8-504(c)(2), 8-505(a)(2), 8-506(2), 8-507(a)(2) and 8-508(2).
7. *See* UCC § 8-503 cmt. 1.
8. *See* UCC §§ 8-106(c), 9-106(a).
9. *See Framework for "Investment Contract" Analysis of Digital Assets* (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets ("[I]ssuers and other persons and entities engaged in the marketing, offer, sale, resale, or distribution of any digital asset will need to analyze the relevant transactions to determine if the federal securities laws apply."); *Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission*, 115th Cong. (Feb. 6, 2018) (Testimony of Chairman Clayton before the Senate Committee on Banking, Housing, and Urban Affairs, Washington D.C.) ("I believe every ICO I've seen is a security.")
10. *See In re Coinflip, Inc.*, CFTC Docket No. 15-29 (Sep. 17, 2015) ("Bitcoin and other virtual currencies are encompassed in the definition [of commodity under Section 1a(9) of the CEA] and properly defined as commodities."). Although questions have been raised regarding whether all Digital Assets qualify as commodities, or just those (such as Bitcoin) that underlie listed futures contracts, *see e.g.* Defs.' Opp'n. to Pl.'s Mot. for Prelim. Inj., *CFTC v. My Big Coin Pay, Inc.*, 1:18-cv-10077-RWZ at 7-10 (D. Mass. Apr. 3, 2018), two district courts have held that all Digital Assets are commodities within the meaning of the CEA. *CFTC v. My Big Coin Pay, Inc.,* 1:18-cv-10077-RWZ (D. Mass. Sept. 26, 2018); *CFTC v. McDonnell*, No. 1:18-cv-00361-JBW-RLM, slip op. (E.D.N.Y. Mar. 6, 2018).
11. Section 15(a)(1) of the Exchange Act.
12. *See* Definition of Terms in and Specific Exemptions for Banks, Savings Associations, and Savings Banks Under Sections 3(a)(4) and 3(a)(5) of the Securities Exchange Act of 1934, SEC Release No. 34- 44291 (May 11, 2001).
13. The application of these regulations to Digital Assets is not clear in many cases. For a high-level summary, *see* Financial Industry Regulatory Authority, *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*, https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf.
14. *See* Section 3(a)(4)(B)(viii) of the Exchange Act. Although most U.S. depository institutions clearly qualify for this exception, the status of other types of banks, such as state-licensed non-depository trust companies, is not as clear in all cases.

15. Custody is broadly defined as "holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them," and includes (i) possession of client funds or securities, (ii) any arrangement under which an adviser is authorized or permitted to withdraw client funds or securities held by a custodian upon instruction to the custodian, and (iii) access to client funds by virtue of an adviser's dual role as both general partner and investment adviser to a limited partnership or other such capacity. Rule 206(4)-2(d)(2) under the Advisers Act.
16. The SEC has not yet addressed whether or under what circumstances Digital Assets that are not securities remain subject to the Custody Rule as "funds."
17. The term "qualified custodian" is defined in the Custody Rule to include: banks or savings associations with deposits insured by the FDIC; broker-dealers registered with the SEC; futures commission merchants registered with the CFTC; and non-U.S. financial institutions that customarily hold financial assets for their customers, so long as they keep the advisory assets separate from their own.
18. Rule 206(4)-2(a)(3) under the Advisers Act.
19. Additionally, investment advisers that also serve as qualified custodians themselves must be subject to an annual surprise examination from an independent public accountant that is registered with and regularly inspected by the Public Company Accounting Oversight Board. Furthermore, that adviser must also obtain or receive from its affiliate an annual report prepared by such an accountant that covers all internal controls the adviser uses relating to providing custody services for client assets.
20. Staff of the SEC's Division of Investment Management has sought input on how and whether the unique characteristics of Digital Assets have affected compliance with the Custody Rule. *See* Letter from Paul G. Cellupica, Deputy Dir. & Chief Counsel, Div. of Inv. Mgmt. to Karen Barr, President & Chief Exec. Officer, Inv. Adviser Ass'n (Mar. 12, 2019), https://www.sec.gov/investment/non-dvp-and-custody-digital-assets-031219-206.
21. *See* Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities, Div. of Trading & Markets, U.S. Sec. & Exch. Comm'n and Office of Gen. Counsel, Fin. Indus. Regulatory Auth. (July 8, 2019), https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities. This staff statement also provided guidance regarding when a broker-dealer's business activities in Digital Assets might not involve "custody," as well as identifying considerations relating to books and records and financial reporting rules and the Securities Investor Protection Act that would be raised when a broker-dealer acts as custodian.
22. Rule 206(4)-2(b)(5) under the Advisers Act.
23. Rule 17f-2 under the Investment Company Act.
24. Section 17(f)(1) of the Investment Company Act.
25. Rule 17f-5 under the Investment Company Act.
26. Rule 17f-1 under the Investment Company Act. In addition, SEC-registered investment companies are able to deposit securities in securities depositories that meet certain requirements and hold assets with futures commission merchants and commodity clearing organizations in amounts necessary to effect certain types of transactions. *See* Rules 17f-4, 17F-6, and 17f-7 under the Investment Company Act.

27. For example, CFTC Regulation § 180.1 prohibits fraud and manipulation in connection with any contract of sale of any commodity in U.S. interstate commerce.
28. *See* Retail Commodity Transactions Involving Virtual Currency, 82 Fed. Reg. 60335 (Dec. 20, 2017).
29. *Commodity Futures Trading Comm'n v. Monex Credit Co.,* 311 F. Supp. 3d 1173 (C.D. Cal. 2018). The case on appeal is *Commodity Futures Trading Comm'n v. Monex Credit Co.*, case number 18-55815, in the U.S. District Court of Appeals for the Ninth Circuit.
30. For example, some of this precedent depends on whether a commodity is "nonfinancial," which in turn depends on whether ownership of the commodity can be conveyed in some manner and the commodity can be consumed. *See* Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement"; Mixed Swaps; Security-Based Swap Agreement Recordkeeping, 77 Fed. Reg. 48208, 48233 (Aug. 13, 2012). However, this precedent was intended to address environmental commodities, such as emission allowances, that do not provide good analogies for many Digital Assets.
31. *See* Section 4d of the CEA and CFTC Regulations §§ 1.20-1.30 (futures segregation rules), 30.7 (foreign futures segregation rules) and Part 22 (cleared swaps segregation rules).
32. *See* CFTC Regulations §§ 1.20(b), 22.4, and 30.7(b).
33. 23 NYCRR § 200.2(q).
34. *See* 23 NYCRR § 200.3(a)-(c).
35. The URVCBA uses the term "virtual currency" throughout, which is very broadly defined. *See* URVCBA § 102(23).
36. The URVCBA was also previously introduced in Connecticut and Nebraska, but not enacted by either state.
37. URVCBA § 102(3)(A).
38. 2019 Wyo. Sess. Laws 322 (to be codified at Wyo. Stat. §§ 34-29-101 to -105 and 34.1-1-210).
39. H.B. 1159, 100th Gen. Assemb., Reg. Sess. (Mo. 2019).

Michael H. Krimminger
Tel: +1 202 974 1720 / Email: mkrimminger@cgsh.com
Michael H. Krimminger is a partner based in the Washington, D.C. office of Cleary Gottlieb Steen & Hamilton LLP. Mr Krimminger advises domestic and international banking and financial institutions, as well as a variety of clients on fintech and related regulatory issues. Mr Krimminger joined Cleary Gottlieb in 2012 after serving for more than two decades with the Federal Deposit Insurance Corporation (FDIC), including as its General Counsel.

Colin Lloyd
Tel: +1 212 225 2809 / Email: clloyd@cgsh.com
Colin Lloyd is a partner based in the New York office of Cleary Gottlieb Steen & Hamilton LLP. He advises on securities and derivatives regulatory, legislative, transactional and enforcement matters. Mr Lloyd frequently counsels U.S. and non-U.S. broker-dealers, swap dealers, investment managers and other clients, as well as technology companies, on the application of U.S. securities and derivatives regulations to new technologies, including cryptocurrencies and distributed ledgers.

Sandra Rocks
Tel: +1 212 225 2780 / Email: srocks@cgsh.com
Sandra Rocks is counsel based in the New York office of Cleary Gottlieb Steen & Hamilton LLP. She advises on commercial and insolvency law in the context of financial market transactions, with a focus on the development and analysis of arrangements designed to mitigate credit risk and minimise adverse regulatory capital implications of various products, including digital assets.

Cleary Gottlieb Steen & Hamilton LLP

2112 Pennsylvania Avenue, NW Washington, DC 20037, USA
Tel: +1 202 974 1500 / Fax: +1 202 974 1999 / URL: www.clearygottlieb.com

An introduction to virtual currency money transmission regulation

Michelle Ann Gitlitz & Michael J. Barry
Blank Rome LLP

Introduction

The proliferation of virtual currencies has allowed individuals to effectuate fast, low-cost, seamless, and secure cross-border transactions. For regulators, the proliferation of virtual currencies and these transactions has also increased potential money laundering, terrorism finance, and consumer protection concerns. This chapter examines when businesses in the virtual currency arena may be obligated to comply with federal and state money transmission laws and regulations in the United States.

At the federal level, the Financial Crimes Enforcement Network ("FinCEN"), a division of the U.S. Department of the Treasury, is charged with protecting the financial system and combatting money laundering and terrorism financing. To carry out this mission, FinCEN manages the collection, processing, storage, dissemination, and protection of financial data, monitors transactions for suspicious activities, and institutes civil and criminal enforcement actions. For entities operating in this area, this means complying with a comprehensive regime of registration, customer due diligence, transaction monitoring, and reporting. At the state level, in addition to complying with the federal regime, any entity operating in the virtual currency arena must also consider the intricate and often ambiguous web of state money transmission laws. State money transmission regulations are not aimed at protecting against money laundering and terrorist financing; rather they focus on consumer protection to ensure that a money transmitter will not lose, steal, or misdirect the consumer's money. Virtually every state has its own money transmission licensing regime, which is obviously inefficient in the context of virtual currency, where technologies and products are designed to operate fluidly across state lines.

The maze of state licensing regulations paired with FinCEN's federal requirements demand thoughtful consideration of legal compliance for any person or business that operates in the virtual currency industry and may be considered a money transmitter.

Federal virtual currency money transmission

FinCEN exercises its regulatory authority pursuant to the Currency and Financial Transactions Reporting Act of 1970, as amended by Title III of the USA PATRIOT Act of 2001 and other legislation, all of which is commonly referred to as the Bank Secrecy Act ("BSA").[1]

The BSA requires that "financial institutions," businesses offering a wide array of broadly defined financial services, monitor their customers and their transactions and provide information about those customers and transaction to FinCEN.[2] These monitoring and reporting requirements include establishing Know Your Customer ("KYC") and Anti-Money

Laundering ("AML") programs and filing Suspicious Activity Reports ("SARs") and Currency Transaction Reports ("CTRs").[3] The data from these SARs and CTRs is analyzed by FinCEN for money laundering and terrorism finance risk and for other evidence of other financial crimes and is used in criminal, tax, and regulatory investigations and proceedings and in connection with certain intelligence and counter-terrorism matters.[4]

Whether an entity or individual meets the definition of a "financial institution" is determined by the type of activities in which that person or entity engages. The term "financial institution" includes any bank, broker or dealer of securities, or any person otherwise subject to supervision by any state or federal bank supervisory authority. For nonbanks, the term "financial institution" also includes "money services business" or "MSB."[5]

An MSB is any person or entity that engages in the following categories of financial activity: (1) dealing in foreign exchange; (2) check cashing; (3) issuing traveler's checks; (4) providing prepaid access; (5) selling prepaid access; and (6) money transmitting. Virtual currency cannot reasonably be analogized to check cashing or traveler's checks. And, in subsequent interpretative guidance, FinCEN has indicated that it will not consider persons participating in virtual currency markets to be dealers in foreign exchange or to be sellers or providers of prepaid access. Thus, the category of MSB that is most relevant to this chapter and to entities operating in the virtual currency arena is money transmitters.

The definition of the term "money transmitter" as contained in the applicable FinCEN regulations ("FinCEN Regulations") is copied below in its entirety.

A. "A person that provides money transmission services. The term "money transmission services" means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means. 'Any means' includes, but is not limited to, through a financial agency or institution; a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both; an electronic funds transfer network; or an informal value transfer system; or

B. Any other person engaged in the transfer of funds."[6]

Whether a person is a money transmitter, including those operating in the virtual currency arena, is a matter of facts and circumstances.[7] However, the term does not include any entity that engages in any of the following activities:

A. "Provides the delivery, communication, or network access services used by a money transmitter to support money transmission services;

B. Acts as a payment processor to facilitate the purchase of, or payment of a bill for, a good or service through a clearance and settlement system by agreement with the creditor or seller;

C. Operates a clearance and settlement system or otherwise acts as an intermediary solely between BSA regulated institutions. This includes but is not limited to the Fedwire system, electronic funds transfer networks, certain registered clearing agencies regulated by the Securities and Exchange Commission ("SEC"), and derivatives clearing organizations, or other clearinghouse arrangements established by a financial agency or institution;

D. Physically transports currency, other monetary instruments, other commercial paper, or other value that substitutes for currency as a person primarily engaged in such business, such as an armored car, from one person to the same person at another

location or to an account belonging to the same person at a financial institution, provided that the person engaged in physical transportation has no more than a custodial interest in the currency, other monetary instruments, other commercial paper, or other value at any point during the transportation;

E. Provides prepaid access; or

F. Accepts and transmits funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds."[8]

Because the foregoing definitions and exemptions offer little in the way of clarity for entities engaged in virtual currency activities, the most relevant resource is subsequent guidance issued by FinCEN specifically on virtual currencies (collectively, the "FinCEN Guidance").

FinCEN Virtual Currency Guidance

FinCEN Guidance first addressed virtual currencies in March 2013.[9] In this Guidance, FinCEN indicated that it would regulate transmitters of virtual currency in the same manner as transmitters of fiat currency.

Under FinCEN Regulations, fiat currency (also referred to as "real" currency) is defined as "the coin and paper money of the United States or of any other country: (i) that is designated as legal tender; (ii) that circulates; and (iii) is customarily used and accepted as a medium of exchange in the country of issuance."[10] Alternatively, under FinCEN Guidance, "virtual currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency."[11]

The March 2013 FinCEN Guidance also drew an important distinction related to the convertibility of the virtual currency. FinCEN defined "convertible virtual currency" ("CVC") as any currency having either "an equivalent value in real currency, or acts as a substitute for real currency."[12] CVCs have been the focus of FinCEN Guidance and entities that operate platforms or models that implicate CVCs are presented with the greatest possibility of qualifying as a money transmitter. Nonconvertible virtual currencies on the other hand – those virtual currencies that cannot be converted to or sold for real currency and do not have any monetary value on the open market – likely do not implicate federal money transmission laws.

The Guidance also creates three categories of participants in the virtual currency ecosystem: users, exchangers, and administrators, described below.[13]

- **User**: A person who obtains virtual currency to purchase goods or services is a user.[14] This includes businesses that are strictly investing in convertible virtual currency for their own account and not for any other party.[15] Under the current Guidance, institutions investing in virtual currencies, such as co-mingled investment funds, are likely considered users. The method of obtaining virtual currency (e.g., "earning," "harvesting," "mining," "creating," "auto-generating," "manufacturing," or "purchasing") is not determinative of whether a person qualifies as a "user," an "administrator" or an "exchanger."[16]
- **Exchanger**: A person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency is an exchanger.[17] Importantly, a person must be engaged in a business; thus, trading simply for personal investment purposes does not qualify one as an exchanger. In addition, one must accept and transmit virtual currency from one person to another or to another location. This covers transactions

where the parties are exchanging fiat and convertible virtual currency, and transactions where parties are exchanging one virtual currency for another virtual currency. However, the mere acceptance of virtual currency in exchange for providing a good or service does not make a person a money transmitter.

- **Administrator**: A person engaged as a business in issuing (i.e., putting into circulation) a virtual currency, and who has the authority to redeem (i.e., to withdraw from circulation) such virtual currency is an administrator.[18]

Users are not considered money transmitters, and thus are not required to register with FinCEN or otherwise comply with BSA regulations. Exchangers or administrators may be considered money transmitters and may be required to register with FinCEN and comply with BSA regulations. However, as indicated previously, this depends on the specific facts and circumstances of the entity's business model.

Classification of persons and entities conducting virtual currency business activities for money transmission purposes

Since issuing the Guidance in March 2013, FinCEN has issued subsequent Guidance on virtual currency that further informs the application of existing money transmission regulations to various business models in the virtual currency arena, including the following:

- *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014) (the "2014 Software and Investment Guidance");
- *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001 (Jan. 30, 2014) (the "2014 Mining Guidance");
- *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System*, FIN-2014-R012 (Oct. 27, 2014) (the "2014 Payment System Ruling"); and
- *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019).

Below is a summary of how the FinCEN Guidance might apply to various players in the virtual currency market.

- **Anonymizing Services**: Businesses providing anonymizing services (also known as "mixers" or "tumblers") that attempt to conceal the source of the transmission of virtual currency are money transmitters when they accept and transmit convertible virtual currency and, therefore, have regulatory obligations under the BSA.
- **Trading Platforms and Decentralized Exchanges**: Peer-to-peer ("P2P") trading platforms are websites where CVC buyers and sellers can connect. Sometimes, these platforms also facilitate trades as an intermediary. Under FinCEN Regulations, a person is exempt from money transmitter status if the person only provides the delivery, communication, or network access services used by a money transmitter to support money transmission services.[19] Therefore, if a CVC trading platform only provides a forum where CVC buyers and sellers post their bids and offers (with or without automatic matching of counterparties), and the parties themselves settle any matched transactions through an outside venue (either through individual wallets or other wallets not hosted by the trading platform), the trading platform does not qualify as a money transmitter under FinCEN regulations. By contrast, if, when transactions are matched, a trading platform purchases the CVC from the seller and sells it to the

buyer, then the trading platform is acting as a CVC exchanger, and thus falls within the definition of money transmitter and its accompanying BSA obligations.[20]

- **Software Developer**: The production and distribution of virtual currency-related software, in and of itself, is not money transmission services. Thus, an entity engaged in the activity is not a money transmitter, even if the purpose of the software is to facilitate the sale of virtual currency.[21]
- **Miners**: Miners play a vital role in allowing many decentralized blockchain-based virtual currency systems to operate properly. Mining is important because virtual currencies or tokens, such as Bitcoin, are initially acquired through mining; unlike paper money, decentralized virtual currencies do not have a central government to issue the currency. This provides a somewhat controlled way to distribute tokens and creates a real incentive for miners to enter the market. Miners also play another vital role: in the traditional banking system, banks maintain an accurate record of parties and details of each transaction; however, since there is no central regulator for decentralized virtual currencies, the miners assume this role.

  Those who mine virtual currencies, whether by "earning," "harvesting," "creating," or "manufacturing," are all classified as users and not money transmitters. Once the virtual currency is mined, a miner – depending on how he or she uses the convertible virtual currency and for whose benefit – may potentially become a money transmitter.[22] Just because the miner acquired the tokens directly by mining them, rather than purchasing or being given them, his or her status as a user is unaffected. Miners may use their mined tokens or currencies to purchase goods, and until they engage in activities that would qualify them as a transmitter, they remain a user.
- **Centralized Virtual Currencies**: A virtual currency that has a centralized repository is a centralized virtual currency ("CVC"). The repository of a CVC is a money transmitter to the extent that it allows transfers of value between persons or from one location (i.e., a user's account in New York) to another (i.e., that user's account in California). In addition, if the CVC repository accepts currency or its equivalent from a user and privately credits the user with an appropriate portion of the repository's own convertible virtual currency, and then transmits that internally credited value to third parties at the user's direction, the CVC repository is a money transmitter.[23]
- **Decentralized Virtual Currencies**: A decentralized virtual currency ("DVC") is a virtual currency that has no central repository and no single person who has the ability to issue or redeem the virtual currency. Persons may obtain the virtual currency through their own computing or mining effort or by purchasing the currency. A person who creates units of a DVC and uses it to purchase real or virtual goods and services is a "user" of the convertible virtual currency and is not subject to regulation as a money transmitter. By contrast, a person who creates units of a DVC, and sells those units to another person for real currency or its equivalent and is engaged in that transfer as a business, is a money transmitter to the extent that he or she is transferring it from one person or location to another person or location. A person who accepts and transmits real currency to one person in exchange for a DVC, but is arguably engaged in the business of providing goods and services, may have a valid argument that he or she is not a money transmitter. The exact scope of the regulation in this context is currently unclear.[24]
- **Natural Persons Providing CVC Money Transmission (P2P Exchanges)**: FinCEN defines an MSB to include both natural and legal persons engaged as a business in

certain activities, "whether or not on a regular basis or as an organized business concern."[25] P2P exchangers are generally natural persons engaged in the business of buying and selling CVCs. P2P exchangers facilitate transfers from one type of CVC to a different type of CVC, as well as exchanges between CVC and other types of value. P2P exchangers may provide their services online or in person. A natural person operating as a P2P exchanger that engages in money transmission services involving real currency or CVCs is a money transmitter and must comply with BSA regulations, regardless of the regularity or formality of such transactions or the location from which the person is operating. However, a natural person engaging in such activity on an infrequent basis and not for profit or gain would be exempt from the scope of money transmission.[26] As a money transmitter, P2P exchangers are required to comply with the BSA obligations that apply to money transmitters, including registering with FinCEN as an MSB and complying with AML program, recordkeeping, and reporting requirements (including filing SARs and CTRs).[27]

- **Wallets**: Wallets are secure virtual currency storage systems used to hold and potentially send or receive virtual currency. Most virtual currencies have official or suggested wallets and the use of a wallet is necessary. The wallet contains a public and private key for each virtual currency address. The private key is a secret number that allows the virtual currency to be spent. The public key is used to ensure that the wallet holder is the owner of the wallet address and can receive funds. The public key is mathematically derived from the private key. The status of a wallet as a money transmitter is primarily determined by whether the wallet company has custody of the private keys for the virtual currency.
- **Custodial Wallets**: Custodial wallet companies are likely money transmitters. They typically accept virtual currencies for users and transmit them when the currencies need to be moved. The custodial wallet is in full control of the transaction and the user cannot facilitate the transaction without the participation and action of the wallet provider. Examples of custodial wallet companies include Bitfinex, Bithumb and Coinbase.
- **Non-Custodial Wallets**: Non-custodial wallet companies are likely *not* money transmitters. These wallets never accept nor transmit virtual currencies; rather, they are a software tool. The user facilitates the transaction and neither the wallet nor the keys are ever in the possession of the non-custodial wallet company. This entity can be thought of as merely a developer of software used to aid the customer in facilitating his or her own transactions. Examples of non-custodial wallet companies include Jaxx, BitGo and Mycellium.
- **Multiple-Signature Wallet**: Multiple-signature wallets are enhanced security wallets that require more than one private key to effect transactions. Typically, the wallet owner maintains one private key while the multiple-signature wallet company maintains an additional key for validation. Generally, to effect a transaction from the owner's multiple-signature wallet, the wallet owner submits a request signed with the wallet owner's private key to the host company. Once the host company verifies this request, it validates and executes the transaction using its second key. If the multiple-signature wallet company restricts its role to creating non-custodial wallets that require adding a second authorization key to the wallet owner's private key in order to validate and complete transactions, the provider is not a money transmitter because it does not accept and transmit value.[28] However, if the company combines the services of a

multiple-signature wallet provider and a custodial wallet provider, that company will then qualify as a money transmitter. Likewise, if the value is represented as an entry in the accounts of the company, the owner does not interact with the payment system directly, or the company maintains total independent control of the value, the company will also qualify as a money transmitter, regardless of the label it applies to itself or its activities.

- **Custodial Exchanges**: Custodial exchanges are virtual currency exchange platforms on which users are able to buy and sell virtual currencies. What distinguishes this type of exchange as custodial is the fact that the exchange is in control of a user's funds, or in other words, the exchange is the custodian of the private keys for the virtual currencies or tokens. Examples of these types of exchanges include Coinbase, GDAX, Kraken, and Bitfinance. Custodial exchanges are money transmitters because they are both buying and selling and accepting and transmitting virtual currencies.
- **Non-Custodial Exchanges**: Non-custodial exchanges are virtual currency exchange platforms on which users are able to purchase and sell virtual currencies. What makes the non-custodial exchange different from the custodial exchange is that the exchange never takes possession of the user's virtual currency or private keys. Examples include Shape Shift and Evercoin. Non-custodial exchanges are likely not money transmitters but merely a source to help connect potential buyers with potential sellers, similar to a message or classifieds board like Craigslist. Because they are never in possession of the currency or private keys, they are never accepting or transmitting nor buying or selling virtual currencies.
- **Token Developers**: Token developers are the individuals who create a token platform and the virtual currency. Satoshi Nakamoto, the creator of Bitcoin, was the first to develop and release to the public a peer-to-peer digital currency platform. A token developer who either gives away his or her tokens or allows mining is simply distributing his or her software and, absent other facts, is not a money transmitter.[29] These token developers never accept and transmit tokens, but rather are simply developing and distributing the software in order to allow other users to operate peer-to-peer. Whether token developers are subject to regulation depends on the business in which they are engaged and whether they are a DVC or CVC, as discussed above.

  A token developer who sells virtual currency or tokens to users, rather than giving them away or allowing users to mine currency, is more complex. A miner who sells the currency he or she has mined and a developer who sells currency he or she has created should be treated the same. To date, the Guidance has not addressed these scenarios, and there is not yet any case law in the area. However, in FinCEN's first civil enforcement action against a virtual currency exchanger, Ripple Labs Inc., FinCEN alleged that Ripple Labs' currency, XRP, made the developer an exchanger subject to BSA regulation.[30]

  Ripple Labs settled, agreeing to a $700,000 penalty and to take certain remedial measures. This settlement is not precedential because it was a negotiated agreement. However, the allegations seemingly contradict the 2014 Software and Investment Guidance and make the treatment of token developers planning to sell their tokens somewhat unclear.
- **Token Issuers**: Although no official guidance has been issued, FinCEN has indicated that those who raise money through an Initial Coin Offering ("ICO") may also have to register as money transmitters. A February 13, 2018 letter from FinCEN to U.S. Senator

Ron Wyden of the Senate Committee on Finance (the "FinCEN Letter") states that FinCEN is working with the SEC and U.S. Commodity Futures Trading Commission ("CFTC") to enforce AML obligations of businesses engaged in ICOs.[31] FinCEN was careful to note that not all ICO issuers must register with FinCEN. Instead, whether an issuer must register depends on the nature of the financial activity involved.[32] The FinCEN Letter further states that a developer that sells convertible virtual currency such as Bitcoin (which has an equivalent value in fiat currency and can be exchanged back and forth for fiat currency), including in the form of an ICO, in exchange for another type of value that substitutes for currency, is a money transmitter and must comply with AML requirements. On August 9, 2018, FinCEN Director Kenneth A. Blanco stated in a speech that "[w]hile ICO arrangements vary and, depending on their structure, may be subject to different authorities, one fact remains absolute: FinCEN, and our partners at the SEC and CFTC, expect businesses involved in ICOs to meet all of their AML/CFT obligations."[33]

- **Payment Systems**: Virtual currency payment processing systems typically process payments and assist in executing transactions by accepting cash from the buyer, keeping that cash, and then paying the seller with the approximate market value of a virtual currency, or vice versa. By keeping a large reserve of virtual currency at all times, the payment processer is able to act as his or her own currency exchange to supply equivalent virtual currency for the cash supplied by the buyer.

  According to FinCEN, payment processing systems that accept and convert both real and virtual currencies are money transmitters because they are exchangers and, therefore, must register.[34] "An exchanger will be subject to the same obligations under FinCEN regulations regardless of whether it acts as a broker (attempting to match two (mostly) simultaneous and offsetting transactions involving the acceptance of one type of currency and the transmission of another) or as a dealer (transacting from its own reserve in either convertible virtual currency or real currency)."[35]

  There is, however, a carve-out from registration for payment processors when four conditions are met:

  (a) the entity providing the service facilitates the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself);

  (b) the entity operates through clearance and settlement systems that admit only BSA-regulated financial institutions;

  (c) the entity provides the service pursuant to a formal agreement; and

  (d) the entity's agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds.[36]

- **Bitcoin ATMs**: Generally, a fiat currency automated teller machine ("ATM") is not subject to FinCEN regulation as a money services business or money transmitter.[37] Fiat ATMs simply allow a consumer to access his or her own account and his or her own fiat currency. There is no exchange because most fiat ATMs are unable to transmit funds to third parties or accounts at other financial institutions.[38] Bitcoin ATMs, however, are not merely an intermediary between a consumer and his or her personal bank. Bitcoin ATMs function as either one-way (converting fiat currency to Bitcoin) or two-way (converting fiat currency to Bitcoin and Bitcoin to fiat currency) machines. In both instances, these machines may act as intermediaries between buyers and sellers – more as a broker than as a teller. Therefore, Bitcoin ATM operators generally must register with FinCEN as money transmitters.

- **Internet Casinos**: Internet casinos are virtual platforms that often accept bets and issue payouts denominated in CVC. Any internet casino that accepts and transmits value denominated in CVC may be regulated under the BSA as a money transmitter, in addition to any laws and regulations applicable to gambling.[39]

Registering as a money services business

Once established, money services businesses have 180 days to register with the U.S. Secretary of the Treasury.[40] Any company or individual serving as a money services business must file a FinCEN Form 107, along with an estimate of business volume for the coming year, information related to the business's ownership and control, and a list of its authorized agents.[41] FinCEN Form 107 requires money services businesses to identify the states in which they have agents and branches, the type of money services activities they plan to carry out (i.e., money transmitter, currency dealer or exchanger, check casher), the number of agents they have authorized to carry out each activity, and the location (financial institution and account number) of their primary transaction account.[42] If accepted, registration must be renewed every two years. If there is any change in ownership or control, transfer of a 10% voting or equity interest, or more than a 50% increase in authorized agents, then the business must re-register.[43]

Money services businesses must comply with recordkeeping, reporting, and transaction monitoring requirements under FinCEN regulations. Examples of these requirements include the filing of reports relating to currency in excess of $10,000 received in a trade or business whenever applicable,[44] general recordkeeping maintenance,[45] and, to the extent any transactions constitute "transmittal of funds" under 31 C.F.R. § 1010.100(ddd), then the money services business must comply with the "Funds Transfer Rule" (31 C.F.R. § 1010.410(e)) and the "Funds Travel Rule" (31 C.F.R. § 1010.410(f)). These requirements apply to both domestic- and foreign-located convertible virtual currency money transmitters, even if the foreign-located entity has no physical presence in the United States, as long as it does business in whole or substantial part within the United States.[46] Compliance requirements may vary depending on whether or not the business is a peer-to-peer exchange or a large, high-volume exchanger.[47]

Failure to comply with these requirements, including submission of false or materially incomplete information, can result in fines up to $5,000 per violation, or per day of a continued violation, and imprisonment of up to five years.[48] While registration is relatively easy, once registered, the compliance obligations are burdensome.

No action letters/requests for rulings to federal or state regulators

If a person or entity is clearly a money transmitter, then federal registration with FinCEN is required, as is potential state licensing, as discussed below. However, there may be situations in which it is unclear whether a person or entity must register as a money transmitter. In such circumstances, it is possible to use "no-action" letters or "requests for rulings" from federal and state regulators. These letters allow a person or entity to explain their business activity to the federal or state regulators to address unclear areas of the law, and to clarify whether particular business activities subject the person or entity to registration or licensing requirements under the federal or state regulatory regimes.

State virtual currency money transmission

State money transmission, unlike federal money transmission, requires licensure, not registration. As a prerequisite to receiving a license and/or in connection with maintaining

a license, states generally require some combination of the following: payment of licensing costs; bonding; minimum net worth requirements; disclosure of applicant employment history; submission to investigations or examinations; audited financials and periodic financial reporting; prior money transmission or financial services business experience; disclosure of litigation and bankruptcy proceedings; and fingerprinting and background checks.

Importantly, even if a person or entity is not a money transmitter under the BSA, they may be a money transmitter in any number of states, or vice versa.

A license is required in any state where the person or company does business, or solicits citizens, regardless of whether he or she or it has any physical presence in the state. Thus, any entity which is planning a global or nationwide rollout of its virtual currency business must satisfy state licensing requirements regardless of where the entity is physically located. Because virtual currency is a borderless medium of exchange, this typically requires an analysis of and possible licensure in all 50 states in the U.S and the District of Columbia.

Whether a particular entity is required to obtain a license in any state depends heavily on the specifics of the entity's business model. The below is meant to provide an overview of whether licensure may be required in a given state for entities engaged in certain virtual currency activities. For many states, we indicated that the state has taken no position on the applicability of its money transmission regulations to virtual currency businesses. However, in many of these states, a conservative reading of the definition of money (with is not necessarily limited to sovereign currency), monetary value (generally defined as "a medium of exchange, whether or not redeemable in money"), stored value (generally defined as "monetary value that is evidenced by an electronic record"), or a payment instrument (which generally includes "an electronic instrument or order for the transmission or payment of money whether or not the instrument is negotiable") would require a virtual currency business to obtain a license. In light of this, some virtual currency businesses have obtained a traditional money transmitter license in certain states. Any true analysis of applicable licensure requirements is inherently fact-specific, necessitating a detailed application of an entity's business model to the particular statutes and guidance in any given state. Due to these intricacies of state money transmission law and the uncertain applications of such laws to virtual currency activities, we recommend that you consult with counsel in determining whether state licensure is required.

State-level analysis

Alabama: Requires a license to transmit virtual currencies because virtual currencies are considered "monetary value" which is subject to regulation.[49]

Alaska: Requires virtual currency money transmitters to enter into a Limited License Agreement with the Alaska Department of Commerce, Community and Economic Development, Division of Banking and Securities.[50]

Arizona: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[51]

Arkansas: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[52]

California: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[53] California Assembly Bill 147, the Uniform Regulation of Virtual Currency Business Act, has not yet been passed.[54]

Colorado: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[55]

Connecticut: Requires a license to transmit virtual currencies.[56]

Delaware: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[57]

District of Columbia: The District has taken no position on virtual currency money transmission as of the date of publication of this chapter.[58]

Florida: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[59] In addition, in January 2019, in *State v. Espinoza*, 264 So. 3d 1055 (Fla. Dist. Ct. App. 2019), a Florida appellate court ruled that the state's money transmitter laws apply to a business engaging in the sale of Bitcoin because Bitcoin is a "payment instrument."

Georgia: Requires a license to transmit virtual currencies.[60]

Hawaii: Requires a license to transmit virtual currencies.[61]

Idaho: Entities that operate an exchange or trade platform that allows users to exchange one digital currency for another, but that do not allow trading in or deposits of fiat currency do not require a license; an entity which sells its own inventory of virtual currency does not require a license, but an entity which holds customer funds while arranging an exchange with a third party and that transmits virtual currency between the parties does require a license.[62]

Illinois: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[63]

Indiana: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[64]

Iowa: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[65]

Kansas: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[66]

Kentucky: The commonwealth has taken no position on virtual currency money transmission as of the date of publication of this chapter.[67]

Louisiana: Only entities operating as an exchanger are likely required to obtain a license to transmit virtual currencies.[68]

Maine: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[69]

Maryland: The state has suggested that it generally does not regulate virtual currency at this time.[70]

Massachusetts: The commonwealth generally does not regulate domestic money transmission. The state also exempts Bitcoin ATMs from "financial institution" and bitcoins from foreign currency transmission regulations.[71] Businesses involved in the dissemination of virtual currencies on the internet are "market place facilitators" subject to sales or use tax collection.[72]

Michigan: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter. Virtual currency transactions are exempt from sales tax and retailers are required to instantly convert the value of the virtual currency to U.S. Dollar as of the day and the exact time of the transaction.[73]

Minnesota: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[74]

Mississippi: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[75]

Missouri: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter, except that it exempts Bitcoin ATM transactions from sales tax.[76]

Montana: The state is the only U.S. jurisdiction that does not regulate money transmission.

Nebraska: The state has taken no current position on virtual currency money transmission as of the date of publication of this chapter.

Nevada: Bitcoin ATM kiosks must be licensed by the state and will require a surety bond requirement.

New Hampshire: The state exempts from licensure "persons who engage in the business of selling or issuing payment instruments or stored value solely in the form of convertible virtual currency or receive convertible virtual currency for transactions to another location."[77]

New Jersey: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[78]

New Mexico: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[79]

New York: A license (known as the BitLicense) is required by the New York State Department of Financial Services to engage in any "Virtual Currency Business Activity," which is broadly defined under the regulations, but has certain significant exemptions.[80]

North Carolina: Requires a license to transmit virtual currency.[81]

North Dakota: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[82]

Ohio: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.

Oklahoma: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.

Oregon: Requires a license to transmit virtual currency.[83]

Pennsylvania: The commonwealth has taken the position that certain virtual currency money transmission activities do not require licensure.[84]

Rhode Island: Effective January 2, 2010, the state will require a license and the provision of certain disclosures to transmit virtual currency and to engage in certain additional virtual currency activities.[85]

South Carolina: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter, but the South Carolina Attorney General has published frequently asked questions that disclose that further guidance with respect to the transmission of virtual currencies will be provided in the "near future."[86]

South Dakota: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.

Tennessee: Tennessee guidance provides that transactions solely involving exchanges of cryptocurrency are not money under the Tennessee Money Transmitter Act. Even the exchange of cryptocurrency for sovereign currency or the exchange of one cryptocurrency for another between two parties is not money transmission. However, the exchange of cryptocurrency for sovereign currency through a third-party exchanger is generally

considered money transmission. In addition, cryptocurrency ATMs may be considered money transmission under certain circumstances.[87]

Texas: The state has taken the position that certain virtual currency money transmission activities do not require licensure while other transactions, including those involving virtual currency ATMs, may require licensure.[88]

Utah: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.

Vermont: Requires a license to transmit virtual currency.[89]

Virginia: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[90]

Washington: Requires a license to transmit virtual currency.[91]

West Virginia: The state has taken no position on virtual currency money transmission as of the date of publication of this chapter.[92]

Wisconsin: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency under certain circumstances.[93]

Wyoming: The state exempts buying, selling, issuing, or taking custody of payment instruments or stored value in the form of virtual currency or receiving virtual currency for transmission from the Wyoming money transmitter licensure requirements.[94]

Attempts to standardize licensing practices

In an attempt to simplify the process and to create some uniformity and efficiency, seven states—Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas, and Washington—have come together to reach a level of reciprocity.[95] In early 2018, these states agreed that if one party state reviews key requirements of state licensing for a money transmitter applicant, including cybersecurity, background checks, and compliance with the BSA, then the other participating states will accept those findings in their own licensing process. This is the first real step toward an integrated 50-state system of licensure and supervision.

* * *

Acknowledgments

The authors acknowledge with thanks the contributions to this chapter by Michael Lupton, Gregory Cronin, Dustin Moaven, David Oberly and Justin Porter.

* * *

Endnotes

1. 31 U.S.C. §§ 5311-5332.
2. *Id.* § 5321(a)(2).
3. *See* FinCEN, BSA Requirements for MSBs, https://www.fincen.gov/bsa-requirements-msbs.
4. This data is also shared with foreign financial intelligence unit counterparts. FinCEN also shares its experience on virtual currency with foreign partners through the Egmont Group of Financial Intelligence Units ("FIU") and other international forums, with the

goal of helping FIUs to better advise reporting entities on what to report about virtual currency transactions or activity and other relevant information for revealing important methods and constituents involved in financing illicit activities.

5. 31 C.F.R. § 1010.100(t).
6. *Id*. § 1010.100(ff)(5).
7. *Id.* § 1010.100(ff)(5)(ii).
8. *Id*. § 1010.100(ff)(5).
9. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013) ("March 2013 Guidance").
10. *Id.* p. 1.
11. *Id.*
12. *Id.*
13. *Id.*
14. *Id.* at p. 2.
15. *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014).
16. *See also Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001 (Jan. 30, 2014) (clarifying that a user is a person that obtains virtual currency to purchase goods or services on the user's own behalf).
17. *Id.* at p. 2.
18. FIN-2013-G001 p. 2.
19. 31 C.F.R. § 1010.100(ff)(5)(ii)(A).
20. *See Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform*, FIN-2014-R011 (Oct. 27, 2014).
21. 2014 Software and Investment Guidance p. 2.
22. 2014 Mining Guidance.
23. FIN-2013-G001 p. 4.
24. FIN-2013-G001 p. 5.
25. 31 C.F.R. § 1010.100(ff).
26. 31 C.F.R. § 1010.100(ff)(8)(iii).
27. *See* FIN-2014-R002 (concerning the regulatory treatment of those persons investing in CVCs).
28. 31 C.F.R. § 1010.l0(ff)(S)(ii)(A).
29. *See* FIN-2014-R002.
30. *See* FinCEN, *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger: Company Agrees to $700,000 Penalty and Remedial Actions*, (May 5, 2015), https://www.fincen.gov/sites/default/files/2016-08/20150505.pdf.
31. The FinCEN Letter is not technically Guidance that must be followed, but the underlying regulations in the FinCEN Letter must be followed.
32. The FinCEN Letter appears to suggest that, at least in certain cases, virtual currency exchanges are subject to the BSA not because they are money services businesses, but because they are broker-dealers.

33. *See* https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block?utm_source=7-28-18+Member+List&utm_campaign=7b8d25b1ba-EMAIL_CAMPAIGN_2018_01_19_COPY_01&utm_medium=email&utm_term=0_e50a6ec6df-7b8d25b1ba-344964271#_ftn1 (accessed June 28, 2019).
34. 2014 Payment System Ruling.
35. *Id.*
36. 2014 Payment System Ruling p. 3.
37. *Application of the Definition of Money Services Business to Certain Owner-Operators of Automated Teller Machines Offering Limited Services*, FIN-2007-G006 (Dec. 3, 2007).
38. *Id.*
39. *See Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019). Casinos, as defined above, also have their own set of BSA/AML obligations. While not specifically exempted from MSB status, when a person falls under FinCEN's definitions of both casino and MSB, in general the regulatory obligations of a casino satisfy the obligations of an MSB, with the exception of registration.
40. 31 U.S.C. § 5330.
41. 31 C.F.R. § 1022.380.
42. *See* FinCEN Form 107 (Mar. 2011).
43. 31 C.F.R. § 1022.380(b)(4).
44. *Id*. § 1027.330.
45. *Id*. § 1027.410.
46. FinCEN pursued enforcement action against BTC-e, an internet-based virtual currency exchange and a foreign-located money services business, for failing to implement basic AML controls that enabled criminals to launder proceeds. FinCEN fined BTC-e $110 million and its administrator, Alexander Vinnik, $12 million – the largest individual penalty ever assessed by FinCEN. FinCEN partnered with the Department of Justice, which pursued BTC-e and Vinnik criminally.
47. *See* FinCEN, *BSA Requirements for MSBs*, https://www.fincen.gov/bsa-requirements-msbs.
48. 18 U.S.C. § 1960.
49. Ala. Code § 8-7A-1, *et seq.* (2018).
50. *See* https://www.commerce.alaska.gov/web/dbs/LimitedLicenseAgreementOrders.aspx (accessed June 28, 2019).
51. Ariz. Rev. Stat. Ann. § 6-1201, *et seq.* (2018).
52. Ark. Code Ann. §§ 23-55-101, *et seq*. (2018).
53. Cal. Fin. Code §2000, *et seq*. (West 2018).
54. Assembly Bill 1123 has been introduced for the second time into the California assembly, which proposes to enact the Virtual Currency Act to prohibit a person from engaging in any virtual currency business, unless licensed by the Commissioner or Business Oversight, or is exempt from licensure.
55. Colo. Rev. Stat. §§ 11-110-106, *et seq*. (2018). *See also* Interim Regulatory Guidance Cryptocurrency and the Colorado Money Transmitters Act, Colorado Department of

Regulatory Agencies, Sept. 20, 2018, https://blockchainlawguide.com/resources/2018-09-20---Interim-Regulatory-Guidance-Cryptocurrency-and-the-Colorado-Money-Transmitters-Act.pdf.

56. Conn. Gen. Stat. § 36a-595, *et seq*. (2018).
57. *See generally* De. Code Ann. tit. 5, §2303 (2018).
58. *See generally* D.C. Code §26-C22 *et seq*. (2018).
59. Fla. Stat. § 896.101, *et seq*. (2018). *See also*, Florida Declaratory Statement No. 2018-538, 91969 (Nov. 19, 2018).
60. Ga. Code Ann. § 7-1-680, *et seq*. (2018).
61. Haw. Rev. Stat. § 489D-1, *et seq*. (2018). *See also* Hawaii Division of Financial Institutions News Release: State Warns Consumers on Potential Bitcoin Issues, Feb. 26, 2014. Coinbase exited Hawaii in 2017, requiring Hawaiian customers to close their accounts, stating that it would be impossible for Coinbase to operate in the state given the reserve requirement for money transmitters in the statute.
62. Idaho Department of Finance, Letter Dated March 12, 2018.
63. 205 Ill. Comp. Stat. Ann. 657/1 *et seq*. (2018). *See also* Illinois Department of Financial and Professional Regulation, Digital Currency Regulatory Guidance (June 13, 2017).
64. Ind. Code §§ 28-8-4-1 *et seq.* (2018). *See also* Money Transmitter License New Application Checklist, Ind. Dep't of Fin. Inst., *available at* http://nationwidelicensingsystem.org/slr/PublishedStateDocuments/IN-DFI-Money-Transmitter-Company-New-App-Checklist.pdf (last updated Feb. 5, 2019).
65. *See generally*, Iowa Code §§533C.102 *et seq.* (2018).
66. Kan. Stat. Ann. §§ 9-508 *et seq*. (2018). *See Regulatory Treatment of Virtual Currencies Under the Kansas Money Transmitter Act*, Kan. Off. of State Bank Comm'r (June 4, 2014), *available at* http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf.
67. *See generally* Ky. Rev. Stat. Ann. §§ 286.11-001 *et seq*. (West 2018).
68. La. Stat. Ann. §§ 6:1031, *et seq.* (2018); *See Consumer and Investor Advisory on Virtual Currency*, La. Off. of Fin. Inst. (Aug. 2014), *available at* http://www.ofi.state.la.us/SOCGuidanceVirtualCurrency.pdf.
69. *See generally* Me. Rev. Stat. tit. 32, §§ 6101 *et seq*. (2018).
70. Md. Code Ann., Fin. Inst. §§ 12-401 *et seq.* (West 2018); *See Virtual Currencies: Risk for Buying, Selling, Transacting, and Investing – Advisory Notice 14-01*, Off. of the Comm'r of Fin. Regulation (Apr. 24, 2014), *available at* https://www.dllr.state.md.us/finance/advisories/advisoryvirtual.pdf.
71. Mass. Division of Banks, Opinion 14-004 (May 12, 2014). 63. 830 CMRH 1.7(b)(1).
72. Mass. Gen. Laws ch. 169, §§ 1 *et seq.* (West 2018); *See* Mass. Div. of Banks, Opinion 18-003 (June 14, 2018), *available at* http://www.mass.gov/files/documents/2018/06/21/Select%20Opinion%2018-003.pdf.
73. *See* Tax Policy Division of the Michigan Dept. of Treasury, Treasury Update, Vol. 1, Issue 1 (November 2015), *available at* https://www.michigan.gov/documents/treasury/Tax-Policy-November2015-Newsletter_504036_7.pdf (accessed June 28, 2019).
74. *See generally* Minn. Stat. §§ 53B.01 *et seq.* (2018).
75. *See generally* Miss. Code Ann. §§ 75-15-1 *et seq* (West 2018).

76. Missouri Dep't of Revenue, LR 7411, Collection of Sales Tax on Bitcoin Transfers Through an Automated Teller Machine (ATM), (Sept. 12, 2014).
77. N.H. Rev. Stat. Ann. § 399-G:3 (2018).
78. *See generally* N.J. Stat. Ann. § 17:15C *et seq.* (2018).
79. N.M. Stat. Ann. § 58-32-101 *et seq*. (2018). *See also Money Service Business: FAQ's*, N.M. Reg. & Licensing Dep't, *available at* http://www.rld.state.nm.us/financialinstitutions/faq-s.aspx.
80. 23 N.Y. Comp. Codes R. & Regs § 200. The New York State regulatory scheme has been the subject of much criticism and has resulted in an exodus of businesses from New York because of the costs and regulatory requirements associated with the BitLicense. As of the date of this chapter, 18 companies have been granted a BitLicense.
81. 51. N.C. Gen. Stat. § 53-208.41, *et seq.* (2018).
82. N.D. Cent. Code § 13-09-01 *et seq.* (2018). *See Frequently Asked Questions – Non-Depository: Money Transmitters*, N.D. Dep't of Fin. Insts. (2018), https://www.nd.gov/dfi/about-dfi/non-depository/frequently-asked-questions-non-depository.
83. Or. Rev. Stat. §§ 717, *et seq*. (2018).
84. *Money Transmitter Act Guidance for Virtual Currency Businesses*, Pa. Dep't of Banking and Sec. (Jan. 2019).
85. *See* R.I. H.B. 5847 (2019).
86. *See* South Carolina Attorney General, *Money Services Frequently Asked Questions*, *available at* http://www.scag.gov/money-services-frequently-asked-questions (accessed June 28, 2019).
87. *See* Memo, Tenn. Dep't of Fin. Inst., *Regulatory Treatment of Virtual Currencies under the Tennessee Money Transmitter Act* (Dec. 16, 2015) *available at* https://www.tn.gov/content/dam/tn/financialinstitutions/new-docs/TDFI%20Memo%20on%20Virtual%20Currency.pdf (accessed June 28, 2019).
88. *See* Texas Dep't of Banking, Supervisory Memorandum 1037, *Regulatory Treatment of Virtual Currency Under the Texas Money Transmitter Act, available at* https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf (accessed June 28, 2019).
89. Vt. Stat. Ann. tit. 8, §§ 2500, *et seq*. (2018).
90. 53. Va. Code Ann § 6.2-1900 *et seq*. (2018). *See also,* Va. State Corp. Comm., *Notice to Virginia Residents Regarding Virtual Currency*, *available at* https://www.scc.virginia.gov/bfi/files/virtcur.pdf (accessed July 25, 2019).
91. Wash. Rev. Code §§ 19.230.010, *et seq*.
92. W. Va. Code §§ 61-15-1 *et seq*. (2018).
93. Wis. Stat. § 217.01, *et seq*. (2018). *See also*, https://www.wdfi.org/fi/lfs/soc/ (accessed June 28, 2019).
94. Wyo. Stat. Ann., §§ 40-22-101 *et seq.* (2018).
95. *See* Conf. of State Bank Supervisors, *State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments*, (Feb. 6, 2018), *available at* https://www.csbs.org/state-regulators-take-first-step-standardize-licensing-practices-fintech-payments (accessed Aug. 5, 2019).

Michelle Ann Gitlitz
Tel: +1 212 885 5068 / Email: mgitlitz@BlankRome.com

Michelle Gitlitz is a securities lawyer who represents corporations, individuals, investment companies and funds in corporate, regulatory, and litigation matters. She co-leads Blank Rome's Blockchain Technology & Digital Currencies group and regularly advises companies as they bring blockchain technology applications to market, raise capital through coin/token issuances and digital securities offerings, establish digital currency mining operations, form private investment funds and hedge funds that invest in emerging technologies and digital currencies, and navigate through state and federal money transmission rules and regulations. Michelle is a frequent presenter on the legal and regulatory aspects of blockchain technology and tokenization. She has participated in MIT's Legal Forum for Artificial Intelligence and Blockchain and has lectured on blockchain and tokenization at MIT's Computational Law Course. Michelle also participated in the United Nations' Blockchain for Impact Global Summit. She is a member of the Wall Street Blockchain Alliance, Chamber of Digital Commerce, Global Legal Blockchain Consortium, and the Accord Project. She is also Vice Chair of Blank Rome's Women's Forum and is the co-founder of a non-profit, Diversity in Blockchain, Inc.

Michael J. Barry
Tel: +1 215 569 5494 / Email: mbarry@BlankRome.com

Michael Barry is a compliance attorney who advises bank and nonbank financial institutions on variety of regulatory and licensing issues. As a member of Blank Rome's Blockchain Technology & Digital Currencies group, he regularly counsels FinTech companies in connection with digital currency applications and other blockchain-based financial products. He is experienced in providing assistance with financial privacy disclosure obligations, drafting user agreements, and creating privacy policies. He also has experience advising clients on federal and state money transmission licensure issues, including assisting with licensure applications and drafting no-action letters. Additionally, Michael regularly advises regulated entities on compliance with obligations arising out of the Bank Secrecy Act, including anti-money laundering issues, suspicious activity reports, and know-your-customer policies.

Blank Rome LLP

1271 Avenue of the Americas, New York, NY 10020, USA
Tel: +1 212 885 5000 / Fax: +1 212 885 5001 / URL: www.blankrome.com

Cryptocurrency compliance and risks: A European KYC/AML perspective

Fedor Poskriakov, Maria Chiriaeva & Christophe Cavin
Lenz & Staehelin

Introduction

The rapid development, increased functionality, and growing adoption of new technologies and related payment products and services globally continue to pose significant challenges for regulators and private sector institutions in ensuring that these technologies are not misused for money laundering ("**ML**") and financing of terrorism ("**FT**") purposes. The underlying reasons for this are numerous and some of such risks were identified and discussed already in 2013 in the Financial Action Task Force ("**FATF**") NPPS Guidance,[1] even though the said report did not specifically refer to "virtual currencies" at the time.

In the last couple of years, a significant number of virtual currencies and other virtual assets ("**VAs**") have emerged and at least some of them attracted significant investment in payments infrastructure built on the relevant software protocols. These payment infrastructures and protocols seek to provide a new method for transmitting value over the internet or through decentralised peer-to-peer networks.

As decentralised, convertible cryptography-based VAs and related payment systems are gaining momentum, regulators and financial institutions ("**FI**") around the world are recognising that VAs and the underlying consensus protocols (1) likely represent the future for payment systems, (2) provide an ever-more powerful new tool for criminals, terrorist financiers and other sanctions-evaders to move and store illicit funds, out of the reach of law enforcement, and, as a result, (3) create unique new challenges in terms of ML/FT risks.[2] Although the global volumes and estimates are relatively low, Europol has estimated in 2017 that 3–4% of Europe's crime proceeds were laundered through cryptocurrencies – the proportion will likely continue to increase rapidly[3] due to the rate of adoption of VAs, including by institutional investors and FIs.

Given the trans-jurisdictional (or borderless) nature of the VA phenomenon, major institutions at the international level have all focused on and issued reports addressing VAs and the risks associated with them, including ML/FT risks. FATF and the European Banking Authority ("**EBA**"), in particular, have issued recommendations in this context, concluding that VA exchange platforms allowing the conversion of VAs into fiat money (and vice versa) are of particular relevance and must be brought within the scope of the respective national anti-money laundering and counter-financing of terrorism ("**AML/CFT**") frameworks. More recently, FATF adopted changes to its Recommendations to explicitly clarify that those apply to financial activities involving VAs and certain virtual asset service providers ("**VASP**").

Key potential risks

Key definitions and concepts

(a) *Definitions*

There is no single global definition of the term "crypto- or virtual currency". In 2012, the European Central Bank ("**ECB**") defined virtual currencies as "*a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*".[4] In 2014, the EBA defined virtual currencies as a "*digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a [fiat currency], but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically*".[5] In its 2014 report on key definitions on virtual currencies, FATF first gave the following definition: "*[T]he digital representation of value that can be digitally traded and functions as: (i) a medium of exchange; and/or (ii) a unit of account; and/or (iii) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.*"

In order to provide for a common regulatory approach through the fifth Anti Money Laundering Directive ("**MLD5**", see also "Current legal and regulatory regime, MLD5", below), the EU decided to adopt a definition of virtual currencies deriving from the FATF's 2014 guidance. According to MLD5, a virtual currency is defined as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically. Given the broad nature of this definition, it is likely that, in practice, most forms of VAs and other transferable cryptographic coins or tokens (as we know them today) fall within the scope of MLD5.

Finally, FATF updated its Recommendations in October 2018 and introduced the definition of VAs, now defined as a "*digital representation of value that can be physically traded, or transferred, and can be used for payment or investment purposes*" (but do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations).[6]

For the purposes of this chapter, we will adopt the definitions and conceptual framework set out in FATF's updated Recommendation.[7] In this respect, we will focus on decentralised convertible VAs and related payment products and services ("**VCPPS**"), to the exclusion of other VA-related securities and/or derivatives products and services, even though these are also relevant for ML/FT risk assessment, in particular crowdfunding methods like ICOs.

(b) *KYC and transaction monitoring*

Know Your Customer ("**KYC**") is the cornerstone of the AML/CFT due diligence requirements that are generally imposed on FIs whose AML/CFT legislation is aligned with international standards. KYC requirements are relatively recent, as they were first implemented in the 70s in both the Swiss and US legislations, before becoming an internationally recognised concept through the issuance of the FATF recommendations.

KYC requires that FIs duly identify (and verify) their contracting parties (i.e., customers) and the beneficial owners (namely when their contracting parties are not natural persons) of such assets, as well as their origin. Together with transaction monitoring, KYC ensures the traceability of assets, as long as those remaining in the financial system (i.e., paper trail) and allow the identification of ML/FT indicia.

Although KYC and transaction-monitoring requirements were globally implemented at a time when VAs did not exist, it appears to be clear today, based on the various initiatives both at the international and national levels, that the application of AML/CFT requirements to VCPPS remains to be clarified.

One of the challenges is that KYC and other AML/CFT requirements were designed for a centralised intermediated financial system, in which regulatory requirements and sanctions can be imposed by each jurisdiction at the level of financial intermediaries operating on its territory (i.e., acting as "gatekeepers"). By contrast, VCPPS rely on a set of decentralised cross-border virtual protocols and infrastructure elements, neither of which has a sufficient degree of control over or access to the underlying value (asset) and/or information, so that identifying a touch-point for implementing and enforcing compliance with AML/CFT requirements is naturally challenging.

Potential AML/CFT risks

It has to be recognised that like any money-transmitting or payment services, VCPPS have legitimate uses, with prominent venture capital firms investing in VA start-ups and developing infrastructure platforms. VAs may, for example, facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the internet. VAs may also facilitate international remittances and support financial inclusion in other ways, so that VCPPS may potentially serve the under- and un-banked.

However, most VAs by definition trigger a number of ML/FT risks due to their specific features, including anonymity (or pseudonymity), traceability and decentralisation. Many of those risks and uses materialise not on the distributed ledger ("**DL**") of the relevant VA, but rather in the surrounding ecosystem of issuers, exchangers and users. Rapidly evolving technology and the ease of new cryptocurrency creation are likely to continue to make it difficult for law enforcement and FIs alike to stay abreast of new criminal uses, so that integrating those in a solid KYC/client due diligence ("**CDD**") framework is a never-ending task.

In addition to potential illicit uses of VCPPS, the use of VAs may facilitate ML by relying on the same basic mechanisms as those used with fiat currency, with a significant potential for abuse of unregulated and decentralised borderless networks underpinning VAs. In a nutshell:

- **Placement**: VAs offer the ability to open a significant number of anonymous or pseudonymous wallets, at no or very low cost, something which is a low-risk method of rapidly placing proceeds of illicit activity.
- **Layering**: VAs enable the source of funds to be obfuscated by means of multiple transfers from wallet to wallet and/or their conversion into different types of VAs across borders. This allows for an easy layering without significant cost or risk, it being understood that recent technological developments such as "atomic swaps" may even further facilitate the misuse of VAs. Incidentally, substantial demand for unregistered ICOs may allow criminals (assuming they control the ICO) to hijack the popular crowdfunding mechanism to convert VA proceeds into other VAs and/or fiat currencies, while adding a seemingly legitimate "front" for the source of funds.

- **Integration**: the use of VAs to acquire goods or services, either directly or through the conversion of the VAs into fiat currency, is facilitated by the ever-increasing list of goods and services for which payment in VAs is accepted, as well as the entry into the VA markets of institutional players both for investment and trading (speculation) purposes, providing substantial liquidity in the VA markets and thereby potentially facilitating large-scale integration by abusing unsuspecting institution actors/investors. Likewise, ICOs with below-average KYC requirements may be abused by criminal actors who may be able to convert their illicit VA holdings into other tokens through subscribing to an ICO, and then exiting the investment immediately upon the relevant coins or tokens becoming listed on any VA exchange.

Naturally, AML/CFT risks are heightened among the unregulated sectors of the cryptocurrency markets. Given regulatory pressure to reject anonymity and introduce AML controls wherever cryptocurrency markets interface with the traditional financial services sector, there are new VAs being created to be more compatible with existing regulations.

However, until such time as novel technological solutions are in place, ML/FT risks are typically addressed by imposing strict AML/KYC requirements on "gatekeepers" such as VA exchangers and other FIs. However, according to the Impact Assessment of the European Commission of July 2016,[8] depending on the evolution of the network of acceptance of VAs, there might come a point in time when there will no longer be a need to convert VAs back into fiat currency if VAs become widely accepted and used. This presents a critical challenge in itself, insofar as it will reduce the number of "touchpoints" (i.e., conversion points from VA to fiat, exchangers, etc.) with the traditional intermediated financial services sector and thereby limit the opportunities for ML/FT risk mitigation through regulation of defined intermediaries. The updated FATF Recommendations, however, significantly extended the scope of entities subject to AML/CFT regulation by ensuring that not only VA activities that intersect with and provide gateways to and from the traditional regulated financial system (in particular VA exchangers) but also crypto-to-crypto exchange platforms, ICO issuers, custodial wallets and other related service providers be regulated for AML/CFT purposes (see "Current international initiatives, FATF" below).

Anonymity/pseudonymity

By definition, decentralised systems are particularly vulnerable to anonymity risks. Indeed, in contrast to traditional financial services, VA users' identities are generally unknown, although in most cases they are only pseudonymous, and there is no regulated intermediary which may serve as "gatekeeper" for mitigation of ML/FT risks.

The majority of VAs, such as *Bitcoin (BTC)* or *Ether (ETH)*, have anonymity or pseudonymity by design. The user's identity is not linked to a certain wallet or transaction. However, while a user's identity is not visible on the relevant DL underpinning the VA infrastructure, information on transactions, such as dates, value and the counterparties' addresses, are publicly recorded and available to anyone. For the purposes of their investigation and prosecution work, enforcement authorities are therefore able to track transactions to a point where the identity may have been linked to an account or address (e.g., wallet providers or exchange platforms).

Some VAs, such as Dash, Monero or Zcash, even go further, as they are designed to be completely anonymous: wallet addresses, transactions and information on transactions are not publicly recorded on the relevant DL and provide for a complete anonymity, preventing the identification of the legal and beneficial owner of the VAs.

In addition, a number of solutions have emerged that allow a certain enhancement to the anonymity and seek to limit traceability of transactions on otherwise pseudonymous VA networks. For instance, mixing services (also known as "*tumblers*" or "*washers*") aggregate transactions from numerous users and enable the actual paper trail of the transactional activity to be obscured. However, while the precise trail of individual transactions might be obscured, the fact that mixing activity has occurred is detectable on the relevant DL.

Traceability

Although the anonymous or pseudo-anonymous design of VAs is an obvious risk of ML/FT, the public nature of the DL acts as a mitigant by offering a complete transaction trail. The DL is an immutable, auditable electronic record of transactions whose traceability may, however, be limited due to user anonymity and anonymising service providers that obfuscate the transaction chain (see also "Technological solutions", below).

The traceability or "trail" risks may not be significant when dealing with a single DL or VA protocol. However, the situation becomes much more complex when considering cross-VA exchanges where it may not necessarily be possible to easily trace conversion transactions from one VA/DL to another, given that such tracing may require access to off-chain records of intermediaries or exchangers, which may be unregulated, and located in multiple jurisdictions. Likewise, with the emergence of technological solutions allowing for so-called "atomic swap", or atomic cross-chain trading, traceability will become an even greater challenge. In essence, it will allow users to cross-trade different VAs without relying on centralised parties or exchanges.

Decentralisation

Most VAs are decentralised, i.e., they are distributed on a peer-to-peer basis and there is no need for validation by a trusted third party that centrally administers the system. As noted by FATF, law enforcement cannot target one central location or entity (administrator) for investigative or asset-seizure purposes, and customers and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them.[9]

This problem is exacerbated by the rapidly evolving nature of the underlying DL technology and VCPPS business models. Without proper safeguards in place, transition from a VCPPS to the fiat financial system may be facilitated by unsuspecting VA exchangers and/or abused by complicit VCPPS infrastructure providers who deliberately seek out jurisdictions with weak AML/CFT regimes.

Legal and regulatory challenges

Current legal and regulatory regime

Despite calls for the adoption of global AML standards for VAs, no such uniform rules have yet emerged. However, we have seen some convergence toward the logical FATF view that VCPPS should be subject to the same obligations as their non-VA counterparts. In this respect, the majority of European jurisdictions that have issued rules or guidance on the matter have typically concluded that the exchange of VA for fiat currency (including the activity of VA "exchanges") is or should be subject to AML obligations.

Differences in national regulations include: (1) varying licensing requirements for VA exchangers and wallet services; (2) treatment of ICOs from an AML regulatory standpoint; and (3) the extent to which crypto-to-crypto exchange is treated differently from crypto-to-fiat exchange. In many cases, the regulatory status of these activities is either ambiguous or case-specific, and partially dependent on new legislation or regulation being adopted.

EU

VAs were first addressed at the EU level when the ECB published its VA report in October 2012. The ECB notably acknowledged that the degree of anonymity afforded by VAs can present ML/FT risks. The ECB further suggested that regulation "would at least reduce the incentive for terrorists, criminals and money launderers to make use of these virtual currency schemes for illegal purposes".[10]

In July 2014, the EBA issued a formal opinion on VAs, indicating in particular that VAs present high risks to the financial integrity of the EU, notably due to potential ML/FT risks. In its January 2019 report, however, the EBA noted that VA-related activity in the EU was regarded as relatively limited and that such activity does not appear to give rise to implications for financial stability.

MLD5

On July 5, 2016, the European Commission presented a legislative proposal to amend MLD4. The proposal was part of the Commission's Action Plan against FT, announced in February 2016. It also responded to the "Panama Papers"[11] revelations of April 2016.

MLD5 was adopted by the Parliament in plenary on April 19, 2018 and the Council of the European Union adopted it on May 14, 2018 as well. It was formally published in the EU's *Office Journal* on June 19, 2018, and entered into force on July 9, 2018. Member States will have until January 10, 2020 to amend their national laws to implement MLD5.

Among different objectives, MLD5 expressly aims at tackling FT risks linked to VAs. In this context, VA exchange platforms and custodian wallet providers have been added in the scope of MLD5. In order to allow competent authorities to monitor suspicious transactions involving VAs, while preserving the innovative advances offered by such currencies, the European Commission concluded that it is appropriate to include in the institutions subject to MLD4 ("obliged entities") all gatekeepers that control access to VAs, and in particular, exchange platforms and wallet providers,[12] as recommended by FATF in its guidance (see "Current international initiatives, FATF" below).

(i) *Providers engaged in exchange services*

Interestingly, MLD5 extends EU AML requirements to "providers engaged in exchange services between virtual currencies and fiat currency". As a result, most crypto-to-fiat (or fiat-to-crypto) exchanges will be covered by MLD5. However, crypto-to-crypto exchanges do not seem to be expressly covered by MLD5.

Notwithstanding this, it is still possible that certain crypto-to-crypto exchanges may fall within the scope of MLD5 if their activities are conducted by "obliged entities" for other reasons, such as custodian wallet services (see (b) below). Further, crypto-to-crypto exchanges could still be regulated at Member State level, depending on how each Member State incorporates MLD5's provisions into its national law, as well as the FATF Recommendations. Likewise, for the time being, it is not clear whether VA ATMs are covered under MLD5.

(ii) *Custodian wallet providers*

Custodian wallet providers are defined entities that provide services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer VAs. The definition appears to only include wallet providers that maintain control (via a private cryptographic key) over customers' wallets and the assets in it, in contrast to pure software wallet providers that provide applications or programs running on users' hardware (computer, smartphone, tablet…) to access public information from a DL and access the network (without having access to or control over the user's private keys).

Switzerland

The Swiss AML legislation does not provide for a definition of VAs, relying upon the FATF's definition used in its 2014 Report. That being said, since the revision of the Swiss Financial Market Supervisory Authority ("**FINMA**") AML Ordinance in 2015, exchange activities in relation to VAs, such as money transmitting (i.e., money transmission with a conversion of VAs between two parties), are clearly subject to AML rules. Before this revision took place, both FINMA and the Federal Council had already identified,[13] on a risk-based approach, the increased risks associated with VA exchangers and the necessity for them to be subject to AML requirements. As such, Switzerland was a precursor in the implementation of this rule, which has now become standard.

In a nutshell, the purchase and sale of convertible VAs on a commercial basis, and the operation of trading platforms to transfer money or convertible VAs from a platform's users to other users, are subject to Swiss AML rules. Before commencing operations, a provider of these kinds of services must either become a member of a self-regulatory organisation ("**SRO**") or apply to FINMA for a licence to operate as a directly supervised financial intermediary ("**DSFI**").

Because convertible VAs can facilitate anonymity and cross-border asset transfers, FINMA considers trading in it to have heightened ML/FT risks, requiring strict CDD, particularly as regards client identification, beneficial ownership and source-of-funds analysis.

Managing compliance AML/CFT risks

Although there are developments on the regulatory front in terms of strengthening requirements applicable to VCPPS providers, there has been practically no guidance by regulators to their respective domestic FIs as to how to approach KYC/CDD from an ML/FT risk assessment perspective when dealing with customers exposed to VA and VCPPS risks, other than a recommendation to adopt a prudent, risk-based approach.

In practice, as with any new line of business, type of client or financial transaction, the central AML/CFT compliance questions for FIs will be whether they: (1) understand the relevant risks; (2) can reasonably manage them; and (3) have the knowledge, tools and resources to do so on an ongoing basis (including policies, procedures, training programmes, etc.). FIs that choose to serve the new types of clients in the VA ecosystem should elaborate and put in place specific policies and procedures to ensure that they are able to comply with their AML obligations despite the VA context.

The specifics of each set of requirements will depend on the type of business, client type and jurisdiction, as well as other factors. That being said, the ability of FIs to confirm the identity, jurisdiction and purpose of each customer, as well as the assessment of the source of wealth and funds, is essential to the fulfilment of AML/CFT requirements. VCPPS actors as customers present specific challenges in each of these aspects, so that FIs must ensure that their policies and procedures allow them to perform these core functions with a degree of confidence which is at least equal to that which FIs would require for their traditional financial services.

Given the varying typology of VCPPS service providers, it is virtually impossible to draw up KYC/CDD standards, procedures and checklists that would be applicable universally. It is therefore understandable that regulators have not issued blanket guidance in this space. As the understanding of VCPPS and related AML/CFT risks evolves, it is likely that international standards and recommendations will emerge, and possibly compliance tools which will simplify the implementation thereof by FIs. In this respect, FIs, VCPPS

providers, developers, investors, and other actors in the VA space should seek to develop technology-based solutions that will improve compliance and facilitate the integration of VCPPS with the existing financial system.

Possible avenues to address compliance concerns

Current international initiatives

FATF

(a) Virtual Currencies – Guidance for a risk-based approach (June 2015 standards)

In June 2015, FATF issued a specific guidance on virtual currencies, focusing on the points of intersection that provide gateways to the regulated financial system – *Guidance for a Risk-Based Approach: Virtual Currencies* (the "**Guidance**"). This Guidance derives from previous reports of FATF, namely the June 2014 *Virtual Currencies Report* and the FATF NPPS Guidance of June 2013.

In accordance with the cardinal risk-based approach principle, the Guidance provides for a certain number of clarifications on the application of the FATF Recommendations to entities involved in VCPPS.

FATF is of the view that domestic entities providing convertible VA exchange services between VA and fiat currency should be subject to adequate AML/CFT regulation in their jurisdiction, like any other FI, and be subject to prudential supervision. In this context, the distinction between centralised and decentralised VAs is a key aspect for the purposes of the risk assessment to be performed. FATF recommends that entities involved in convertible and decentralised VCPPS be subject to an enhanced due diligence process, as such activities are regarded of higher risk due to the inherent anonymity element and challenges to perform proper identification (i.e., the underlying protocols on which the major part of the decentralised VCPPS are currently based do not provide for the participants' identification and verification) (see also "Anonymity/pseudonymity", above).

It is important to note that FATF does not recommend prohibiting VCPPS. On the contrary, such prohibition could drive such activities underground and lead to a complete lack of visibility and control over them. As a result, in case of prohibition of VCPPS, FATF recommends implementing additional mitigation measures, taking also into account the cross-border element in their activities.

As regards transaction monitoring, FATF is of the view that countries must ensure that originator and beneficial owner information is always included when convertible VA exchangers conduct convertible VA transfers in the form of wire transfers. Certain *de minimis* thresholds may, however, be implemented in order to exclude lower risk transactions. Transaction monitoring remains a key risk mitigant in the convertible VA world, as long as a conversion of VAs occurs.

(b) FATF Recommendations

FATF updated its Recommendations in October 2018 to address the rapidly evolving risks related to VAs and to clarify how the FATF Recommendations apply in the case of financial activities involving VAs, the updated Recommendations specifically address and target virtual asset service providers ("**VASPs**"), defined as any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual assets and fiat

currencies; (ii) exchange between one or more forms of virtual assets; (iii) transfer of virtual assets; (iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Those new definitions significantly expand the scope of entities subject to AML/CFT regulation since the June 2015 Guidance by ensuring that VASPs (not only fiat to VA exchanges but also crypto-to-crypto exchange platforms, ICO issuers, custodial wallets and other related service providers), be regulated for AML/CFT purposes, as well as licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. That being said, the above-mentioned definitions remain somewhat vague, and their interpretations remain to be determined.

(c) Interpretive Note to Recommendation 15

FATF adopted an Interpretive Note to Recommendation 15 on June 21, 2019, setting out requirements for effective regulation, supervision and monitoring of VASPs. Under this note, VASPs should be licensed or registered and be subject to effective regulation and supervision to ensure that they take the necessary steps to mitigate AML/CTF risks. To this end, VASPs should (1) be supervised or monitored by a competent authority (not a self-regulatory body), which should conduct risk-based supervision or monitoring and have power to impose a range of disciplinary and financial sanctions, and (2) adopt a number of preventive measures to mitigate ML and FT risks (including but not limited to CDD, record-keeping, suspicious transaction reporting and screening all transactions for compliance with targeted financial sanctions). In particular, VASPs should conduct CDD for occasional transactions above a USD/EUR 1,000 threshold. According to Paragraph 7(b) of the Interpretive Note, which was open for consultation, VASPs should obtain and hold required and accurate originator and beneficiary information in relation to VA transfers, and share this information with beneficiary VASPs and counterparts, as well as competent authorities (often referred to as the "travel rule"). Further, the specific requirements relating to wire transfers (such as monitoring the availability of information, taking freezing actions and prohibiting transactions with designated persons and entities) as set out under Recommendation 16 would apply on the same basis to transfers of VAs.

The Interpretative Note finally highlights the need for international cooperation and information exchange to prevent and combat ML/FT risks associated to VAs.

While the "travel rule" has been a longstanding requirement for FIs internationally, the implementation of this requirement for VASPs to collect and transfer customer information during transactions will undoubtedly present a challenge considering the very nature of DL technologies. Indeed, whereas FIs rely on established interbank communication systems (such as SWIFT, TARGET or SIC) to move funds and share information, no established communication system yet exists for VASPs and DL technologies – as they stand – usually only require a recipient address to effect a transfer, which renders difficult – if not impossible – ownership verification by VASPs and determination of whether the recipient address is managed by another obliged VASP or a non-custodial wallet which would fall outside the FATF Recommendations.

(d) Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019 Standards)

In June 2019, FATF published the *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, which builds upon the FATF's June 2015

standards on the risk-based approach ("**RBA**") to VAs and VASPs and which is intended to help both national authorities in understanding and developing regulatory and supervisory responses to VA activities and VASPs, as well as to help VASPs in understanding their AML/CFT obligations. Under the RBA and in accordance with paragraph 2 of the Interpretative Note, countries should identify, assess, and understand the ML/TF risks in relation to VA financial activities or operations and VASPs and focus their AML/CFT efforts on potentially higher-risk VAs. Similarly, countries should require VASPs to identify, assess, and understand the ML/TF risks. Finally, FATF indicated that it will monitor the implementation of the new requirements by countries and service providers and conduct a 12-month review in June 2020.

Latest discussions and developments

G-20

In its latest communication of June 8 and 9, 2019, the G-20 reaffirmed its commitment to applying the recently amended FATF Standards to VAs and related service providers for AML/FT purposes. It is likely that essentially the G-20 will continue to rely upon the FATF's position to ensure that global solutions are implemented at a broader level (through the 37 FATF Member States and the nine FATF-Style Regional Bodies).

Bank of International Settlement

In its statement on VAs of March 2019, the BIS recalled that VAs have exhibited a high degree of volatility and are considered an immature asset class given the lack of standardisation and constant evolution. In this respect, the BIS highlighted the various risks that VAs present for banks, including AML/CFT risk, but also liquidity, credit, market, operational, legal and reputation risks. Accordingly, the Basel Committee set out its prudential expectations related to banks' exposures to VSs and related services that banks must at a minimum adopt (such as conducting comprehensive analyses of the risks noted above, implementing a clear and robust risk management framework that is appropriate for the risks of VA exposures and related services). It is expected that the Basel Committee clarify the prudential treatment of such exposures to appropriately reflect the high degree of risk of VAs and is coordinating its work with other global standard setting bodies and the Financial Stability Board.

Creation of specific FIUs

The creation of specific Financial Intelligence Units ("**FIUs**") for VA-related transactions could be one of the measures to be implemented at national level which would have an impact at the international level. The cooperation between such specific FIUs would improve investigatory assistance and international cooperation in this respect (as stated in the Guidance).

Self-regulation & codes of conduct

Like Switzerland, certain jurisdictions attach great importance to self-regulation in the context of AML/CFT. Specific codes of conduct and self-regulations issued by SROs monitoring the compliance of affiliated FIs may be one of the measures that could be taken to address the ML/FT issue in relation to VAs, quickly and efficiently. FIs active in the sector of crypto-currencies, such as VA exchangers, could be specifically targeted by self-regulations adapted to their activities and providing for more clarity on their KYC and due diligence duties. Regulators and/or legislators could issue general guidelines and principles in this area, while specialised SROs could enrich them with detailed and practical recommendations until a consensus is found at the international level.

Central bank crypto-currencies

Based on the various statements and reports on VAs issued by central banks in different jurisdictions, it appears that central banks agree that VAs such as *BTC* and *ETH* are not meant to replace fiat currency. According to the *International Monetary Fund Global Financial Stability Report* dated April 2018, the use of crypto-currencies as a medium of exchange has been limited and their high volatility has prevented them from becoming a reliable unit of account. In this context, VAs do not appear to pose at present macro-critical financial stability risks, although if widely used, they may raise issues about, *inter alia*, ML and investor and consumer protection.

Notwithstanding the above, certain central banks (such as Riksbank, Norges Bank and the Bank of England) are currently contemplating issuing their own central bank crypto-currencies (the "**CBCC**") in order to take advantage of the dematerialisation of the currency (triggering costs reductions) and facilitate international transactions by avoiding currency exchanges issues and providing for instantaneous transfers. Other central banks are following the evolution of the developments of VAs closely, including the Swiss National Bank (SNB).

CBCCs could be viewed as a solution to mitigate the ML/FT risks, as the transactions related thereto would necessarily go through a regulated financial intermediary subject to AML/CFT regulations. This presupposes a new generation of centralised crypto-currencies which will not have the same level of anonymity and transferability as the current crypto-currencies. In this respect, it is worth noting that the Bank for International Settlements indicated in its March 2018 report, *Central bank digital currencies*, that the issuance of CBCCs could come, in addition to more efficient and safer payments and settlement systems, with some benefits from an AML/CFT perspective. To the extent that CBCCs allow for digital records and traces, it could indeed improve the application of rules aimed at AML/CFT. To date, we are not aware of central banks having issued their own CBCCs (with the exception of the specific case of Venezuela which has issued a state crypto-currency backed by the country's oil and mineral reserves (i.e., the petro)).

Technological solutions?

According to certain authors and actors active in the crypto-currency field, the specific features of DL technologies and protocols could be used to mitigate the ML/FT risks in relation to VAs. KYC, beneficial owner and transactional information could be registered and verified on a dedicated DL, in the form of a global network of unalterable information (or global data repository) that would be accessible by "gatekeepers" and law enforcement. This solution, although very promising at first sight, would raise significant technical and legal issues. Among the latter, one should mention the legal requirements in terms of data protection and, as the case may be, banking secrecy. Furthermore, the access to information and its use by public authorities such as criminal prosecution authorities would have to be strictly regulated in order to avoid any intervention outside the applicable mutual assistance channels. In this respect, and as one of the main challenges, such a private DL would need to comply with rules enacted at an international level by the jurisdictions whose FIs would be involved in such network. It appears, therefore, that there are a certain number of obstacles as of today to use DL technologies for AML/CFT purposes, especially in the absence, at this stage, of clear guidance and standards at the international level.

As mentioned in the FATF 2015 Report on VAs, other technical solutions may be available. Third party digital identity systems, as well as new business models, could be developed to

facilitate customer identification/verification, transaction monitoring and other due diligence requirements. In particular, in FATF's view, application programming interfaces ("**APIs**") that provide customer identification information, or allow FIs to set conditions that must be satisfied before a VA transaction can be sent to the recipient, could be used to reduce the ML/CTF risks associated with a VCPPS. A certain number of fintech companies have already started to develop technological AML solutions.

Conclusion

VCPPS are still in the early stages of development, but are gaining momentum. As adoption increases and innovation relevant to AML/CFT compliance becomes embedded in the VCPPS "genetics", we may witness the emergence of improved existing VA protocols or entirely new VAs, built on fundamentally different underlying principles that could include build-in controls, trusted "gatekeepers", digital identity interfaces and transaction monitoring.

Unfortunately, for as long as consistent and recognised standards and/or compliance tools are lacking, many legitimate actors in the VCPPS space will continue to be denied access to traditional banking services in a number of jurisdictions, and/or be "de-risked" by FIs. To the extent that international standard-setters, national regulators, FIs and VCPPS service providers and innovators recognise the opportunities and benefits of VCPPS globally, they should cooperate to define best practices and standards, as well as training programmes for the next generation of VA "compliance officers". Indeed, applying existing concepts and approaches tailored to an intermediated, centralised financial infrastructure simply does not work when transposed to VA ecosystems which abide by different rules and principles by design.

* * *

Endnotes

1. *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, June 2013, http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf.
2. Communication from the Commission of the European Parliament and the Council on an Action Plan for strengthening the fight against FT. Strasbourg, February 2, 2016.
3. Europol, *Drugs and the Darknet – Perspectives for Enforcement,* 2017.
4. European Central Bank, *Virtual Currency Schemes*, October 2012.
5. European Banking Authority, Opinion on virtual currencies, July 4, 2014.
6. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.
7. Available here: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
8. Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of ML or FT and amending Directive 2009/101/EC, July 5, 2016 ("**MLD4**").
9. FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2014.

10. Report of the ECB on Virtual Currency Schemes, October 2012.
11. The documents, some dating back to the 1970s, were created by, and taken from Panamanian law firm and corporate service provider Mossack Fonseca, and were leaked by an anonymous source.
12. European Commission, *Explanatory Memorandum*, proposal for a Directive of the European Parliament and of the Council amending MLD4.
13. Swiss Federal Council Report on Virtual Currencies, June 25, 2014.

Fedor Poskriakov
Tel: +41 58 450 71 31 / Email: fedor.poskriakov@lenzstaehelin.com

Fedor Poskriakov is a partner at Lenz & Staehelin in the banking and regulatory group in Geneva and specialises in banking, securities and finance law. He regularly advises on various regulatory, contractual and corporate matters. His practice covers banking, investment management and alternative investments, including private equity and hedge funds. He also advises on complex asset structuring and protection for business and private assets. His other practice areas include compliance advisory, internal investigations, private clients and fintech. Highlighted as a "Next Generation Lawyer" (*The Legal 500*, 2019), Fedor Poskriakov is recognised for his "impressive expertise in the Fintech space" (*Who's Who Legal*, 2019) and "his great understating of the blockchain technology itself, combined with his concrete experience in translating this into practice" (*Chambers*, 2019). Mr Poskriakov is admitted to the Bar in Geneva. He has a law degree (*lic. iur.*) from the University of Geneva.

Maria Chiriaeva
Tel: +41 58 450 70 00 / Email: maria.chiriaeva@lenzstaehelin.com

Maria Chiriaeva is a senior associate in the Banking and Finance group in Geneva and specialises in banking, securities and finance law. She regularly advises on various regulatory, contractual and corporate matters. Her practice covers banking, investment management and alternative investments. Her areas of expertise also include compliance advisory and internal investigations. Maria Chiriaeva is admitted to the Bar in Geneva. She has a Master's in economic law from the University of Geneva.

Christophe Cavin
Tel: +41 58 450 70 00 / Email: christophe.cavin@lenzstaehelin.com

Christophe Cavin works as an associate in the Geneva office and is a member of the Banking and Finance group and the Investigations group, respectively. His main areas of practice include banking and finance, regulatory, investigations, corporate, commercial and contractual matters. Christophe Cavin is admitted to the Bar in Geneva and New York. He has a Master's in commercial law from the University of Geneva and an LL.M. from the University of Pennsylvania Law School.

Lenz & Staehelin

Route de Chêne 30, CH-1211 Geneva 6 / Brandschenkenstrasse 24, CH-8027 Zurich, Switzerland
Tel: +41 58 450 7000 / +41 58 450 8000 / Fax: +41 58 450 7001 / +41 58 450 8001 / URL: www.lenzstaehelin.com

The potential legal implications of securing proof of stake-based networks

Angela Angelovska-Wilson, DLx Law
Evan Weiss, Proof of Stake Alliance

Introduction

A consensus mechanism is a fault-tolerant mechanism that is used in blockchain systems to achieve the necessary agreement on the single state of the network among distributed parties. The consensus mechanism is the system that allows a blockchain to function without the need to trust one single actor because agreement is reached by a number of different parties who all have the incentive to act fairly and in the best interest of the entire network.

The first consensus mechanism, Proof of Work ("PoW"), was described in the Bitcoin white paper and is utilized in the Bitcoin protocol.[1] In Bitcoin, the security of the network relies on a PoW algorithm in the form of block mining. Each node that wants to participate in mining is required to solve a computationally difficult problem to ensure the validity of the newly mined block; solutions are rewarded with bitcoins. The protocol is fair in the sense that a miner with p fraction of the total computational power can win the reward and create a block with the probability p.

Operation of the PoW protocol in Bitcoin is such that security of the network is supported by physically scarce resources: (i) specialized hardware needed to run computations; and (ii) electricity spent to power the hardware. This makes PoW systems inefficient from a resource standpoint. To increase their share of rewards, Bitcoin miners are compelled to engage in an arms race and to continuously deploy more resources in mining. While this makes the cost of an attack on Bitcoin prohibitively high, the energy intensive requirements of the Bitcoin protocol have resulted in proposals to build similar systems that are much less energy resource-intensive while still assuring the security and scalability of a distributed network.

In order to address the intensive energy resource requirements as well as network scaling in PoW systems, there has been a movement towards the development and implementation of different consensus mechanisms in distributed ledger networks. Some of the current consensus mechanisms under development include, but are not limited to: Proof of Elapsed Time ("PoET"); Proof of Authority ("PoA"); Proof of Capacity ("PoC"); Proof of Activity ("PoAc"); Proof of Burn ("PoB"); Delegated PoS; Practical Byzantine Fault Tolerance ("PBFT"); Federated Byzantine Agreement ("FBA"); Proof of Importance ("PoI"); and Direct Acyclic Graphs ("DAGs"). The most widely known and developing alternative to PoW consensus mechanism is Proof of Stake ("PoS").[2] While, as noted above, there are a number of other consensus mechanisms under development, the majority are based and designed as an improvement to either PoW or PoS.

PoS was initially suggested in 2011 and the first cryptocurrency to implement it was Peercoin in 2012.[3] The idea behind PoS is simple: instead of mining power, the probability to create a block and receive the associated reward is proportional to a user's ownership stake in the system. An individual stakeholder who has p fraction of the total number of coins in circulation creates a new block with p probability.

The rationale behind proof of stake is also fairly simple – users with the highest stakes in the system have the most interest to maintain a secure network, as they will suffer the most if the reputation and price of the cryptocurrency associated with the PoS network would diminish because of the attacks.

In PoS networks, miners are replaced with validators who are required to stake tokens in order to validate blocks. PoS networks, which may either have an infinite maximum supply or a finite supply of digital assets, mint new digital assets each time a transaction is added to its blockchain, also known as staking or inflation rewards ("Rewards"). Rewards act as the primary incentive mechanism to encourage participation in developing and validating transactions on PoS networks, which in turn, helps secure the network and attract new developers and users (i.e., foster "network effects").

In order to potentially earn Rewards, a digital asset holder will either, depending on the PoS network, (i) stake their own digital asset as collateral ("Principal"), (ii) delegate their transaction validation rights ("Validation Rights") to a staking as a service ("StaaS") provider, which allows the service provider to validate new transaction blocks of the underlying network and earn Rewards ("Staking") on the holders' behalf, or (iii) transmit the custody of their digital assets to a StaaS provider who posts the Principal and validates transactions on their behalf. Based on the design of the particular network, validators are incentivized to participate in good faith because they not only risk forfeiting the opportunity to earn Rewards (and suffer the effects of inflation while others earn Rewards), but also risk losing their digital assets/Principal if they act maliciously (i.e., through a "double spend" attack) or negligently (i.e., node(s) being offline) (collectively, "Slashing").

To incentivize digital asset holders to Stake and thus participate in securing network transactions, PoS networks have established Staking inflation rates ranging from 5–50% on an annualized basis.[4] Depending on the network and its particular implementation of PoS, staking can be both technically complex and time-consuming. There are security and technical complexities involved with establishing and maintaining a Staking operation and running validator nodes. Further, digital asset holders risk having their digital assets Slashed and/or Rewards lost if the Staking process is not properly managed. Understanding such complexities, some PoS networks (i.e., Tezos, Cosmos, Polkadot, Harmony, EOS) ("Delegated Proof of Stake Networks", or "DPoS") allow digital asset holders to Delegate their Validation Rights to a third party validator, while also allowing the asset owner to maintain custody of the underlying digital asset ("Delegation"). Thus, participants in these networks can self-custody their digital asset but Delegate their Validation Rights to a StaaS provider. Other PoS networks require the StaaS providers to take custody of the digital asset to validate transactions and earn Rewards ("Pure PoS").

In consideration for these Staking services, StaaS providers usually receive a percentage of the Reward earned by each client. Depending on the applicable network, Rewards will either be (i) sent directly to a StaaS provider controlled wallet, which the StaaS provider then distributes to the holder's original wallet address ("Non-Direct Network"), or (ii) held in a network distribution wallet and the holder will be required to submit an on-chain transaction to withdraw the Rewards ("On-Chain Network").[5] When interacting with On-Chain DPoS

networks, StaaS providers never control or transmit a token holder's virtual currency or Rewards. When interacting with Non-Direct DPoS or Pure PoS networks, StaaS providers will be required to transmit any earned Rewards (and in case of Pure PoS networks the initial Principal) back to the holder. The distribution of all Rewards will usually be sent to the wallet address which the holder initially delegated from.

The increasing use and implementation of PoS in various distributed ledger networks has added an additional layer of complexity to the legal and regulatory issues involved in the regulation of distributed ledger networks and cryptocurrencies including complex legal issues relating to regulatory status and treatment under existing laws, compliance (including valuation, custody and reporting), application of security laws, taxation, and anti-money laundering. In this chapter, we aim to address the application of U.S. federal securities and money transmission laws to PoS arrangements in which token holders Delegate their digital assets to StaaS providers who Stake on their behalf.

Securities law issues

The initial securities law question related to PoS networks is whether the Delegation of Validation Rights (or the custodying of digital assets is a Pure PoS network) is considered a security under Section 2(a)(1) of the Securities Act of 1933, as amended (the "Securities Act"). Section 2(a)(1) enumerates a list of instruments that constitute securities and includes "investment contracts". When an instrument or arrangement is not obviously one of the other items on the list of enumerated instruments, an investment contract analysis is conducted to determine if the instrument or arrangement is subject to the securities laws. In determining whether a transaction constitutes an investment contract, the SEC and courts apply the test set forth in the *SEC v. W.J. Howey Co.* (the "Howey Test").[6] Under the Howey Test, an investment contract is "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party."[7] The Howey Test "embodies a flexible rather than a static principle" and was designed to capture "the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits."[8]

Investment of money

The first element of the Howey Test requires that the participant provide an investment of money to the promoter. The term "money" captures more than traditional fiat currency; it also includes goods, services, promissory notes, and other "exchanges of value."[9] The Supreme Court provided additional context to this element of the test in *Marine Bank v. Weaver* when it stated that for an instrument to be a security, the investor must risk financial loss.[10]

The investment of money factor of the Howey Test ultimately requires a Network-by-Network analysis. Depending on the terms of the Delegation relationship and the Network being supported, some holders will never risk financial loss by Delegating to a StaaS provider. With certain DPoS Networks like Tezos, the holder only transfers its Validation Rights to the StaaS and does not transfer custody of the underlying digital asset. Additionally, in the Tezos Network, a large portion of validators post the Principal requirement themselves (which are the only digital assets subject to Slashing), so the holders who Delegate are not subject to Slashing risks. The holder is not exposed to any risk of losing their digital assets, but only the risk that he or she will not earn Rewards. If the holder abstained from Staking, they would, either way, forgo Rewards and suffer from Network inflation. In Networks without delegator Slashing and where the validators post the

Principal, there is no true risk of financial loss and thus the investment of money element is not met.[11]

In other Networks like Cosmos, however, holders are required to post Principal and thus may lose their self-custodied assets if a StaaS provider is Slashed during the Delegation period. These Networks are sometimes referred to as Bonded Proof of Stake Networks (collectively, "BPoS Networks"), and BpoS Networks are a subset of DPoS Networks.[12] However, based on currently available data, the probability of a holder being Slashed is low when delegating to a StaaS providers which have extremely high uptime rates and systems built to ensure that Slashing does not occur. In *Marine Bank*, the Supreme Court focused on the Court of Appeals' failure to provide sufficient weight to the crucial fact that the purchaser of a certificate of deposit is virtually guaranteed payment in full due to FDIC insurance.[13] As more data becomes available and PoS offerings further develop it is probable that an insurance coverage and other mechanisms are implemented that the chances of Slashing are so remote that a client is "virtually guaranteed payment in full."[14] Nevertheless, since there is still a chance that some amount of the client's digital assets could be lost, it is likely that a court would rule that the investment of money element of the Howey test is present with respect to BPoS Networks.

Additionally, in Pure PoS networks like Cardano, holders are required to transmit the custody of their tokens to the StaaS provider. These tokens will be subject to Slashing risks along with the risk that the StaaS provider never returns custody of the originally delegated tokens. Thus, it is very likely that a court would hold that a Pure PoS holder meets the investment of money element when Delegating their tokens.

Common enterprise

The SEC in their recently released Framework for "Investment Contract" Analysis of Digital Assets (the "Framework"), takes the position that "[i]n evaluating digital assets, we have found that a 'common enterprise' typically exists."[15] StaaS providers usually take a percentage of all earned Rewards and combine Validation Rights of holders. When taking into account the sharing of Rewards and the pooling of Validation Rights it is likely that a Delegation relationship will meet the common enterprise element of the Howey Test.

Expectation of profits

An "expectation of profit" generally means expected capital appreciation resulting from the development of the initial investment or expected participation in earnings resulting from the use of investor funds.[16]

As discussed herein, a holder's primary motivation to engage in Staking can be to withstand inflation and to secure the applicable Network rather than an "expectation of profits." If digital asset holders fail to Stake their interest in a Network, it is likely that the underlying relative value of those assets will decrease and ultimately the assets will become worthless if the Network is unsecured and subject to double spending and other malicious attacks that compromise the integrity of the immutability and fungibility of the Network's blockchain. Accordingly, it could be argued that the main objective for Staking may not necessarily be earning a "profit," but rather, securing the functionality and survival of the Network. Additionally, Rewards are designed as an incentive mechanism for digital asset holders to participate in securing the Network. If a holder chooses not to participate, his or her interest in the Network is diluted due to inflation as others participate and receive Rewards; however, as the percentage of holders participating in Staking approaches 100%, holders are less likely to return a profit and thus are more likely to continue Staking to protect their assets against network inflation losses.[17]

If StaaS providers or Networks advertise Rewards as a profit opportunity it is very likely that a holder would be reasonable in expecting a profit from Staking. Currently some StaaS providers advertise Staking opportunities with terms like "interest," "dividend" and "yield."[18] The use of these financial terms makes it much more likely that holder would engage and delegate their assets in hopes of earning profits. Analysis of this element of the Howey test is particularly fact-specific and dependent on the operation of a particular StaaS provider and the Networks they choose to support.[19]

From the efforts of others

The final element of the Howey Test asks "whether the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise."[20] The Supreme Court added this element after determining that investors do not need securities law protections if they can exercise control over the profit-generating activities so that their own efforts will determine whether or not the enterprise is successful.[21]

Purchaser primary purpose

Courts have examined a purchaser's primary purpose in interacting with a promoter (i.e., whether an investor intends to rely on a promoter to enhance an asset's value or whether the purchaser instead intends to rely upon market forces dictating the value in an underlying asset). In both *Noa v. Key Futures* and *SEC v. Belmont Reid and Co.*, the Ninth Circuit ruled that the Howey test was not met because purchasers of rare materials were not reliant on the seller of the materials for expected economic return but instead were relying on the market of the underlying materials.[22]

In both *Belmont* and *Noa*, there was a high probability that the natural resources would be obtained by the promoter and thus the expectation of profit by the purchaser was based on the market factors of the underlying commodities as opposed to the efforts of the promoter in obtaining them. However, in *SEC v. C. M. Joiner Leasing Corp.*, where the promoters of small acreage oil and gas leases agreed to drill a test well in the vicinity, the investors were speculating on the ability to find the commodity and relying on the promoters skill and expertise to test drill and identify it.[23] The Supreme Court held that an investment contract existed since the investors were paying a discounted price for the land and speculating on the success of the promoter for their profits.[24]

It can be argued that when holders choose to Delegate to a StaaS provider, their primary purpose is to further their interest as a stakeholder in the underlying Network. Similar to CMC's mining operation, StaaS providers are responsible for running the software that validates transactions and earns Rewards. In both cases, the client's motivation in engaging with the provider is based on the value of the underlying asset. Similar to how CMC acted as a seller, StaaS providers act as service providers for their clients. Like the Ninth Circuit's analysis in *Belmont*, if the risk of a service provider's non-performance was dispositive to the "efforts of others" element of the Howey Test, securities laws would apply to all prepaid service contracts. In all service relationships, there is a risk of non-performance by the provider; however, this concern is mitigated by contractual agreements and remedies, not securities laws. Unlike in *Joiner* where investors were speculating on the discovery of oil, currently StaaS providers are more akin to *Belmont* and *Noa*, where the probability of delivering the underlying asset is extremely high with a potential success rates of earning Rewards between 95–100%.[25] Moreover, based on the extreme volatility of the underlying digital assets,[26] it is unlikely that the majority of profit or loss will come from Staking since inflation rates currently average anywhere from 5–15%.[27] When analyzing these numbers

together, if holders have an expectation of economic return, it is likely based on market forces of the underlying digital asset and not from the efforts of the StaaS provider.

Digital asset holder's control

Another major factor courts have examined in regards to the "efforts of others" element is the control the participant is able to exercise over the enterprise.[28] If the participant is able to exert both practical and legal control over the enterprise, even if the participant chooses to Delegate such control, courts have been hesitant to rule that an investment contract exists.[29] Conversely, the courts are likely to find an investment contract exists where (i) the control of the investor over the investment is illusory, (ii) the investor lacks the skill or experience necessary to exercise control, or (iii) the investor is so dependent on the unique skill or expertise of the sponsor or manager that they cannot practically be replaced without affecting the success of the venture.[30]

DPoS Networks are designed to provide significant amounts of both legal and actual control to the holder when Delegating their assets. In Both *Williamson v. Tucker* and *Fargo Partners v. Dain Corn,* courts looked at the legal agreements between the parties to determine if the participant had a termination right or the ability to replace the party to whom they delegated power.[31]

Similarly to *Williamson*, *Fargo*, and *Perrv*, when interacting with a StaaS provider, holders usually have significant control over both their Validation Rights and custody of digital assets. The holder is only temporarily choosing to Delegate their assets to the StaaS provider for the sole purpose of Staking.[32] The client still retains control and decision making over their digital assets.[33] Per the terms of most Delegation agreements or StaaS providers' terms of service, a holder can revoke and terminate their Delegation at will.[34] If a holder is unhappy with their StaaS provider, finds a more desirable StaaS provider, wants to sell their digital assets, and/or no longer wishes to Stake their digital assets, the client can seamlessly revoke their Delegation and take back full control of their assets. However, it's important to note that with respect to BPoS and Pure PoS Networks, holders have less control over their assets. BPoS Networks have unbonding periods which could impact the timing of when the client is able to re-Delegate or transfer their digital assets.[35] The majority of the BPoS Networks possess unbonding periods of less than the 30 days referenced in *Fargo* and *Perrv*, further demonstrating that the holder has the necessary control over their Delegation.[36] Additionally, Pure PoS requires transferring custody of the underlying digital assets to the StaaS provider. The holder might have a contractual relationship with the StaaS provider that allows the holder to terminate the relationship at any time. However, since the StaaS provider will have custody of the assets, it makes the argument that the holder has the requisite level of control more difficult.

However, notwithstanding the *legal* ability to retain control and terminate the governing agreement, courts will examine the relationship between the parties to make sure the participant *actually has the skill or experience necessary* to exercise control. In *Albanese v. Florida Nat'l Bank* and *SEC v. Rubera*, although the participants had the legal ability to terminate their agreements with the promoters, courts found investment contracts existed because participants didn't have the actual ability to either service the property or find a replacement service provider.[37]

Holders who Delegate to StaaS providers not only usually possess the legal ability, but also the practical capacity to exert control over their digital assets.[38] Unlike the subject matter in *Rubera* and *Albanese*, which required domain knowledge, management skills and relationships, terminating a Delegation relationship for both BPoS and DPoS Networks is

simpler and only requires access to (i) the network via the internet, and (ii) a holder's private keys. Further, the process of terminating or transferring a Delegation is substantively similar to the process that a holder undertakes to Delegate to a StaaS provider. Thus, if a holder successfully Delegates to a StaaS provider, such holder would also have the required domain knowledge and ability to exert control over those same Validation Rights.[39]

Finally, courts will look at whether the investor is so dependent on some unique entrepreneurial or managerial ability of the sponsor or manager that the manager cannot be replaced.[40] The StaaS space is developing rapidly with a large number of competent service providers currently in operation. The services that StaaS operators provide are functionally similar, with industry best practices utilized for operating staking nodes and security. Validators may ultimately differentiate themselves from other providers through user experience, brand, price, and customer service. There are currently over 400 Tezos bakers and over 150 Cosmos validators, many of which can be viewed as competent providers of Staking services.[41] Accordingly, if a holder wishes to transition from one StaaS to another provider they will be able do so easily and obtain substantially similar services.

Securities-related policy considerations

Digital assets are novel and in many ways unlike other regulated financial products, thus they face interpretative obstacles in determining whether—and to what extent—existing regulations are applicable. As with any type of financial innovation, it is extremely important to examine the policy reasons behind the financial regulations to make sure they are applied properly to any offering of new financial products and services. Furthermore, the case law around investment contracts has stressed the importance of flexibility when the Supreme Court stated that "form should be disregarded for substance and the emphasis should be on economic reality."[42] While on its face, the Delegation relationship could be viewed as an investment contract, the economic realities of such transactions do not warrant the application of the securities laws, which would not necessarily further the interests of investor protection.

The Acts were passed in reaction to the Stock Market Crash of 1929 and the ensuing Great Depression. As stated on the SEC's website: "[t]he laws and rules that govern the securities industry in the United States derive from a simple and straightforward concept: all investors, whether large institutions or private individuals, should have access to certain basic facts about an investment prior to buying it, and so long as they hold it."[43] Rather than providing the SEC the authority to approve securities based on their merits, the Acts require that securities sold through a public offering be registered with the SEC and that the issuer disclose certain information to investors in connection therewith. The underlying premise of such a disclosure regime is that if investors have full and accurate information, they can make fully informed investment decisions.[44] Investors do not receive *all* information about a company, but rather *material* investment information.[45] Through issuer disclosure, shareholders are able to make informed decisions and hold boards of directors and management accountable for any misallocation or misuse of their invested funds. If they are displeased with management, they have the ability to change management behavior and the direction of the company by exercising their right to vote at annual and special shareholder meetings or sell their shares. The shares of stock the investors own represent an entitlement to the company's cash flows via dividends and it is therefore important that they receive financial information regarding the company in order for them to appropriately value their holdings.

Characterizing the Delegation relationship as an investment contract does not further the disclosure or investor protection principles of the Acts. Clients are not equity holders of StaaS providers and do not have any rights to the profits generated by the business. Clients choose to Delegate to StaaS providers because they need a trusted service provider. Having access to a StaaS' financial statements would not further the client's interests as the client is not an investor or equity holder in the StaaS. Moreover, because distributed ledger networks are based on transparency, there is a significant amount of public information regarding validators, which limits the information asymmetry problems most investors usually face. Through staking marketplaces, Network block explorers, community-run websites, and StaaS operator websites, clients have the ability to review performance statistics, payouts, fees, assets under delegation and information regarding StaaS management teams. The amount of current public information provides the necessary transparency for holders to choose a competent validator. Additionally, clients are able to verify payout records on the Networks so they can verify they received the full amount of Rewards owed to them.[46] Requiring StaaS operators to go through the costly and time-consuming registration process to serve retail holders would severely hinder innovation and competition in the United States, while also failing to provide a material impact on the protection of digital asset holders. Further, the high costs of registration and ongoing compliance would likely be passed on to holders in the way of increased fees.

Finally, when determining whether to apply federal securities laws, it is important to understand the relationship of the parties and how investors could be injured. If the Delegation Agreement and any similar contracts with third party StaaS providers are considered investment contracts, non-accredited digital asset holders would likely be unable to Delegate. Accordingly, digital asset holders may (i) Delegate to a non-U.S. based StaaS provider (who might not be a competent or trustworthy provider), or (ii) fail to Delegate their digital assets at all and subsequently suffer a depreciation in the value of their assets in a Network due to inflation. If the policy decision in the United States is to allow these unaccredited investors to buy, sell and use digital assets, then they should also have the ability to participate in securing the Networks and earning Rewards.

Money transmission issues

Over the last several years, one of the most significant legal issues that has arisen with respect to distributed ledger networks and virtual currencies is the application, licensing and compliance obligation with respect to money transmission laws and regulations. The initial money transmission question related to PoS networks is whether StaaS providers would be considered money transmitters under the Bank Secrecy Act ("BSA") and thus required to register as a Money Service Business ("MSB") with U.S. Financial Crimes Enforcement Network ("FinCEN") and obtain licenses in each of the states that require it.

In 1986, Congress enacted the Money Laundering Control Act ("MLCA"),[47] which established money laundering as a federal crime and introduced civil and criminal forfeiture for violations of the reporting and recordkeeping requirements under the BSA.[48] Over time, the BSA has grown and adapted in response to the evolution of the criminal money laundering system through the addition of mandatory identity verification procedures[49] and the development of anti-money laundering program ("AML Program"). The BSA and corresponding regulations ("BSA Regulations") are administered by FinCEN and subject banks and other financial institutions, including money services businesses MSBs, to a wide range of anti-money laundering obligations.

The BSA regulates persons (which includes both entities and individuals) that (i) provide money transmission services, or (ii) are "engaged in the transfer of funds."[50] "Money transmission services" is defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[51] Ultimately, whether a person provides "money transmission services" is a matter of facts and circumstances.

In 2013, FinCEN published guidance on the "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (the "2013 Virtual Currency Guidance"), which makes clear that FinCEN interprets "money transmission services" as encompassing products it refers to as "convertible virtual currency," and entities engaged in certain activities it deems "money transmission" involving such virtual currency.[52] On May 9, 2019, FinCEN issued guidance relating to how the Bank Secrecy Act (BSA) and its implementing regulations relating to money services businesses (MSBs) apply to certain businesses that transact in convertible virtual currencies ("2019 Virtual Currency Guidance") (together the 2013 Virtual Currency Guidance and 2019 Virtual Currency Guidance – "Virtual Currency Guidance"). The 2019 Virtual Currency Guidance consolidates existing FinCEN regulations and related administrative rulings and guidance issued by FinCEN since 2011, and then applies these rules and interpretations to common business models. Specifically, FinCEN focuses on whether participants in certain convertible virtual currency business models would be characterized as money transmitters for purposes of the BSA regulations or may be eligible for an exemption from the money transmitter obligations thereunder.

In brief, for an entity to be subject to MSB regulation within the parameters of the Virtual Currency Guidance, the threshold considerations are whether the entity provides "money transmission services" as an "Administrator" or "Exchanger" of a token that is a "convertible virtual currency." A convertible virtual currency is a virtual currency that has "an equivalent value in real currency or acts as a substitute for real currency."[53] We review the categories referenced in the Virtual Currency Guidance below:

Administrators

FinCEN defines an Administrator as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.[54] The Virtual Currency Guidance states that an administrator that "buys or sells convertible virtual currency for any reason is a money transmitter."[55]

Based on the requirements under the Virtual Currency Guidance, StaaS providers clearly ought not to be classified as an Administrator as they are not clearly not the virtual currency issuers and do not put virtual currency into circulation. StaaS companies are service providers that only interact with decentralized virtual currencies after they have been sold or issued.

Exchanger

The Virtual Currency Guidance defines an Exchanger of decentralized virtual currency as "a person engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currency."[56] In the Virtual Currency Guidance, FinCEN sets forth two situations when a person is an Exchanger of a virtual currency. First, "a person is an exchanger and a money transmitter if the person accepts such decentralized convertible currency from one person and transmits it to another person as part of the acceptance and

transfer of currency, funds, or other value that substitutes for currency."[57] Second, a person is an exchanger if the person "buys or sells virtual convertible currency for any reason, unless a limitation to or exemption from the definition applies."[58] The Virtual Currency Guidance goes on to state that "a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission and is a money transmitter;"[59] however, this proposition was qualified in subsequent letter rulings discussed below.

As stated above, the Department of Treasury ("Treasury") defines money transmission services as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[60] Treasury added the phrase "*to another person or location*" to the definition of "money transmission services" in 2011 to "explicitly convey that transactions involving the acceptance of currency from one person at one location and the return of that currency to the same person at the same location would not be considered money transmission service."[61]

When interacting with On-Chain DPoS Networks, StaaS providers would not provide money transmission services because they take no part in transferring virtual currencies. A holder Delegates their Validation Rights to a StaaS provider's Staking node. The StaaS provider then pools the Validation Rights of its all its clients and validates transactions on the Network. The Rewards earned by the StaaS provider are then sent to a Network controlled distribution wallet. At their discretion, the token holder can separately submit request transactions to the Network controlled distribution wallet and their portion of the earned Rewards will be sent directly to the wallet initially Delegated from.

When interacting with Non-Direct and Pure PoS Networks, a more detailed analysis is required. There is an argument that StaaS providers do not provide money transmission services when interacting with Non-Direct Networks because they do not transfer virtual currencies to another person or location. A holder Delegates their digital assets or Validation Rights to a StaaS provider's Staking node. The StaaS provider then pools the assets or rights of its clients and validates transactions on the Network. The Rewards earned by the StaaS are then sent the StaaS's controlled wallet. Once the StaaS receives a Reward in the StaaS-controlled wallet it distributes the Reward back to the client's original wallet address. In this instance, the StaaS provider could potentially make an argument that they are not transmitting virtual currency between multiple parties or locations but just between themselves and their clients since Treasury explicitly stated that transactions between two parties is not money transmission.

However, it is likely that FinCEN would take the position that the Rewards in Non-Direct or Pure PoS Networks are accepted by StaaS provider directly from the Network itself and then transmitted back to the client. FinCEN would likely argue the Network is the transmittor and the StaaS provider is the money transmitter executing the transaction between the Network and client.[62] Additionally, FinCEN has taken an extremely broad position on the what constitutes a "person" or another location.[63]

User

In the 2013 Virtual Currency Guidance, FinCEN described a User as "someone who obtains convertible virtual currency and uses it to purchase real or virtual goods or services."[64] A User is not an MSB under FinCEN's regulations.[65] In a subsequent ruling involving Bitcoin mining (the "Mining Ruling"), FinCEN provided additional guidance on what constitutes a User.[66] In the Mining Ruling, FinCEN explained that how a User "obtains a virtual currency

may be described using any number of ... terms" and emphasized that "what is material to the conclusion that a person is not an MSB is not the mechanism by which a person obtains the convertible virtual currency, but what the person uses the convertible currency for, and for whose benefit."[67] FinCEN then observed that Bitcoin mining "imposes no obligations ... to send mined Bitcoin to any other person or place for the benefit of another," and reasoned that to the "extent that a user mines Bitcoin and uses the Bitcoin solely for the user's own purposes and not for the benefit of another, the user is not an MSB under FinCEN's regulations."[68] FinCEN noted in particular that a "conversion transaction" – involving the conversion of the mined virtual currency for another virtual currency – does not render a person an exchanger so long as the transaction is done "solely for the user's own purposes and not as a business service performed for the benefit of another."[69]

FinCEN ruling FIN-2014-R002 and the Mining Ruling, both further clarify what constitutes for the benefit of another, when they reference previous rulings involving persons that would have been exempted from MSB status, "but for their payments to third parties *not* involved in the original transaction."[70]

StaaS providers could be considered a User under the Virtual Currency Guidance if they operate in a way in which they do not utilize Rewards for the benefit of anyone other than themselves.[71] Further, FinCEN's rulings state that transactions involving parties involved in the original transaction are exempt from MSB status.[72] The fact that the clients are the original party to the Delegation could provide evidence that the StaaS provider does not transmit for the benefit of third parties as described in the Mining Ruling.

Activity integral to sale of goods and services

FinCEN has carved out certain activities from the definition of "money transmission services." Of most relevance to StaaS providers is the activity integral to the sale of goods and services exemption. This is an exemption for entities that "accept and transmit funds integral to the sale of goods or the provisions of services, other than money transmission services by the person who is accepting and transmitting the funds."[73] The Virtual Currency Guidance provided additional color on the exemption in relation to virtual currency when it stated that the exemption is not applicable "when the *only* services being provided are money transmission services."[74] Specifically explaining that an Exchanger whose sole purpose is to connect a user with an Administrator to facilitate the purchase or sale of a virtual currency does not provide a service other than money transmission.

FinCEN has stated that there are three fundamental conditions that must be met for the exemption to apply:[75]

1. The money transmission component must be part of the provision of goods or services distinct from money transmission itself.
2. The exemption can only be claimed by the person that is engaged in the provision of goods or services distinct from money transmission.
3. The money transmission component must be integral (that is, necessary) for the provision of the goods or services.

FinCEN has provided some guiding posts on how these conditions are applied to different situations.[76] In FIN-2014-R004, FinCEN found that a company that offers escrow services to buyers and sellers of digital goods was not a MSB because the company's money transmission activities are necessary and integral to its provision of escrow services.[77] The escrow service company provided assurance that the buyer had enough resources to pay for the good and that the resources would not be released until the transaction was finalized (i.e. the buyer accepted and did not return the goods). FinCEN stated that acceptance and

transmission of funds did not constitute a separate and discrete service provided in addition to the underlying service of transaction management, but that they were a necessary and integral part of the service itself.

StaaS providers are service providers that offer a number of different software services including: security (state of the art multi-sig, encryption & authentication), customer service, software services (dashboard and interfaces), monitoring and alerting systems, and Reward audits and distribution (collectively, the "Services"). The process of Staking can be technically complex and there are significant operational risks which, if not mitigated, could result in the Slashing or loss of virtual currencies for holders. The breadth of service offerings and StaaS providers technical and operational expertise are among the reasons why clients decide work with StaaS providers as opposed to engaging in staking by themselves. Any transmission of virtual currency is a necessary step in order for the StaaS provider to fulfill its obligations to its clients and for the clients to generate the benefit of staking with the StaaS (i.e. receipt of their Rewards). StaaS providers services are similar to the aforementioned debt management company and escrow service provider. All three entities offer clients a service that allows them to more efficiently interact with third parties (i.e. the networks). The Services facilitate for the client the earning of Rewards. Any money transmission conducted by the StaaS provider is limited to transmitting Rewards to clients *in conjunction with* the staking delegation relationship entered into between the parties. Any money transmission activities are a necessary and integral part of the comprehensive Services.

In contrast, in FinCEN Ruling FIN-2008-R007,[78] FinCEN found that a company that accepted and transmitted funds in a confidential manner in order to protect a consumer's personal and financial information from a merchant when the consumer purchased goods or services was a money transmitter. This company, unlike a StaaS provider, played no active process in arranging, monitoring, verifying or endorsing the transactions that it processed. StaaS providers take an active role by (i) arranging the transactions by utilizing software to Stake the virtual currencies on the specific network, (ii) monitoring nodes to ensure they are online validating transactions, and (iii) endorsing transactions by continuously verifying transactions on that specific network to earn Rewards. The Services offered to clients provides clear evidence that StaaS providers offer and executes multiple services independent of money transmission.

As stated in multiple FinCEN rulings, a company must meet the three fundamental conditions in order to satisfy the activity integral to the sale of goods and services exemption. We review each condition as it applies to StaaS providers below.

The money transmission component must be part of the provision of goods or services distinct from money transmission itself

The general service StaaS providers furnish is to assist clients in Staking their PoS virtual currencies so that they can earn Rewards and not be injured by the inflation programmatically built into the Network. The delivery of Services occurs prior to any money transmission by the StaaS and thus those services (security, monitoring, and customer support) are separate from the money transmission itself. However, as discussed in more detail below, any transmission of Rewards is a key part of the Services and necessary for client to receive the benefit of engaging with the StaaS provider.

The exemption can only be claimed by the person that is engaged in the provision of goods or services distinct from money transmission

The StaaS provider is the party providing the Services to their clients. Therefore, the StaaS is able to claim the exemption due to the services it provides that are distinct from money transmission.

The money transmission component must be integral (that is, necessary) for the provision of the goods or services

As discussed above, the Services are composed of a number of different offerings which are required to properly and safely Stake virtual currencies. The transmission of virtual currency is necessary and integral to all the other Services provided otherwise the client would lose out to Network inflation and would not receive any Reward for staking their virtual currencies with the StaaS provider. The Services provide a way for clients to easily and reliably earn Rewards on their virtual currencies and, although the majority of Services are separate and distinct, money transmission is necessary for the client to receive the benefit of engaging with the StaaS provider.

2019 Virtual Currency Guidance

The 2019 Virtual Currency Guidance provided additional clarity applicable to StaaS providers in Section 5.4, which analyzes virtual currency money transmission performed by mining pools and cloud miners.[79] Mining pools are utilized by persons who combine their computer processing resources to form a group which then enhances the entire groups chances of receiving mining rewards.[80] Mining pools may be managed by a controlling persons (centralized pools) who acts as a leader of the pool (the "Group Leader") and claims the total amount of mining rewards issued to the group.[81] The Group Leader then distributes the in-kind mining rewards to the other pool members (presumably in proportion to the computer processing provided by such pool member).[82] The Group Leader usually takes a fee from the mining rewards for managing the pool. Prior to the 2019 Virtual Currency Guidance there was an open question of whether the Group Leader's distribution of mining rewards to pool members would be considered money transmission under the BSA.

The 2019 Virtual Currency Guidance provided clarity to this open question when it stated that in certain situations the Group Leader would not be taking part in money transmission activity as they are providing money transmission integral to the provision of services. "When the leader of the pool, the cloud miner, or the unincorporated organization or software agency acting on behalf of its owner/administrator transfer CVC to the pool members or contract purchasers to distribute the amount earned, this distribution *does not qualify as money transmission* under the BSA, as these transfers are integral to the provision of services (the authentication of blocks of transactions through the combined efforts of a group of providers, or through the equipment of the cloud miner)."[83] However, the 2019 Virtual Currency Guidance did go on to state that if the leader combines its managing and renting services with the service of hosting virtual currency wallets on behalf of the pool members then such activity would fall under FinCEN's definition of money transmission for engaging in account based money transmission.[84]

FinCEN's clarification and the application of the Activity Integral to Sale of Goods and Services exemption to mining pool operators makes it likely that the exemption would equally apply to StaaS providers. StaaS providers pool Validation Rights of their clients to authenticate blocks of transactions for PoS Networks. StaaS providers earn Rewards from the Network for correctly validating transactions. StaaS providers are then required to distribute those earned Rewards to clients after taking their service fee. StaaS providers relationships to its clients are almost identical to the relationship the Group Leader has with the mining pool members. Thus as long as StaaS providers do not host wallets on their clients behalf, it is very likely that the distribution of Rewards would not be considered money transmission under FinCEN's guidance.[85]

Conclusion

Existing PoS networks will continue to mature and as new PoS networks launch, it will be extremely important that regulators and policymakers provide clarity and guidance on the application of the myriad of laws and regulations as maybe applicable to PoS and SaaS. In addition to the application of U.S. federal securities and money transmission laws to PoS arrangements in which token holders Delegate their digital assets to StaaS providers who Stake on their behalf that we have addressed in this article, a number of additional complex legal issues will need to be addressed in order to assure the further development and innovation in PoS networks and for developers and service providers to have certainty as they design their networks and services in a regulatory compliant manner.

* * *

Endnotes

1. https://bitcoin.org/bitcoin.pdf.
2. https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ.
3. https://university.peercoin.net/#/9-peercoin-proof-of-stake-consensus.
4. Inflation rates are programmatically fixed in the network protocol. Some inflation rates are variable where the participation rate increases the inflation rate decreases (i.e. in Cosmos the inflation rate is set at a maximum of 20% but it gradually decreases as more token holders stake their tokens).
5. There are a few other variations of the Reward payout mechanism; however the two discussed in this article are the most utilized options at the time of writing.
6. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
7. *Id.*
8. *Id.*
9. *Uselton v. Commercial Lovelace Motor Freight, Inc.,* 940 F.2d 564, 574-75 (10th Cir. 1991); see also *Frazier v. Manson*, 484 F. Supp. 449, 452 n.5 (N.D. Tex. 1980) (limited partnership interests received in exchange for services, rather than money, met the "investment of money" requirement although limited partners participation in day-to-day operation of the business precluded security status due to Howey's efforts of others requirement).
10. *Marine Bank v. Weaver*, 455 U.S. 551, 558 (1982). [hereinafter "**Marine Bank**"] ("deposits are insured by the Federal Deposit Insurance Corporation. Since its formation in 1933, nearly all depositors in failing banks insured by the FDIC have received payment in full").
11. It is important to note that if the instrument that the promoter is offering is a security, the SEC has taken an extremely broad approach to what could be considered a securities "offering." The SEC has previously issued guidance stating that even requiring participants to sign up on the issuer's website and disclose valuable personal information in order to obtain shares of the issuers stock constitutes an offering of securities. *See Simplystocks.com*, SEC No-Action Letter (Feb 4, 1999). However, this broad approach only applies to the offering of securities (e.g., shares of stock in a company) and not the investment of money factor in the Howey Test. The Delegation relationship and the underlying Rewards are not independently securities (though

Rewards might be depending on the applicable Network) and thus the requirement for an investment of money is higher and the client must actually risk financial loss.

12. In BPoS Networks, bonding is the process in which a holder expresses its commitment to the Network by locking a defined amount of their digital assets for a certain time period. By bonding, the holder signals to the Network that it is a trustworthy actor and accepts the rules and regulations of the Network. Bonding periods can last anywhere from five days to three weeks.
13. *See* Marine Bank at 455 ("The Court of Appeals failed to give appropriate weight to the important fact that the purchaser of a certificate of deposit is virtually guaranteed payment in full, whereas the holder of an ordinary long-term debt obligation assumes the risk of the borrower's insolvency.").
14. Additionally, it is important to note that the Rewards earned during the Delegation period have a significant likelihood of increasing the amount of digital assets held by the client, while the digital assets subject to Slashing are only a small percentage (5% in Cosmos) of the client's total assets.
15. *See* SEC's Strategic Hub for Innovation and Financial Technology *"Framework for "Investment Contract" Analysis of Digital Assets* (April 3, 2019), https://www.sec.gov/files/dlt-framework.pdf.
16. *See United Housing Found., Inc. v. Forman*, 421 U.S. 837, 855 (1975) ("By profits, the Court has meant either capital appreciation resulting from the development of the initial investment, as in Joiner, supra, (sale of oil leases conditioned on promoters' agreement to drill exploratory well), or a participation in earnings resulting from the use of investors' funds, as in *Tcherepnin v. Knight*, *supra* (dividends on the investment based on savings and loan association's profits.") [hereinafter "**Forman**"].
17. For example, over 80% of all "Tezzies" (i.e., the digital asset associated with the Tezos network) are currently being Staked. This percentage could even rise given the current growth and professionalization of the StaaS market. Even so, such participation numbers provide evidence that holders might not have an "expectation of profit" from Staking, but rather elect to Stake to protect the value of the underlying digital asset and combat inflation. However, if Network Staking participation rates are lower it could provide evidence that holders are Delegating in hope of earning profits.
18. Some StaaS providers utilize the terms "inflation rate" and "inflation rewards" instead of "interest rate," "dividend" or "yield."
19. It is important to note that the tax implications for Delegators earning rewards are unclear, but that there may be tax consequences from either income or capital gains perspectives depending on how the IRS determines these arrangements should be treated. For one perspective on this, *See* Ben Davenport, A Stake to the Heart Why Uncle Sam Loves Proof of Stake (April 26, 2019), https://medium.com/@bendavenport/a-stake-to-the-heart-57fcd8ec323b.
20. *See SEC v. Glenn W. Turner Enterprises Inc.*, 474 F.2d 476, 482 (9th Cir. 1973) ("[T]he fact that the investors here were required to exert some efforts if a return were to be achieved should not automatically preclude a finding that the Plan or Adventure is an investment contract. To do so would not serve the purpose of the legislation. Rather we adopt a more realistic test, whether the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise.").

21. *See SEC v. Unique Financial Concepts, Inc.*, 196 F.3d 1195, 1201 (11th Cir. 1999) ("[T]his Court has clearly stated that the crucial inquiry for the third element is the amount of control that the investors retain under their written agreement.") (internal citations, quotations and brackets omitted).
22. *SEC v. Belmont Reid & Co.* involved a promoter ("**CMC**") that was involved in a gold mining operation who obtained prepayments from purchasers for the purchase of gold coins that would be obtained as a result of the mining operation. *SEC v. Belmont Reid & Co.,* 794 F.2d 1388 (9th Cir. 1986). The Ninth Circuit explicitly acknowledged that the "purchaser's greatest risk under the prepayment plan was the possible failure of CMC to deliver the coins," and that it would be easy to assert that the failure or the success of the enterprise depended significantly on the managerial efforts of CMC. *Id.* However, the court ruled in favor of CMC stating that same non-performance risk exists in the context of any sale-of-goods contract in which the buyer pays in advance, and therefore that such a dependence on the promoter's efforts could not itself satisfy the Howey Test without making any such sale-of-goods contract a security. *Id.* The Ninth Circuit determined that the purchasers who prepaid for the gold coins "had as their primary purpose to profit from the anticipated increase in the world price of gold . . . In short, the purchaser[s] were speculating in the world gold market . . . To the extent the purchasers relied on the managerial skill of [the promoters] they did so as an ordinary buyer, having advanced the purchase price, relies on an ordinary seller." *Id.* at 1391.

    Additionally, in *Noa v. Key Futures, Inc.*, the Ninth Circuit held that if the expectation of economic return from an instrument is based on market forces, and not on the efforts of a promoter, then the instrument does not satisfy this element of the Howey Test. *Noa v. Key Futures, Inc.*, 638 F.2d. 77 (9th Cir. 1980). The Ninth Circuit focused on the existence of a separate national market for silver that purchasers could sell into and that was not dependent on Key Futures.
23. *SEC v. C. M. Joiner Leasing Corp.*, 320 U.S. 344, 64 S.Ct. 120, 88 L.Ed. 88 (1943).
24. See *id*. ("Without the drilling of the well, no one's leases had any value, and, except for that undertaking, they had been obtained at no substantial cost. The well was necessary not only to fulfill the hopes of purchasers, but apparently even to avoid forfeiture of their leases.").
25. *See* https://stakingrewards.com/ (last accessed July 21, 2019).
26. *See* CNBC, "Cryptocurrencies have shed almost $700 billion since January peak" https://www.cnbc.com/2018/11/23/cryptocurrencies-have-shed-almost-700-billion-since-january-peak.html (last accessed July 21, 2019). In 2018, the Digital Asset market declined over 80% with some Digital Assets losing over 90% of their value.
27. *See* note 16 *supra,* clients are required to pay federal and state taxes on the receipt of Rewards which further diminishes any expectation of profit.
28. *See*, e.g. *Williamson v. Tucker*, 645 F.2d 404, 418 (5th Cir. Tex 1981) [hereinafter "**Williamson**"]; *Mr. Steak, Inc. v. River City Steak. Inc.*, 324 F. Supp. 640 (D. Colo. 1970) [hereinafter "**Mr. Steak**"]; *Ballard & Cordell Corp. v. Zoller & Dannenberg Exploration, Ltd.*, 544 F.2d 1059 (10th Cir. Colo. 1976) [hereinafter "**Ballard**"].
29. This control analysis has arisen in a number of contexts. *See*, e.g, Williamson, 645 F.2d 404 (joint venture interests); Mr. Steak, 324 F. Supp. 640 (restaurant franchise); Ballard, 544 F.2d 1059 (oil & gas interest); *Fargo Partners v. Dain Corp.*, 540 F.2d 912 (8th Cir. N.D. 1976) (purchase of apartment complex).
30. *See* Williamson at 418.

31. In *Williamson*, purchasers brought an action involving a joint venture formed for the purpose of developing real estate. Pursuant to the joint venture agreement, the sponsor/manager could be removed with the vote of 60% or 70% of the joint venture interests. *Id.* at 409. The Fifth Circuit held in favor of the developer reasoning that "[s]o long as the investor has the right to control the asset he has purchased, he is not dependent on the promoter or on a third party for those essential managerial efforts which affect the failure or success of the enterprise." *Id.* at 421.

    In *Fargo Partners v. Dain Corn.*, the purchaser bought an apartment complex and granted the seller the exclusive right to manage and market the property. *Fargo Partners v. Dain Corn.*, 540 F.2d 912 (8th Cir. N.D. 1976). However, the management agreement with the seller provided the purchaser the ability to terminate the contract upon 30 days' notice. *Id*. at 914. The Eighth Circuit held that there was no investment contract since the purchasers owned the property and had the ability to terminate the contract with the seller. *Id.* at 915.

    Likewise, in *Perrv v. Gammon*, the court would not convert an ordinary sale of real estate into a securities transaction because the partnership had the right to terminate the management agreement with 30 days' notice and also retained ultimate control over the property. *Perrv v. Gammon*, 583 F. Supp. 1230 (N.D. Ga. 1984).

32. *See Williamson* at 423 ("We must emphasize, however, that a reliance on others does not exist merely because the partners have chosen to hire another party to manage their investment.").

33. *See Aldrich v. McCulloch Prodes*, 627 F.2d 1036 (10th Cir. Colo. 1980) ("Obligation to perform minimum managerial functions or to provide basic improvements does not transform a real estate sale into a securities transaction.").

34. *See* https://www.chorus.one/cosmos/tos/ (last visited July 21, 2019).

35. Tezos holders are able to transfer or sell their tokens immediately; however, it will take approximately 21 days for the holder to re-delegate to a new validator. Cosmos holders are able to re-delegate their token to another validator immediately, but their tokens are bonded and subject to transfer restrictions for 21 days after Delegating.

36. In *Howey*, the service contract gave the defendant service company a leasehold interest plus exclusive possession of the land, generally for a 10-year period without the option of cancellation.

37. In *Albanese v. Florida Nat'l Bank* and *SEC v. Rubera*, the Eleventh Circuit held that the purchase of ice machines coupled with a leaseback and a management agreement with the seller constituted an investment contract. *Albanese v. Florida Nat'l Bank*, 823 F.2d 408 (1lth Cir. Fla. 1987). Under the management agreement, the seller both supplied and serviced the ice machines and paid proceeds from the machines to the investor. *Id.* at 411. Similar to *Fargo*, the leaseback and management agreements provided the investor with the ability to terminate the management agreement if the seller breached the agreement or within 90 days after the participant repaid its purchase loan to the seller. *Id.* The court held that any control of the investors was "illusory because the investors had no realistic alternative to allowing seller to manage their investments." *Id.* at 412. The investors could only place the machines in locations where the seller had availability, which was determined by the seller's contacts and sales efforts in finding such locations. *Id.* Further, the investors did not have any relevant experience in placing, managing or servicing ice machines, and there was no evidence that other

companies existed that offered the wide range of management services that the seller provided with respect to the ice machine. Accordingly, the court held that any control by the investors was illusory and that an investment contract existed. *Id.*

In *SEC v. Rubera*, the Ninth Circuit focused on the investors' practical ability to exert control over the property at issue. *SEC v. Rubera*, 350 F. 3d 1084 (9th Cir. Or. 2003). The promoter therein maintained a business that sold pay telephones and simultaneously entered into service agreements with purchasers whereby the promoter would select the location of the telephones, install the telephones, maintain the telephones, pay all monthly telephone and utility bills, and obtain all regulatory certifications. *Id.* at 1087. The promoter offered four different service level offerings and over 90% of the investors selected the highest level of service, indicating they expected the promoter to manage the telephones. *Id.* The court held that the "question of an investor's control over his investment is decided in terms of practical as well as legal ability to control." *Id.* at 1093. Similar to *Albanese*, when looking at the investor's ability to control the relationship, the court focused on the experience and knowledge of the investor and the promoter's managerial skill. *See id.* ("The degree of experience and knowledge of the investor and the promoter's managerial skill are relevant to determining practical ability to control."). In *Rubera*, the investors were relying on the promoter's particular experience and skill in the telecommunications industry since the majority of the investors did not have any relevant experience in the industry, which was evidenced by the vast majority opting for the highest service level. *See id.* ("Sales agents promoted the investment opportunity in part by highlighting Alpha's experience and skill in the telecommunications industry. Moreover, although a small fraction of investors did not choose Level Four, all investors in the telephone investment program entered into some sort of service agreement with Alpha, with the vast majority opting for the highest level of service. Therefore, it is clear that investors relied on Alpha's managerial skill and effort to make the telephone investment program a success.").

38. *See Affco Invs. 2001, LLC v. Proskauer Rose, LLP*, 625 F.3d 185, 190 (5th Cir. 2010) ("Even though an investor might retain "substantial theoretical control," courts look beyond formalities and examine whether investors, in fact, can and do utilize their powers.").
39. As discussed above, holders who delegate tokens for Pure PoS networks have much less control over their assets since the StaaS provider is required to take custody of the tokens to participate in Staking.
40. *See Williamson* at 424 ("the partner or venturer is so dependent on some unique entrepreneurial or managerial ability of the promoter or manager that he cannot replace the manager of the enterprise or otherwise exercise meaningful partnership or venture powers").
41. *See* https://stakingrewards.com/ (last accessed July 21, 2019).
42. *Tcherepnin v. Knight,* 389 U.S. 332, 336 (1967).
43. *See* The Investor's Advocate: How the SEC Protects Investors, Maintains Market Integrity, and Facilitates Capital Formation, http://www.sec.gov/about/whatwedo.shtml.
44. *See* Daniel M. Gallagher, The Importance of the SEC Disclosure Regime, Harvard Law School Forum on Corporate Governance and Financial Regulation (July 16, 2013). https://corpgov.law.harvard.edu/2013/07/16/the-importance-of-the-sec-disclosure-regime/.

45. *Id.*
46. *See* https://stakingrewards.com/ (last accessed July 21, 2019).
47. 18 U.S.C. §§ 1956, 1957.
48. The Bank Secrecy Act, enacted in 1970, established reporting and recordkeeping requirements on banks and other financial institutions. *See* Pub. L. 91-508 (Oct. 26, 1970); *See* also 31 U.S.C. § 5311.
49. *See* Anti-Drug Abuse Act of 1988, Pub. L. 100-690 (Nov. 1, 1988).
50. 31 C.F.R. § 1010.100(ff)(5)(i) (B) (2011).
51. *Id*.
52. FinCEN, *Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013), [hereinafter "**2013 Virtual Currency Guidance**"], available at https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
53. For the remainder of the Article we will reference convertible virtual currency or digital assets as "virtual currency."
54. 2013 Virtual Currency Guidance at 2.
55. *Id*., at 3–4.
56. *Id.,* at 2.
57. *Id*.
58. *Id*. at 3.
59. *Id*. at 5.
60. 31 C.F.R. § 1010.100(ff)(5)(i) (B) (2011).
61. 76 Fed. Reg. 43592 (July 21, 2011).
62. *See* FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," FIN-2019-G001, Page 3, (May 9, 2019), hereinafter [**2019 Virtual Currency Guidance**], available at https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

    ("A "transmittor," on the other hand, is "[t]he sender of the first transmittal order in a transmittal of funds… In other words, a transmitt**or** initiates a transaction that the money transmitt***er*** actually executes.").
63. *See* May 2019 Guidance at page 7 ("person" means "[a]n individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities cognizable as legal personalities."). FinCEN could argue that a Network would be considered a "person" under the BSA.

    See id. at 13 ("The 2013 VC Guidance also clarified that FinCEN interprets the term "another location" broadly" … "For example, transmission to another location occurs when an exchanger selling CVC accepts real currency or its equivalent from a person and transmits the CVC equivalent of the real currency to the person's CVC account with the exchanger. This circumstance constitutes transmission to another location because it involves a transmission from the person's account at one location (e.g., a user's real currency account at a bank) to the person's CVC account with the exchanger.").

64. 2013 Virtual Currency Guidance at 2.
65. *Id.*
66. FinCEN Ruling, FIN-2014-R001 "Application of FinCEN's Regulations to Virtual Currency Mining Operations," dated January 30, 2014 [hereinafter "**Mining Ruling**"].
67. *Id.*
68. *Id.*
69. *Id*.
70. FinCEN Ruling, FIN-2014-R002 "Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity," dated January 30, 2014.
71. Most StaaS provider contractual obligations are structured in a way that neither creditors or sellers have rights to any of the Rewards received by the StaaS providers.
72. Mining Ruling, *supra* note 61, at 2.
73. 31 C.F.R. § 1010.100(ff)(5)(ii) (F) (2011).
74. 2013 Virtual Currency Guidance, supra note 13, at 4–5, (explaining that an exchanger that connects a user with an administrator to facilitate the purchase or sale of a convertible virtual currency does not provide a service other than money transmission).
75. FinCEN Ruling FIN-2014-R011, "Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform," dated October 27, 2014.
76. Similarly, in FinCEN Ruling 2004-4, FinCEN determined that a debt management company was not a money transmitter. *See* FinCEN Ruling FIN-2008-R011, "Whether a Company that Engages in Microfinance is a Money Services Business," February 20, 2009. The debt management company was instrumental in negotiating a payment plan that adjusted the total amount of debt, was binding on both the creditor and the debtor, and required the participation of the debt management company as a payment processor. FinCEN concluded that to the extent that money transmission conducted by the debt management company was limited to submitting payment to creditors on behalf of debtors *in conjunction with* the debt management plan, the debt management business was not a money transmitter by virtue of such activities.
77. FinCEN Ruling 2004-4, "Definition of Money Services Business (Debt Management Company)," November 24, 2004.
78. FinCEN Ruling FIN-2008-R007, "Whether a Certain Operation Protecting On-Line Personal Financial Information is a Money Transmitter," May 27, 2008.
79. *See* May 2019 Guidance at Page 28.
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.*
84. The key distinction FinCEN makes in determining if a Group Leader is a money transmitter is whether the Group Leader is transmitting rewards to pool members virtual currency wallets that are also hosted by the Group Leader. The May 2019 Guidance also distinguishes between "hosted wallets" and "unhosted wallets." Hosted

wallets are those wallets where the user's funds are controlled by third parties. Whereas unhosted wallets the user control the funds.

85. *See* May 2019 Guidance, FinCEN provided four criteria to assist in determining if a wallet is "hosted" or "unhosted": "(a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the CVC runs; and, (d) whether the person acting as intermediary has total independent control over the value."

Angela Angelovska-Wilson
Tel: +1 202 365 1448 / Email: angela@dlxlaw.com

Angela Angelovska-Wilson is an early distributed ledger technology adopter and a leading authority in the evolving global legal and regulatory landscape surrounding distributed ledger technology and smart contracts. Prior to co-founding DLx Law, Angela served as the Chief Legal & Compliance Officer of Digital Asset and was part of the founding team. Prior to joining Digital Asset, Angela was a partner at Reed Smith where she regularly advised clients on the implementation of new technologies to finance and the complex regulatory schemes involved in the development, creation, marketing, sale and servicing of various financial services and products. Before Reed Smith, Angela spent most of her career in various roles at Latham & Watkins, where she was recognized by *The Legal 500 US* as among the top finance attorneys in the U.S. Angela has a deep understanding of the Fin-Tech industry and in particular the distributed ledger industry, having been involved in a number of startups in various roles, as an employee, entrepreneur and advisor. In addition to DLx Law, Angela is also co-founder of Sila Inc., an innovative technology company.

Evan Weiss
Tel: +1 571 247 5528 / Email: evan@proofofstakealliance.org

Evan Weiss is currently the President and Founder of the Proof of Stake Alliance (POSA), a non-profit focused on bringing legal and regulatory clarity to the Proof of Stake industry through education and dialogue with regulators and policymakers. Evan also serves as an advisor and investor to companies in the blockchain and cryptocurrency sector. Prior to POSA, Evan was an Associate at Holland & Knight LLP where his practice focused on mergers & acquisitions and venture financings. Evan received his J.D. from the George Washington University Law School with High Honors, and his B.S. from the University of Mary Washington.

DLx Law

4913 43rd St. NW, Washington, D.C. / 114 East 25th Street, New York, NY 10010, USA
Tel: +1 212 994 6845 / URL: www.dlxlaw.com

Legal issues surrounding the use of smart contracts

Stuart Levi, Alex Lipton & Cristina Vasile
Skadden, Arps, Slate, Meagher & Flom LLP

"Smart contracts" are a critical building block in the development and evolution of many types of transactions executed on distributed ledger technologies such as blockchains.[1] By automating processes and increasing outcome certainty, smart contracts can offer important benefits in a system that effectively relies on computer networks to process transactions. This article examines whether smart contracts are enforceable legal agreements under contract law in the United States, and highlights certain legal and practical considerations that will need to be addressed before smart contracts can be widely adopted in commercial contexts.

Smart contracts: An introduction

"Smart contracts" is a term used to describe computer code that automatically executes all or parts of the transaction steps of an oral or written agreement between two parties. The code can either be the sole manifestation of the agreement between the parties ("code-only smart contracts") or complement a traditional natural language-based contract by effectuating certain provisions of that contract ("ancillary smart contracts"). The critical difference between smart contracts and natural language contracts is how they handle performance: natural language contracts generally rely on the parties to perform the contract's obligations, whereas smart contracts perform the parties' obligations automatically once triggered. By eliminating the need for human intervention, smart contracts potentially reduce the execution and enforcements costs of the contract process. As a basic example, consider an agreement between an insurer and a farmer that will pay the farmer in the event temperatures drop below a certain degree. In a natural language contract, the farmer would need to check the temperature each day, make a claim if the temperature falls below the agreed-upon degree, and then wait for the insurer to verify the claim and pay the farmer (or dispute the claim). If a smart contract component was added, the smart contract could automatically receive a feed of the official recorded temperature (using a measure agreed by the parties) and then automatically transfer funds from the insurer's account to the farmer's account if the temperature drops below the agreed-upon level.

Standards organizations and trade associations have also begun to acknowledge the impact that smart contracts could have on transactions in their areas. For example, the International Swaps and Derivatives Association ("ISDA") has signaled an openness to smart contracting in the derivatives context, though ISDA noted that any use of smart contracts must comply with existing legal requirements such as ISDA's documentation standard.[2]

The concept of smart contracts was first articulated by the computer scientist and cryptographer Nick Szabo and predates the development of blockchain technology.[3] Since

then, the ability to store immutable code and data in a transparent way on a blockchain, and the interest in disintermediating human intervention, has generated widespread interest in developing smart contracts. As with other data stored on a blockchain (such as the amount of cryptocurrency held by an address), smart contract code is replicated across multiple nodes and executed according to the same consensus mechanism on a blockchain. Moreover, because smart contracts use the same asymmetric cryptography, in which users rely on private keys and public keys, as other blockchain-based transactions, smart contracts allow parties to authenticate each other, and provide a level of security not present in many other automated transactions.

Although smart contracts have great potential to reduce transaction costs and minimize outcome uncertainty, they currently can replace only the types of contractual provisions that can be represented in specific and objective terms, such as "if X occurs, then execute step Y." Subjective provisions, such as whether a party used commercially reasonable efforts, cannot be translated into smart contracts. In this respect, smart contracts are not particularly "smart." It is therefore important not to confuse smart contracts with efforts being made in the areas of artificial intelligence and machine learning.

In addition, smart contracts will often need to rely on external (i.e., "off-chain") resources before they can execute a transaction. In the crop insurance example above, the recorded temperature would be such an off-chain resource. The reliance on off-chain resources presents several problems. For example, smart contracts cannot "pull" data from off-chain resources; rather, that data must be "pushed" to the smart contract, so the parties need to agree on a single, definitive, off-chain resource willing to and capable of pushing relevant data to the smart contract. Without such clarity, there would not be a consensus as to whether the contract should trigger, and the transaction would not execute. In our example, the farmer may argue that the weather service he consulted recorded a temperature of 31 degrees, while the insurer might claim a temperature of 33 degrees.

In order to address these issues, parties to smart contracts use "oracles"—trusted third parties that retrieve mutually-agreed off-chain information and then push that information to the smart contract at predetermined times. While oracles represent an elegant, and for the time-being necessary, solution to smart contracts' functional need to access off-chain resources, they introduce a potential point of failure in what might otherwise be a fully automated and decentralized transaction system. An oracle might cease conducting business, experience a system failure, be hacked, or provide erroneous data. Indeed, a hacker looking to impact smart contracts would likely have an easier time exploiting the oracle's data feed than hacking the smart contract itself.

Are smart contracts legally enforceable under contract law in the United States?[4]

Given that the use of smart contracts is in its incipient stages, there is no case law precedent that directly addresses the enforceability of smart contracts and, as discussed below, there are only a handful of state statutes purporting to address this issue directly.[5] However, the fact that smart contracts are not drafted in natural language prose should not impact their enforceability under the principles generally applicable to contracts.

The Uniform Commercial Code and Statute of Frauds

As a preliminary matter, in order to be legally enforceable, smart contracts must comply with applicable state writing and signing requirements. The most relevant requirements in this respect flow from two sources: the Uniform Commercial Code ("U.C.C."), a comprehensive set of laws governing all commercial transactions in the United States; and

state laws that identify agreements that must be in writing and signed to be enforceable (referred to as the "statute of frauds"). The U.C.C. has been adopted in whole or in part by all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands; and all states except Louisiana have adopted a statute of frauds.

The "written agreement" requirement

Under the U.C.C. and statute of frauds, not every contract needs to be in writing. Under the U.C.C., the following contracts generally must be in writing: (i) a contract for the sale of goods priced at or over $500;[6] (ii) lease contracts relating to personal property requiring total payments of $1,000 or more;[7] and (iii) certain agreements creating a security interest.[8] The specifics of what terms must be in writing vary by the subject matter. For example, a contract for the sale of goods must generally specify the goods at issue and the price,[9] while a lease must generally include the required payments, the term, and a reasonable description of the leased property.[10] Similarly, each state's statute of frauds generally requires a written agreement for: (i) agreements relating to executorship, suretyship, marriage; (ii) performance to be undertaken over one or more years after the execution of the agreement; and (iii) agreements for the sale of an interest in land.[11]

The question is whether a smart contract, effectively a piece of computer code, can satisfy the writing requirement under the U.C.C. and statute of frauds. Historically, courts have recognized that under the U.C.C., a written agreement does not necessarily need to be natural language prose.[12] Indeed, the U.C.C. specifies that any type of "intentional reduction to tangible form" is sufficient.[13] This is consistent with the U.C.C. policy that the "writing" requirement is meant to assure that the intention of the parties is manifest. Thus, courts have held, for example, that emails can satisfy the U.C.C. "writing" requirement.[14] Smart contracts should be treated no differently than other forms of electronic records. This is not to say that all smart contracts, by definition, will satisfy the U.C.C. requirement. Just as an email may be inconclusive as to what the parties actually intended, so too a smart contract may be too vague. That said, given the objective nature of smart contract code and the parameter certainty required to effectuate a transaction, most smart contracts for the sale of goods or for leases should satisfy the U.C.C. "writing" requirement, particularly if the parties use an ancillary smart contract where the code just executes certain terms in the natural language agreement.

A similar analysis can be applied under the statue of frauds. Under these state laws, a valid writing need not be written entirely in natural language prose nor be comprehensive.[15] As with contracts interpreted under the U.C.C., courts have taken an expansive view as to what can satisfy the "writing" requirement under the statute of frauds, focusing on the intent of the parties to create a binding agreement.[16] Thus, terms conveyed through e-mail or even types of telegraphic code can form binding contracts.[17]

In addition, the writing under the statue of frauds generally need only contain the agreement's "essential terms" which can vary depending on the type of transaction.[18] As noted above, given the nature of smart contracts, the "essential terms" (such as price and what is being delivered) will likely be captured by the code itself. And, even if the essential terms are not capable of being expressed in "if-then" terms, smart contracts can be used as ancillary tools to natural language contracts that include those terms.

The signature requirement

Both the U.C.C. and the statute of frauds require that a contract have valid signatures to be binding. This requirement can also be satisfied when using smart contracts. The U.C.C. specifies that a signature can be "any symbol executed or adopted with present intention to

adopt or accept a writing."[19] Similarly, the statute of frauds generally recognizes that a signature may be any symbol made by a party with the present intent to authenticate a writing or contract.[20] Courts typically look to the intent of the parties and whether the signing parties proffered a signature with an intention to authenticate the writing.[21] Since smart contract transactions on a blockchain need to be affirmatively authenticated by each party using public-private key cryptography, a digital signature on a smart contract should constitute a "symbol executed or adopted with present intention to adopt or accept a writing"[22] and satisfy the flexible signature requirements of the U.C.C. and statute of frauds.

The E-SIGN Act and UETA

The Electronic Signatures in Global National Commerce Act ("E-SIGN Act") and state laws modeled on the Uniform Electronic Transactions Act ("UETA") also provide important support for the concept that smart contracts should be treated as legally enforceable agreements. Under each of these acts, electronic records and electronic signatures used in interstate or foreign commerce transactions generally cannot be denied legal effect solely because they are in electronic form.[23] Although E-SIGN is a federal law, and generally preempts state laws, individual states may "modify, limit, or supersede"[24] the E-SIGN Act if they adopt UETA or satisfactory "alternative procedures or requirements."[25] UETA has been adopted by 47 states, the District of Columbia, Puerto Rico and the Virgin Islands.

The key question is whether the blockchains on which smart contracts are stored are "electronic records" and therefore enjoy protection under these acts, and whether the digital signatures used with smart contracts can be deemed protectable "electronic signatures."

Both the E-SIGN Act and UETA define electronic records broadly to include any "record created, generated, sent, communicated, received, or stored by electronic means."[26] An explanatory comment to UETA indicates that this includes any "[i]nformation processing systems, computer equipment and programs . . . and similar technologies" and any "information stored on a computer hard drive."[27] There should be little dispute that a blockchain satisfies this broad definition since, at a minimum, it stores records by electronic means. Moreover, at least one court has suggested that a database is an electronic record under UETA,[28] providing important guidance given that a blockchain is an encrypted and distributed database.

The E-SIGN Act and UETA also define electronic signatures broadly. Under both acts, an "electronic signature" includes any "electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record."[29] Moreover, UETA expressly states that this definition encompasses a "digital signature using public key encryption technology."[30] As with the statute of frauds and the U.C.C., a digital signature based on asymmetric cryptography that is used to sign a smart contract should meet the E-SIGN Act and UETA definition of a legally valid electronic signature.

The E-SIGN Act and UETA also include an additional concept that supports the enforceability of smart contracts. Under these acts, an agreement cannot be denied legal effect because the parties used an "electronic agent" which each act defines to include a "computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual."[31] Smart contracts which run self-executing code agreed to by the contracting parties would seem to fit squarely within this definition. The comments to UETA also contemplate the possibility that electronic agents could conduct transactions with other electronic agents or autonomously, which could occur as smart contracts and artificial intelligence continue to develop.[32]

In order to rely on the foregoing protections of UETA, the parties must first agree in a non-electronic writing that they will conduct all or part of a transaction electronically. Thus, one party could not implement a smart contract without the express written consent of the other party. Similarly, if a written record needs to be made available to a consumer, the E-SIGN Act requires affirmative consumer consent before an electronic record can be used, which consent can be withdrawn at any time.[33] The right for consumers to withdraw their consent at any time under the E-SIGN Act may create operational complications given the self-executing nature of most smart contracts.

As noted above, only 47 states have adopted UETA. Illinois (through the state's Electronic Commerce Security Act),[34] New York (through the state's Electronic Signatures and Records Act),[35] and Washington (though a state statute that recognizes the E-SIGN Act as applying to state and local transactions)[36] have each adopted their own unique e-signature statutes in lieu of a statute modeled on UETA. While these three states adopt broad definitions of electronic records and electronic signatures, none offer the added protection of electronic agents set forth in the 47 states that have adopted UETA.

Specific state laws applicable to smart contracts

Although, as discussed above, there are strong arguments that existing state laws already provide a sound basis for the enforceability of smart contracts, to date, four states have amended their laws specifically to allow for the enforceability of blockchain-based contracts. Many believe that these states have done so in order to appear "blockchain friendly" to attract blockchain-based companies. However, in their attempts to provide greater clarity on this issue and incentivize blockchain-based development, these states may have created more uncertainty, in part because of how these laws will be interpreted and in part because of the implicit suggestion that existing laws did not cover smart contract transactions.

Arizona

In March 2017, Arizona became the first state to amend its version of UETA, the Arizona Electronic Transactions Act ("AETA") to address blockchain technology. The AETA as amended provides that a "signature that is secured through blockchain technology is . . . an electronic signature," and "a record or contract that is secured through blockchain technology is . . . an electronic record."[37] The AETA further states that "[s]mart contracts may exist in commerce" and that contracts "may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term."[38] Blockchain technology is defined to mean "distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth."[39] A smart contract is defined as "an event-driven program, with state, that runs on a distributed, decentralized, shared and replicated ledger that can take custody over and instruct transfer of assets on that ledger."[40] Although these definitions are broad, they employ multiple ambiguous terms whose exact meaning litigants and courts may debate.

Nevada

In June 2017, Nevada amended its version of UETA, the Nevada Electronic Transactions Acts ("NETA") to state that an "electronic record" includes, without limitation, a blockchain.[41] The statute defines blockchain to mean "an electronic record of transactions or other data which is: (i) [u]niformly ordered; (ii) processed using a decentralized method by which one or more computers or machines verify the recorded transactions or other data; (iii) [r]edundantly maintained or processed by one or more computers or machines to

guarantee the consistency or nonrepudiation of the recorded transactions or other data; and (iv) [v]alidated by the use of cryptography."[42] A recent amendment, which will go into effect in October 2019, clarifies that the definition of blockchain includes, without limitation, a public blockchain.[43] Smart contracts are not directly addressed in the statute, and note that the definition of blockchain is fairly different than that adopted by Arizona.[44]

Ohio

In June 2018, Ohio amended its version of UETA to state that "a record or contract that is secured through blockchain technology is considered to be in an electronic form and to be an electronic record."[45] The law also amends the definition of electronic signatures to state that "a signature that is secured through blockchain technology is considered to be in an electronic form and to be an electronic signature"[46] and that "a record or signature may not be denied legal effect or enforceability solely because . . . the contract contains a smart contract term." The amendment mirrors Arizona's definition of blockchain technology, defining it as "distributed ledger technology that uses a distributed, decentralized, shared, and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable, and provides an uncensored truth."[47]

Tennessee

In March 2018, Tennessee amended its UETA to clarify that "a record or contract that is secured through distributed ledger technology is considered to be in an electronic form and to be an electronic record."[48] It further provides: "[a] cryptographic signature that is generated and stored through distributed ledger technology is considered to be . . . an electronic signature."[49] Tennessee adopted some of the blockchain technology definition used by Arizona and Ohio, but categorized it as "distributed ledger technology" and made some important modifications. Specifically, distributed ledger technology is defined as "any distributed ledger protocol and supporting infrastructure, including blockchain, that uses a distributed, decentralized, shared, and replicated ledger, whether it be public or private, permissioned or permissionless, and which may include the use of electronic currencies or electronic tokens as a medium of electronic exchange."[50] Similarly, the state's definition of "smart contracts" mirrors that of Arizona and Ohio but adds some additional language. A "smart contract" is defined to mean "an event-driven computer program, that executes on an electronic, distributed, decentralized, shared, and replicated ledger that is used to automate transactions, including, but not limited to, transactions that: (A) [t]ake custody over and instruct transfer of assets on that ledger; (B) [c]reate and distribute electronic assets; (C) [s]ynchronize information; or (D) [m]anage identity and user access to software applications."[51, 52]

Other legal considerations

In addition to the foregoing statutes generally governing the enforceability of contracts, smart contracts may be subject to a variety of legal frameworks depending on their terms and consideration. This may include state and federal commodities and securities laws and regulations; anti-money laundering laws and regulations; and state money transmission laws. Developers of, and parties to, smart contracts must discern which regulations apply and what such compliance entails, including registration and documentation requirements.

Challenges with the widespread adoption of smart contracts

Given the existing legal frameworks for recognizing electronic contracts, it is quite likely that a court today would recognize the validity of code that executes provisions of a smart

contract—what we have classified as ancillary smart contracts. There is also precedent to suggest that a code-only smart contract might enjoy similar legal protection. The challenge to widespread smart contract adoption may therefore have less to do with the limits of the law than with potential clashes between how smart contract code operates and how parties transact business. We set forth below certain of these challenges:

How can non-technical parties negotiate, draft and adjudicate smart contracts?

A key challenge in the widespread adoption of smart contracts is that parties will need to rely on a trusted, technical expert to either capture the parties' agreement in code or confirm that code written by a third party is accurate. While some analogize this to hiring a lawyer to explain "the legalese" of a traditional text-based contract, the analogy is misplaced. Non-lawyers typically can understand simple short-form agreements as well as many provisions of longer agreements, especially those setting forth business terms. But a non-programmer would be at a total loss to understand even the most basic smart contract and is therefore significantly more beholden to an expert to explain what the contract "says."

To some extent, the inability of contracting parties to understand the smart contract code will not be a hindrance to entering into ancillary smart contracts. This is because for many basic functions, text templates can be created and used to indicate what parameters need to be entered and how those parameters will be executed. For example, assume a simple smart contract function that extracts a late fee from a counterparty's wallet if a defined payment is not received by a specified date. The text template could prompt the parties to enter the amount of the expected payment, the due date and the amount of the late fee. However, a party may want to confirm that the underlying code actually will perform the functions specified in the text, and that there are no additional conditions or parameters—especially where the template disclaims any liability arising from the accuracy of the underlying code. This review will require a trusted third party with programming expertise.

In cases where such templates do not exist, and new code must be developed, the parties will need to communicate the intent of their agreement to a programmer. Simply handing that programmer a copy of the legal agreement would be inefficient since it would require the programmer to try to decipher a legal document. Parties relying on ancillary smart contracts therefore may need to draft a separate "term sheet" of functionality that the smart contract should perform and that can be provided to the programmer.

The parties also may want written representations from the programmer that the code performs as contemplated. The net result is that for customized arrangements that do not rely on an existing template, the parties may need to enter into a written agreement with the smart contract programmer, not unlike the contract that parties may enter into with a provider of services for Electronic Data Interchange transactions today.

Insurance companies could also create policies to protect contracting parties from the risk that smart contract code does not perform the functions specified in the text of an agreement. Although the parties would also want to review (or have a third party review) the code, insurance can provide additional protection given that the parties might miss errors when reviewing the code. The parties would also take some additional comfort from the fact that the insurance company likely conducted its own code audit before agreeing to insure the code.

Code-only smart contracts used for business-to-consumer transactions could pose an additional set of issues that will need to be addressed. Courts are wary of enforcing agreements where the consumer did not receive adequate notice of the terms of the agreement,[53] and may be hesitant to enforce a smart contract where the consumer was not also provided with an underlying text agreement that included the complete terms.

Finally, as the validity or performance of smart contracts increasingly become adjudicated, courts may need a system of court-appointed experts to help them decipher the meaning and intent of the code. Today, parties routinely use their own experts when technical issues are at the center of a dispute. While both federal courts and many state courts have the authority to appoint their own experts, they rarely exercise that authority.[54] That approach may need to change if the number of standard contract disputes that center on interpreting smart contract code increases.

Liability of the smart contract developer

As noted above, in many cases, the parties to a smart contract will not have the technical capability to create a smart contract, and may therefore hire a third party to create the smart contract, or may rely on a smart contract "template" offered by a third party. In such cases, there is the possibility of programmer error or that the parties did not accurately convey what they intended to the developer. Parties will need to consider the ramifications of these situations and the appropriate allocation of risk and liability.

Developers of smart contracts may also need to be wary of their own liability in cases where smart contract code they developed is used for unlawful purposes. In October 2018, Brian Quintenz, Commissioner of the Commodity Futures Trading Commission ("CFTC"), suggested that smart contract code developers could be held accountable for aiding and abetting CFTC violations where they "could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations."[55] In November 2018, the Securities and Exchange Commission ("SEC") settled charges of operating an unregistered securities exchange against Zachary Coburn, the founder and developer of EtherDelta, a decentralized digital asset exchange. Although the SEC's order appears to be based, in part, on Coburn's control over EtherDelta's operations and his role as founder, the order also lists the fact that Coburn "wrote and deployed the EtherDelta smart contract to the Ethereum Blockchain" as a factor in finding that Coburn caused EtherDelta to violate the Securities Exchange Act of 1934.[56]

While some cases of developer liability will be clear, such as where a developer was actively part of an illegal scheme, it is likely that given the open source nature of many blockchain projects, developers will have little insight into how their smart contract code is being used, or by whom.

Outside the CFTC context, jurisprudence on contributory liability in the context of peer-to-peer technologies may provide useful precedent in balancing the need to protect developers with the need to provide redress to parties that are harmed by smart contracts put to unlawful use. For example, under *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*,[57] peer-to-peer file-sharing sites are not liable for users' infringing uses if: (1) they are not distributing their product with the "object of promoting its use to infringe"; (2) they either (a) do not have actual knowledge of specific infringements, or (b) if they do have knowledge, they are not in a position to block the infringing conduct and have failed to do so; and (3) the product is capable of substantial noninfringing use.

While *Grokster* dealt with contributory infringement under copyright law, courts may apply its core principles in the context of developer liability for blockchain-based smart contracts. In order to minimize potential liability, smart contract developers should not only avoid developing smart contracts with the object of enabling illegal use, but should also use reasonable efforts to block unexpected unlawful use.

What is the "final" agreement between the parties?

When analyzing traditional text-based contracts, courts will examine the final, written document to which the parties have agreed in order to determine whether the parties are in compliance or breach. Courts have long emphasized that it is this final agreement that represents the mutual intent of the parties—the "meeting of the minds."

In the case of code-only smart contracts, the code that is executed—and the outcome it produces—represents the only objective evidence of the terms agreed to by the parties. In these cases, email exchanges between the parties as to what functions the smart contract "should" execute, or oral discussions to that effect, likely would yield to the definitive code lines as the determinative manifestation of the parties' intent.

With respect to ancillary smart contracts, a court likely would look at the text and code as a unified single agreement. The issue becomes complicated when the traditional text agreement and the code do not align. In the crop insurance example described above, assume the text of an agreement specifies that an insurance payout will be made if the temperature falls below 32 degrees, while the smart contract code triggers the payment if the temperature is equal to or below 32 degrees. Assuming that the text agreement does not state whether the text or code controls in the event of an inconsistency, courts will need to determine—perhaps on a case-by-case basis—whether the code should be treated as a mutually agreed amendment to the written agreement or whether the text of the agreement should prevail. In some respects, the analysis should be no different than a case where the provisions of a main agreement differ from what is reflected in an attached schedule or exhibit. The fact that here the conflict would be between text and computer code and not two text documents should not be determinative, but courts may take a different view.

One solution will be for parties to use a text-based contract where the parameters that trigger the smart contract execution are not only visible in the text but actually populate the smart contract. In our example, "less than 32 degrees" would not only be seen in the text, but also would create the parameter in the smart contract itself, thereby minimizing the chances of any inconsistency.

The automated nature of smart contracts

One of the key attributes of smart contracts is their ability to automatically and relentlessly execute transactions without the need for human intervention. However, this automation, and the fact that smart contracts cannot easily be amended or terminated unless the parties incorporate such capabilities during the creation of the smart contract, present some of the greatest challenges facing widespread adoption of smart contracts.

For example, with traditional text contracts, a party can easily excuse a breach simply by not enforcing the available penalties. If a valued customer is late with its payment one month, the vendor can make a real-time decision that preserving the long-term commercial relationship is more important than any available termination right or late fee. However, if this relationship had been reduced to a smart contract, the option not to enforce the agreement on an *ad hoc* basis likely would not exist. A late payment will result in the automatic extraction of a late fee from the customer's account or the suspension of a customer's access to a software program or an internet-connected device if that is what the smart contract was programmed to do. The automated execution provided by smart contracts might therefore not align with the manner in which many businesses operate in the real world.

Similarly, in a text-based contractual relationship, a party may be willing to accept, on an *ad hoc* basis, partial performance to be deemed full performance. This might be because of

an interest in preserving a long-term relationship or because a party determines that partial performance is preferable to no performance at all. Here, again, the objectivity required for smart contract code might not reflect the realities of how contracting parties interact.

Amending and terminating smart contracts

At present, there is no simple path to amend a smart contract, creating certain challenges for contracting parties. For example, in a traditional text-based contract, if the parties have mutually agreed to change the parameters of their business deal, or if there is a change in law, the parties quickly can draft an amendment to address that change, or simply alter their course of conduct. Smart contracts currently do not offer such flexibility. Indeed, given that blockchains are immutable, modifying a smart contract is far more complicated than modifying standard software code that does not reside on a blockchain. The result is that amending a smart contract may yield higher transaction costs than amending a text-based contract, and increases the margin of error that the parties will not accurately reflect the modifications they want to make.

Similar challenges exist with respect to terminating a smart contract. Assume a party discovers an error in an agreement that gives the counterparty more rights than intended, or concludes that fulfilling its stated obligations will be far more costly than it had expected. In a text-based contract, a party can engage in, or threaten, so-called "efficient breach," *i.e.*, knowingly breaching a contract and paying the resulting damages if it determines that the cost to perform is greater than the damages it would owe. Moreover, by ceasing performance, or threatening to take that step, a party may bring the counterparty back to the table to negotiate an amicable resolution. Smart contracts do not yet offer analogous self-help remedies.

Projects are currently under way to create smart contracts that are terminable at any time and more easily amended. While in some ways this is antithetical to the immutable and automated nature of smart contracts, it reflects the fact that smart contracts only will gain commercial acceptance if they reflect the business reality of how contracting parties act.

Objectivity and the limits of incorporating desired ambiguity into smart contracts

The objectivity and automation required of smart contracts can run contrary to how business parties actually negotiate agreements. During the course of negotiations, parties implicitly engage in a cost-benefit analysis, knowing that at some point there are diminishing returns in trying to think of, and address, every conceivable eventuality. These parties no longer may want to expend management time or legal fees on the negotiations, or may conclude that commencing revenue-generating activity under an executed contract outweighs addressing unresolved issues. Instead, they may determine that if an unanticipated event actually occurs, they will figure out a resolution at that time. Similarly, parties may purposefully opt to leave a provision somewhat ambiguous in an agreement in order to give themselves the flexibility to argue that the provision should be interpreted in their favor. This approach to contracting is rendered more difficult with smart contracts where computer code demands an exactitude not found in the negotiation of text-based contracts. A smart contract cannot include ambiguous terms nor can certain potential scenarios be left unaddressed. As a result, parties to smart contracts may find that the transaction costs of negotiating complex smart contracts exceed that of a traditional text-based contracts.

It will take some time for those adopting smart contracts in a particular industry to determine which provisions are sufficiently objective to lend themselves to smart contract execution. As noted, to date, most smart contracts perform relatively simple tasks where the parameters of the "if/then" statements are clear. As smart contracts increase in complexity, parties may

disagree on whether a particular contractual provision can be captured through the objectivity that a smart contract demands.

Do smart contracts really guarantee payment?

One benefit often touted of smart contracts is that they can automate payment without the need for dunning notices or other collection expenses and without the need to go to court to obtain a judgment mandating payment. While this is indeed true for simpler use cases, it may be less accurate in complex commercial relationships. The reality is that parties are constantly moving funds throughout their organization and do not "park" total amounts that are due on a long-term contract in anticipation of future payment requirements. Similarly, a person obtaining a loan is unlikely to keep the full loan amount in a specified wallet linked to the smart contract. Rather, the borrower will put those funds to use, funding the necessary repayments on an *ad hoc* basis.

If the party owing amounts under the smart contract fails to fund the wallet on a timely basis, a smart contract looking to transfer money from that wallet upon a trigger event may find that the requisite funds are not available. Implementing another layer into the process, such as having the smart contract seek to pull funds from other wallets or having that wallet "fund itself" from other sources, would not solve the problem if those wallets or sources of funds also lack the requisite payment amounts. The parties might seek to address this issue through a text-based requirement that a wallet linked to the smart contract always have a minimum amount, but that solution simply would give the party a stronger legal argument if the dispute was adjudicated. It would not render the payment operation of the smart contract wholly automatic. Thus, although smart contracts will render payments far more efficient, they may not eliminate the need to adjudicate payment disputes.

Risk allocation for attacks and failures

Smart contracts introduce an additional risk that does not exist in most text-based contractual relationships—the possibility that the contract will be hacked or that the code or protocol simply contains an unintended programming error. Given the relative security of blockchains, these concepts are closely aligned; namely, most "hacks" associated with blockchain technology are really exploitations of an unintended coding error. As with many bugs in computer code, these errors are not glaring, but rather become obvious only once they have been exploited. For example, in 2017 an attacker was able to drain several multi-signature wallets offered by Parity of $31 million in ether.[58] Multi-signature wallets add a layer of security because they require more than one private key to access the wallet. However, in the Parity attack, the attacker was able to exploit a flaw in the Parity code by reinitializing the smart contract and making himself or herself the sole owner of the multi-signature wallets. Parties to a smart contract will need to consider how risk and liability for unintended coding errors and resulting exploitations are allocated between the parties, and possibly with any third party developers or insurers of the smart contract.

Governing law and venue

One of the key promises of blockchain technology, and by extension smart contracts, is the development of robust, decentralized and global platforms. However, global adoption means that parties may be using a smart contract across far more jurisdictions than might exist in the case of text-based contracts. The party offering terms under a smart contract would therefore be best-served by specifying the governing law and venue for that smart contract. A governing law provision specifies what substantive law will apply to the interpretation of the smart contract, whereas a venue clause specifies which jurisdiction's courts will adjudicate the dispute. In cases where governing law or venue is not specified, a plaintiff

may be relatively unconstrained in choosing where to file a claim or in arguing which substantive law should apply given the wide range of jurisdictions in which a smart contract might be used. Given that many early disputes concerning smart contracts will be ones of first-impression, contracting parties will want some certainty surrounding where such disputes will be adjudicated.

Conclusion

As smart contracts are in their nascent stages, so is the law surrounding their enforceability and use. While there are strong arguments that properly constructed smart contracts are enforceable under existing statutes governing electronic contracts, certain issues must be resolved before they can enjoy widespread adoption in complex commercial transactions. While smart contracts have potential to change the way markets operate, their impact will invariably be shaped by how such applications fit within the contours of the law.

* * *

Acknowledgment

The authors acknowledge the assistance of Daniel Chase, a law student at Berkeley Law.

* * *

Endnotes

1. Blockchains are one type of "distributed ledger technology" in which data is organized in blocks and new data can only be appended to the chain. For purposes of this article, we refer to blockchains, but most of the legal issues presented here apply to other forms of distributed ledger technology as well.
2. *See* International Swaps and Derivatives Association, *ISDA Legal Guidelines For Smart Derivatives Contracts: Introduction* (Jan. 2019), https://www.isda.org/a/MhgME/Legal-Guidelines-for-Smart-Derivatives-Contracts-Introduction.pdf.
3. *Compare* Nick Szabo, *Smart Contracts: Building Blocks for Digital Market* (1996) *with* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008).
4. There is no federal contract law in the United States; rather, the enforceability and interpretation of contracts is determined at the state level. Thus, while certain core principles apply consistently across state lines, and there has been a drive to harmonize state laws by the National Conference of Commissioners on Uniform State Laws, any conclusions regarding the enforceability of smart contracts must be tempered by the reality that states may adopt different views.
5. For a comprehensive overview of the enforceability of smart contracts, see *"Smart Contracts" & Legal Enforceability* (Cardozo Blockchain Project Research Report No. 2, Oct. 16, 2018), https://cardozo.yu.edu/sites/default/files/Smart%20Contracts%20Report%20%232_0.pdf; *see also* Uniform Law Commission, *Guidance Note Regarding the Relation Between the Uniform Electronic Transactions Act and Federal ESIGN Act, Blockchain Technology and 'Smart Contracts'* (Feb. 11, 2019) (opining that state UETA provisions do not require amendment to enable use of blockchain technology and smart contracts in electronic transactions).

6. U.C.C. § 2-201.
7. *Id.* § 2A-201.
8. *Id.* § 9-203(b)(3)(A).
9. *Id.* § 2-201.
10. *Id.* § 2A-201.
11. *See, e.g.*, Restatement (Second) Contracts § 110. Contracts that fail to comply with the statute of frauds remain enforceable in some cases, such as cases wherein promissory estoppel applies. *See* Restatement (Second) Contracts § 90.
12. *See, e.g.*, Apex Oil Co. v. Vanguard Oil Serv. Co., 760 F.2d 417, 420, 423 (2d Cir. 1985).
13. U.C.C. § 1-201(43).
14. *See, e.g.*, Bazak Int'l Corp. v. Tarrant Apparel Grp., 378 F. Supp. 2d 377, 392 (S.D.N.Y. 2005) ("Although e-mails are intangible messages during their transmission, this fact alone does not prove fatal to their qualifying as writings under the UCC[.] [F]orms of communication regularly recognized by the courts as fulfilling the UCC "writing" requirement, such as fax, telex and telegraph, are all intangible forms of communication during portions of their transmission. Just as messages sent using these accepted methods can be rendered tangible, thereby falling within the UCC definition, so too can e-mails.")
15. *See*, *e.g.*, Bibb v. Allen, 149 U.S. 481, 497–98 (1893) (holding that a contract written in telegraphic cipher code was binding); Cloud Corp. v. Hasbro, Inc., 314 F.3d 289, 295–96 (7th Cir. 2002).
16. *See, e.g.*, Leeds v. First Allied Connecticut Corp., 521 A.2d 1095, 1097 (Del. Ch. 1986) (explaining an agreement is binding when "a reasonable negotiator . . . would have concluded, in that setting, that the agreement reached constituted agreement on all of the terms that the parties themselves regarded as essential[.]").
17. *See*, *e.g.*, Bibb, 149 U.S. at 497–98; Naldi v. Grunberg, 908 N.Y.S.2d 639, 645 (App. Div. 2010).
18. *See*, *e.g.*, *Ross v. Ross*, 172 A.3d 1069, 1075 (N.H. 2017); Simmonds v. Marshall, 292 A.D.2d 592, 592 (2d Dep't 2002); Leeds v. First Allied Connecticut Corp., 521 A.2d at 1097.
19. U.C.C. § 1-201(37).
20. Restatement (Second) Contracts § 134; U.C.C. § 1-201(37).
21. *See*, *e.g.*, SD Protection, Inc. v. Del Rio, 498 F. Supp. 2d 576, 584 (E.D.N.Y 2007); U.C.C. § 1-201 cmt 37.
22. *See* U.C.C. § 1-201(37); *see also* Restatement (Second) Contracts § 134.
23. 15 U.S.C. § 7001(a)(1); UETA § 7(a), (c)-(d). There are certain exceptions to these acts (such as wills) that will not impact the majority of smart contract usage.
24. 15 U.S.C. § 7002(a).
25. 15 U.S.C. § 7002(a)(2)(A).
26. UETA § 2(7); *see also* 15 U.S.C. § 7006(4).
27. *Id.* § 2 cmt. 6.
28. *See* Godfrey v. Fred Meyer Stores, 124 P.3d 621, 631 (2005) (Armstrong, J., concurring).

29. UETA § 2(8); *see also* 15 U.S.C. § 7006(5).
30. *Id*. § 2 cmt. 7.
31. *Id*. § 2(6); 15 U.S.C.§ 7006(3).
32. *Id.* § 2 cmt. 5
33. 15 U.S.C. § 7001(c)(1).
34. 5 Ill. Comp. Stat. 175/5-110.
35. N.Y. State Tech. § 304.
36. Wash. Rev. Code § 19-360.010–360.040.
37. Ariz. Rev. Stat. Ann. § 44-7061.
38. *Id.*
39. *Id.*
40. *Id.*
41. Nev. Rev. Stat. Ann. § 719.090.
42. Nev. Rev. Stat. Ann. § 719.045, as amended by 2019 Nev. S.B. 162. Note that the amended version of this statute will become effective on October 1, 2019.
43. 2019 Nev. S.B. 162.
44. *See also* 2019 Nev. S.B. 163.
45. Ohio Rev. Code Ann. § 1306.01(G).
46. *Id.* § 1306.01(H).
47. *Id.* § 1306.06(A).
48. Tenn. Code Ann. § 47-10-202(b).
49. *Id.* § 47-10-202(a).
50. *Id*. § 47-10-201(1).
51. *Id.* § 47-10-201(2).
52. Note that other states, including California, Colorado, Connecticut, Delaware and Vermont, have enacted blockchain-related laws as well, though these laws do not specifically address the issue of blockchain-based contracts.
53. *See*, *e.g.*, Nicosia v. Amazon.com, Inc., 834 F.3d 220, 237–38 (2d. Cir. 2016) (reversing the district court's dismissal for failure to state a claim and holding that reasonable minds could disagree as to whether Amazon provided the consumer with reasonable notice of the mandatory arbitration provision at issue).
54. *See* Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure*, Section 6304 (3d ed. supp. 2011) ("In fact, the exercise of Rule 706 powers is rare under virtually any circumstances. This is, at least in part, owing to the fact that appointing an expert witness increases the burdens of the judge, increases the costs to the parties, and interferes with the adversarial control over the presentation of evidence."); Stephanie Domitrovich, Mara L. Merino & James T. Richardson, *State Trial Judge Use of Court Appointed Experts: Survey Results and Comparisons*, 50 Jurimetrics J. 371, 373–74 (2010).
55. Brian Quintenz, Commissioner, U.S. Commodity Futures Trading Commission, Remarks at the 38th Annual GITEX Technology Week Conference (Oct. 16, 2018), https://www.cftc.gov/pressroom/speechestestimony/opaquintenze16.

56. In re Zachary Coburn, Securities Act Release No. 84553 (Nov. 8, 2018), https://www.sec.gov/litigation/admin/2018/34-84553.pdf.
57. 545 U.S. 913, 918–19; 936–37 (2005) (holding that one who "distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties").
58. *See* Haseeb Qureshi, "*A Hacker Stole $31M of Ether—How it Happened, and What it Means for Ethereum*," *FreeCodeCamp* (July 20, 2017), https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce.

Stuart Levi
Tel: +1 212 735 2750 / Email: stuart.levi@skadden.com
Stuart D. Levi is co-head of Skadden's Intellectual Property and Technology Group, and he coordinates the firm's blockchain, outsourcing and privacy practices. Mr. Levi has a broad and diverse practice that includes outsourcing transactions, technology and intellectual property licensing, fintech and blockchain matters, privacy and cybersecurity advice, branding and distribution agreements, cloud computing agreements, technology transfers, strategic alliances and joint ventures. Mr. Levi also counsels clients on website and technology policies, intellectual property strategy and regulatory compliance. His background in computer science and the information technology industry allows Mr. Levi to understand the technology and business drivers underlying transactions and agreements in these areas.

Alex Lipton
Tel: +1 212 735 3006 / Email: alex.lipton@skadden.com
Alex is an Intellectual Property and Technology associate in Skadden's New York office. He earned his A.B. from Harvard University (2011) and J.D. from NYU School of Law (2016).

Cristina Vasile
Tel: +1 212 735 2247 / Email: cristina.vasile@skadden.com
Cristina is an Intellectual Property and Technology associate in Skadden's New York office. She earned her B.A. and M.A. from NYU (2008, 2009) and her J.D. from NYU School of Law (2016).

Skadden, Arps, Slate, Meagher & Flom LLP

4 Times Square, New York, New York 10036, USA
Tel: +1 212 735 3000 / URL: www.skadden.com

U.S. Federal Income Tax implications of issuing, investing and trading in cryptocurrency

Mary F. Voce & Pallav Raghuvanshi
Greenberg Traurig, LLP

Introduction

Cryptocurrency is often issued in an initial coin offering ("**ICO**") as "coins" or "tokens." Broadly, tokens can be classified as "utility tokens," which provide users with access to the blockchain platform developed by the issuer or products or services provided by the issuer on the blockchain platform, or as "security tokens," which represent certain rights with respect to an entity, either as equity or debt. Furthermore, there are so-called "intrinsic" or "convertible" cryptocurrencies that generally are used as a medium of exchange (*e.g.*, Bitcoin, Litecoin, etc.) or give access to a platform on which other blockchain projects are built (*e.g.*, Ether, Neo, Eos, etc.). Some cryptocurrencies, such as Ether, can be viewed as hybrid tokens that can be used as a medium of exchange for ICOs of other cryptocurrencies, but also allows smart contracts for other blockchain projects to be built on its platform.

This chapter is intended as a primer on certain U.S. Federal Income Tax implications of cryptocurrency transactions and structures. Because of the dearth of authorities directly on point, much of the discussion below is based on analogies to the tax treatment of other property where the rules are more developed or on the application of the language of statutory provisions, regulations, and other authorities.

Notice 2014-21: In general

While the IRS has recently promised that additional guidance will be forthcoming, the only relevant formal guidance issued by it to date is Notice 2014-21.[1] The basic rule of Notice 2014-21 is that cryptocurrency is property for United States federal income tax purposes and not "currency." Therefore, taxpayers may not use cryptocurrency as a functional currency for purposes of Internal Revenue Code ("**IRC**" or "**Code**") Section 985, and transactions in cryptocurrency would never be Section 988 transactions.[2] Further, the rules applicable to foreign currencies do not apply to transactions in cryptocurrencies.[3]

More troubling for taxpayers is that, if cryptocurrencies are property, every disposition of cryptocurrency is a disposition of property. Each time cryptocurrency is purchased for fiat currency (such as U.S. dollars), basis must be recorded and tracked, and each time a chunk of cryptocurrency is disposed of, gain or loss is recognized.[4]

One problem with Notice 2014-21 is that it appears to be limited by its terms to what we would call "cryptocurrency," rather than to utility tokens or equity tokens. It seems to apply only to cryptocurrency that can be used to pay for goods or services or that is held for investment purposes, and focuses on cryptocurrency that has an equivalent value in fiat

currency, or that acts as a substitute for fiat currency (referred to as "convertible" cryptocurrency). The remainder of this article assumes that all tokens are property and not money and discusses U.S. federal income tax issues only unless otherwise indicated.

Initial coin offerings/first token sales

Startup companies may use ICOs as a means of raising funds. An ICO is the issuance of newly generated tokens for other cryptocurrencies or, less commonly, for fiat currency. Issuers can offer non-functional tokens, the proceeds from which are used by the issuer to develop its platform, product or services. Once the platform or product is fully functional, token purchasers can use the tokens for accessing the platform, product or services developed by the issuer. Alternatively, unless token purchasers are subject to a "lock-up" period, they can be exchanged for other tokens or fiat currency.

Less commonly, companies issue tokens that represent an ownership interest in the company or other property, or that are intended simply as a means of exchange.

Tax implications of ICOs for domestic issuers

In general

The issuance by a U.S. issuer of utility or convertible tokens for cash, tokens, or other property may be treated as a sale (or, potentially, a license) of property or a promise to perform services in the future. As discussed below, in many of these situations, a domestic issuer will recognize income upon the issuance of the tokens or, potentially, later, when the services are performed.

Character and source of income

The U.S. tax implications to the issuer of tokens depend on whether income from their issuance will be characterized as sales, royalty or services income, and on the source of such income (*i.e.*, the jurisdiction in which it arises for U.S. tax purposes).

In 1998, the IRS issued Treas. Reg. § 1.861-18 (also known as the "Software Regulations"), which provide a framework for determining the character of income from the transfer of intangible property. Although the Software Regulations were issued long before blockchain technology was even contemplated, they logically can be used as a starting point for determining the character and source of income from a cryptocurrency transaction.

Under such regulations, income from the transfer of intangible property is classified as: (1) the sale of copyright rights; (2) the license of copyright rights; (3) the sale of a copyrighted article; (4) the lease of a copyrighted article; (5) the provision of services related to a computer program; or (6) the provision of know-how related to a computer program.[5]

(a) Treatment of transfer of tokens as a sale

Generally, the issuance of tokens should not result in the transfer of copyright rights because token purchasers generally do not acquire unfettered rights with respect to the underlying blockchain technology. While tokens can provide the right and ability to build upon a blockchain platform, this right would appear to be more in the nature of a service or a license rather than a right to prepare a derivative work. For example, creating a private blockchain on the Ethereum platform requires the installation of "Geth." A private blockchain created with Geth is a new asset facilitated by Ethereum, but is not a derivative of Ethereum.

However, the issuance of tokens might be analogized to a sale of intangible property that has indicia of a copyrighted article in that the purchaser acquires all of the benefits and burdens of an asset that is separate from the underlying blockchain platform and that can be used in perpetuity.[6] In that case, the character of the income from the sale of a token will

depend upon the character of the token in the hands of the transferor. It is unlikely that newly issued tokens qualify as capital assets in the hands of the issuer. Since newly issued tokens are created with the intention of selling them, they could be viewed as inventory.

If the tokens are inventory and were "produced" by the issuer, such income would be sourced based on the location of production of such inventory.[7] However, the place of "production" of the tokens might not be at all clear. In a situation where the tokens are issued based on open-source technology, with all the actual development to come afterward, the jurisdiction of the issuer might be the place of production. However, the place where the concept was created or tested or where the programmers sit might be a more realistic alternative.

(b) Treatment as a license

The issuance of a token could, to some extent, be viewed as including a license to use the issuer's blockchain platform (*e.g.*, to access content on the platform or to build a separate blockchain project keyed off the issuer's blockchain IP, although this might also be viewed as a service (as discussed below)).[8] To the extent the issuance is treated as a license, the amount received for the tokens would be considered a royalty, which would be ordinary income, and the source of the royalty would be the place where the token is used, which may not be easily determined.[9]

(c) Treatment as a service

Potentially, the consideration received for the issuance of tokens could be treated as compensation for the provision of services provided by the issuer.

This treatment could apply to pre-ICO tokens where the issuer accepts consideration from the investors subject to an obligation to use the consideration to develop the issuer's technology, although the issuer's efforts generally would be considered services only if the token holders would have an ownership interest in the IP that is developed, which is unlikely in most cases. Any income from services would be ordinary income and generally would be sourced to the location where the services are performed.[10] Services performed by individuals generally are sourced to the place where they are located when the services are performed.[11] If equipment is involved in the performance of services, the location of the equipment is also considered.[12]

A blockchain platform may also provide automated services by acting as an online intermediary linking customers with providers or by hosting or streaming information or content that can be accessed by token holders. In such a case, sourcing the revenue will present more than the usual challenges for sourcing income because of the decentralized nature of blockchain technology.

Timing of recognition of income by issuers

Generally, income must be recognized immediately upon receipt of consideration for the transfer of property or the provision of services – *i.e.*, in the case of an ICO, at the time of the issuance. However, in certain limited circumstances, an accrual basis issuer can defer taxation on at least a portion of the amount received to the succeeding taxable year if the receipt of the consideration is treated as an advance payment for future goods or services (*e.g.*, for pre-functional tokens).[13] The sale of pre-functional tokens or an agreement to sell future tokens (also known as Simple Agreement for Future Tokens (SAFT)) could also potentially be viewed as a forward contract to develop the technology and deliver the functional tokens in the future. Generally, under the common law open transaction doctrine, the execution of a forward contract will not be a taxable event until the transaction is closed.[14]

However, if the governing documents do not contain a refund provision, it is highly likely that the amount received by the issuer would be considered income at the time received.

Regardless of when the income is recognized, a U.S. issuer should be able to offset such income with operating losses (or depreciation or amortization of capitalized expenses) incurred prior to issuance to the extent eligible to be carried forward. For foreign issuers, operating losses can be carried forward only if the issuer files timely and accurate U.S. income tax returns for the years in which the losses were incurred.[15]

Tax consequences to issuer of use of tokens by purchasers

Notice 2014-21 provides that a taxpayer who receives cryptocurrency as payment for goods or services must include in gross income or gross receipts the fair market value of the tokens, measured in U.S. dollars as of the date the tokens are received. Thus, if the issuer provides a service that is accessed by using tokens it had previously issued, the issuer would include, in income, the fair market value of the tokens at the time of their use. The issuer's tax basis in the tokens received in exchange for the services would be the fair market value of the tokens at the time of their receipt.

Tax implications for token purchasers in an ICO

Purchase of tokens

The purchase of tokens in an ICO using fiat currency should not be a taxable event for the purchaser. However, if tokens are purchased using another cryptocurrency, a U.S. taxpayer would recognize gain or loss equal to the difference between the value of the tokens purchased and the tax basis in the cryptocurrency exchanged therefor.

A purchaser's basis in the tokens acquired would be their purchase price in U.S. dollars (or translated into U.S. dollars at the time of purchase if purchased using another cryptocurrency).

Sale or use of tokens

If tokens are sold or transferred in exchange for goods or services, the transaction generally will be a taxable event and will give rise to capital gain or ordinary income depending on their character. The amount of the gain or loss will be the difference between the token holder's basis in the tokens sold or exchanged and the amount of fiat currency or the fair market value of property or services receives for them.[16]

If the tokens were held as an investment or for trading, then the gain or loss generally should be capital gain or loss, and would be short-term or long-term depending on whether the tokens were held for more than one year. If the tokens were held by an individual as personal-use property and not for investment (e.g., to access media, to shop or for comparable purposes), such property would be a capital asset and any gain (but not loss) recognized on the disposition of such cryptocurrency generally would be treated as described above.

Furthermore, although Notice 2014-21 is silent with respect to the use of tokens in transactions that might otherwise result in non-recognition, presumably the language in Q&A # 1 to the effect that, "general tax principles applicable to property transactions apply to transactions using virtual currency" would cover this situation. Accordingly, the contribution of tokens or cryptocurrency to a corporation in exchange for its stock or to a partnership in exchange for a partnership interest should not result in any gain or loss if a transfer of any other property would result in non-recognition (e.g., pursuant to IRC § 351 or § 721).

If the tokens are not held as capital assets or Section 1231 assets (e.g., if they constitute inventory), and do not qualify for tax-free treatment under a non-recognition provision, the token purchaser would recognize ordinary gain or loss on their sale or exchange. To date, there is no *de minimis* exception for small transactions, and a significant issue for token holders is how to determine the basis of the particular tokens used and the value of the property or services received in return.[17]

Hard forks, soft forks, airdrops and awards/rewards

The term "airdrop," as used currently in an evolving cryptocurrency jargon, means a project founder's distribution of tokens, coins or other digital assets to holders of existing cryptocurrency without any consideration from the token recipient. Generally, airdrops occur when a new blockchain project distributes free tokens to existing holders of certain cryptocurrency such as Bitcoin and Ethereum. Issuers may also issue tokens as rewards for using an app, purchasing merchandise, referring customers, watching advertisements, etc.

A "hard fork" is a material change to a blockchain-system protocol that generally (but not always) results in a split of the existing blockchain protocol pursuant to which the nodes running on the existing version of the blockchain are no longer accepted in the updated version. As a result, a new blockchain is created that follows the updated rules, while the pre-split blockchain that follows the legacy rules still exists. A holder of a pre-split cryptocurrency generally receives additional cryptocurrencies that are generated by the newly created blockchain. For example, Bitcoin hard forks that occurred in August 2017 and October 2017 created a split in the existing Bitcoin blockchain and pre-split Bitcoin holders received Bitcoin Cash and Bitcoin Gold, respectively.

A soft fork is a backward-compatible method of upgrading existing nodes. If a majority consensus is reached for the new rules, then only the new chain is followed. In soft forks, holders may also be required to take affirmative action to get access to or convert their outdated tokens (which may be worthless) for the upgraded tokens.

Generally, a U.S. taxpayer's gross income means all income from whatever source derived,[18] and the Supreme Court defined gross income as an undeniable accession to wealth over which the taxpayer has complete dominion.[19] Thus, it is likely that the IRS would consider receipt of tokens by a taxpayer via hard forks, airdrops or rewards as undeniable access to wealth and therefore taxable.[20] However, it may be difficult to determine the time (if at all) as of which a taxpayer can be considered to have complete dominion over such tokens. For example, most airdrops target owners of Ethereum. However, an Ethereum owner will not have dominion and control over an airdropped token unless such owner's Ethereum is kept on an ERC-20 compatible wallet that supports Ethereum and provides private keys. Thus, if an owner's Ethereum is held on an exchange, s/he will not have any access to (and may not even be aware of) the airdropped tokens.[21] Similarly, at the time of the hard fork of Bitcoin Cash from Bitcoin, holders were provided with an equal number of Bitcoin Cash; however, such holders might not have had dominion and control over the Bitcoin Cash until their wallets were upgraded to support Bitcoin Cash.

Tokens received in hard forks, airdrops, or as rewards generally must be included in income at their fair market value. Most airdropped tokens have zero value at the time of the airdrop and will not result in any taxable income. However, tokens received in hard forks, *e.g.*, Bitcoin Cash, may have a significant value, which can be determined by looking at the price for which it is being traded on an exchange at the time the taxpayer acquires dominion over such tokens. The value of tokens received as rewards will have to be determined based on the facts.[22]

Notice 2014-21 does not provide any guidance for determining the fair market value of tokens that are not listed on an exchange. In such cases, the general rules of taxation apply, and the taxpayer must make a good faith effort to determine the value of such tokens by considering all the relevant factors. The income, if any, of a holder on the receipt of tokens in a hard fork or airdrop or as a reward should be treated as ordinary income as there is no sale or exchange of a capital asset that resulted in such accretion to wealth. The basis in the tokens received should be equal to the amount included in income.

The tax treatment of a soft fork may be different because the holder of the original tokens generally must exchange those tokens for the new tokens to preserve any value. Absent guidance to the contrary, such an exchange is likely to be a taxable event, although arguably the involuntary conversion rules of IRC § 1033 might apply. Generally, gain on such an exchange should qualify as capital gain if the exchanged tokens were held by the taxpayer as personal or investment assets.

Use of a foreign jurisdiction for token issuance

A foreign issuer generally can avoid U.S. taxation on an ICO if it avoids critical contact with the U.S. However, some or all of the income of a foreign issuer can be subject to U.S. tax to the extent the income of the issuer is sourced to the U.S., which will depend on the character of the income (sales, royalties or services), where the management of the entity is located, where decisions are taken, whether marketing activities or sales take place in the United States, and any number of other factors. As a general rule, gain on a sale of personal property by a foreign person is sourced to the jurisdiction of the seller.[23] However, if the tokens constitute inventory in the hands of the issuer (which is likely), special rules apply. If the inventory is considered to be "produced" by the issuer, then the income is allocated and apportioned between sources within and without the U.S. based on where the "production activities" occurred.[24] This might not be readily apparent, although the location of the individuals who developed the concept, the promoters and the IP developers are logical places to start.

Notwithstanding that a foreign issuer might avoid U.S. tax on an ICO, U.S. shareholders of the foreign issuer may not be as fortunate. First, if the IP was developed in the U.S., any contribution of such IP to a foreign corporation in exchange for its stock generally will be a taxable event,[25] and, in certain circumstances, could result in a corporate "inversion" that would cause the foreign corporation to be treated as a U.S. corporation.[26] Any actual sale or license of such IP by a U.S. person to a foreign entity also would result in a taxable event, and would be subject to the U.S. transfer pricing rules.[27] These rules require that payments between related parties for the purchase, license, lease or use of property be set at arm's length rates, which requires that the consideration received (whether as a lump sum or over time) be commensurate with the income attributable to the IP.

Furthermore, income generated by an ICO or from ongoing operations of a foreign issuer that is a controlled foreign corporation ("**CFC**")[28] could give rise to Subpart F income or global intangible low-taxed income ("**GILTI**") that may be includible in the income of any direct or indirect U.S. shareholder of such CFC that owns, directly or indirectly, at least 10% of its voting power or value (a "U.S. 10% Shareholder"). In addition, if a foreign corporation qualifies as a passive foreign investment company ("**PFIC**"), it could generate a roster of issues for certain of its direct or indirect U.S. owners who are not caught by the CFC rules.[29]

Investing, trading and dealing in cryptocurrencies

While the dividing line is blurred, a person generally will be a trader rather than an investor in cryptocurrencies if its trading is frequent and substantial.[30] While both traders and dealers may buy and sell within a very short period of time and take advantage of cross-border price-differential arbitrage, the major distinction between dealers and traders is that dealers have "customers" to whom they are selling rather than simply non-customer counterparties.

Cryptocurrencies held by an investor or a trader generally will qualify as capital assets and gain or loss from their sale or other disposition generally will constitute capital gain or loss, which will be short- or long-term depending on whether the cryptocurrency sold or disposed of was held for more than one year.

Source of income

As a general rule, income from the sale of personal property (other than inventory) by a United States resident is sourced to the United States, and by a nonresident is sourced outside the United States.[31]

Taxation of U.S. traders in cryptocurrencies

U.S. taxpayers who trade in cryptocurrencies may be taxable or tax-exempt (e.g., IRAs or other retirements funds, charitable organizations, etc.). U.S. taxpayers who are individuals generally would be subject to the U.S. federal income tax at rates graduating to a maximum of 37% in the case of short-term capital gains and ordinary income, and 20% in the case of long-term capital gains. Such individual investors may also be subject to the 3.8% net investment income tax ("**NIIT**") on their net investment income, which is likely to include income from cryptocurrencies or a crypto fund.

U.S. taxable investors that are corporations generally would be subject to U.S. federal income tax at a flat 21% rate regardless of whether the income allocated to it is capital gain or ordinary income and regardless of its source.[32]

U.S. tax-exempt entities generally would be subject to tax on any gains from trading in cryptocurrencies only to the extent that such income is characterized as unrelated business taxable income ("**UBTI**"). For this purpose, gains and losses from dispositions of "property" are specifically excluded from UBTI unless the property is subject to acquisition indebtedness or is inventory held for sale to customers in the ordinary course of an unrelated trade or business.[33] Cryptocurrency is classified as "property" for tax purposes. Therefore, assuming an exempt entity is a trader or invests in a fund that is a trader in cryptocurrencies and does not otherwise hold cryptocurrency for sale to customers, its gain might not be treated as UBTI.[34]

Taxation of foreign traders in cryptocurrency

The U.S. taxation of non-U.S. traders in cryptocurrencies depends on whether the income earned is characterized as income that is effectively connected with a U.S. trade or business ("**ECI**") or investment income.

ECI

Trading in stock, securities or commodities constitutes a trade or business for U.S. income tax purposes and, if such activities are carried on in the U.S., they generally will generate ECI. However, there is a limited exception to ECI treatment for gains and losses that qualify for the "Trading Safe Harbor" under IRC § 864(b)(2). Under that provision, foreign persons that trade in stock, securities or commodities (and derivatives based on stock, securities or commodities) in the United States *for their own account* are not considered to be engaged

in a U.S. trade or business. Such trading can be done in the U.S. by the taxpayer through its personnel or through a resident broker, commission agent, custodian, or other agent.[35]

The principal issue for foreign traders in cryptocurrencies is that cryptocurrencies, with limited exceptions, will not qualify as stock, securities or commodities for U.S. tax purposes. The definition of a security for tax purposes is very different than for securities law purposes, and includes only stock in a corporation; interests in widely held or publicly traded partnerships or trusts; notes, bonds, debentures, or other evidences of indebtedness,[36] and it appears unlikely that most types of cryptocurrency could qualify as securities under any of these categories. To qualify as a commodity, a cryptocurrency would have to be traded in and listed on commodity exchanges located in the United States, such as the CME or the CBOE, and not constitute goods or merchandise that are traded in "ordinary commercial channels."[37]

The IRS has issued a private letter ruling involving foreign currencies, which are also treated as "property" for U.S. tax purposes, in which it took the position that in order for trading in a foreign currency to qualify for the Trading Safe Harbor, the *specific* foreign currency in which the trading occurred had to be traded on a commodities exchange.[38]

Bitcoin derivatives are currently traded on exchanges that are regulated by the CFTC trading activity in Bitcoin or Bitcoin derivatives (but not in other cryptocurrencies) may qualify for the Trading Safe Harbor.

Notwithstanding that income from trading in cryptocurrencies may not qualify for the Trading Safe Harbor, if a trader operates from outside the U.S. (i.e., if the trader is an individual, such individual, or if the trader is an entity, its personnel, are located outside the U.S., decisions are taken outside the U.S. and trades are placed outside the U.S.), it should not be considered to be engaged in a U.S. trade or business, and thus should not be taxable by the U.S.

Investment income

Gain or loss from the sale by a foreign individual or entity of cryptocurrency that is held as an investment should not be subject to U.S. tax as it should qualify as capital gain or loss and be sourced to the country of the foreign seller. Again, however, U.S. members of such an entity may be subject to U.S. tax if, *inter alia*, the entity is a partnership or other form of tax transparent entity, or if the U.S. anti-deferral rules apply.

* * *

Endnotes

1. 2014-16 IRB 938, 03/25/2014.
2. IRC § 988(c)(1).
3. Notice 2014-21 Q&A #2.
4. This is complicated by the fact that lots of cryptocurrencies are not fungible. Each time a taxpayer disposes of a lot of, e.g., Bitcoin, the specific lot or lots must be specified in the block. It would be welcome relief if future IRS guidance provides that a simplified accounting method, such as FIFO or LIFO, could be used.
5. Treas. Reg. § 1.861-18(c).
6. *See* Treas. Reg. §1.861-18(c)(ii).

7. IRC § 863(b).
8. It is also possible that some states may take the position that if it is treated as a license to use Software as a Service ("SaaS") or Platform as a Service ("PaaS"), it might be subject to sales and use tax under existing state sales tax rules (for states that tax such services).
9. IRC § 861(a)(4).
10. IRC § 861(a)(3).
11. IRC §§ 861(a)(3), 862(a)(3).
12. *See*, *e.g.*, *Comm'r v. Hawaiian Philippine Co.*, 100 F2d 988 (9th Cir. 1939), cert. denied, 307 US 635; Piedras Negras Broadcasting Co., 43 BTA 297 (1941).
13. IRC § 451(c).
14. *See*, *e.g.*, Rev. Rul. 2003-7; *Estate of Andrew J. McKelvey, et al. v. Commissioner,* 148 T.C. No. 13 (Apr. 19, 2017).
15. IRC § 882(c); Treas. Reg. § 1.882-4(a); *Swallows Holding, Ltd. v. Commissioner*, 515 F.3d 162 (3d Cir. 2008).
16. *See* Notice 2014-21 Q&A #5.
17. Notice 2014-21 Q&A # 13 specifically provides that a person who in the course of a trade or business makes a payment using virtual currency worth $600 or more in a taxable year to an independent contractor for the performance of services is required to report that payment to the IRS and to the payee on Form 1099-MISC.
18. IRC § 61.
19. *See Commissioner v. Glenshaw Glass*, 348 U.S. 426, 431 (1955).
20. *See*, *e.g.*, Treas. Reg. § 1.61-14(a); *Cesarini v. U.S.*, 296 F.Supp. 3 (N.D. Ohio 1969); *Hornung v. Commissioner*, 47 T.C. 428, 1967 (T.C. 1967); *Haverly v. United Case*, 513 F.2d 224 (7th Cir. 1975).
21. *See* Treas. Reg. § 1.451-2(a); Rev. Rul. 80-300, 1980-2 C.B. 165.
22. Perhaps the IRS will see fit to treat tokens received as rewards like frequent flying miles and not assert that such rewards are income unless and until further guidance is provided. *See* Announcement 2002-18, 2001-CB 621.
23. IRC § 865(a).
24. IRC § 863(b).
25. IRC § 367.
26. IRC § 7874.
27. IRC § 482.
28. A CFC is a foreign corporation owned more than 50% (by vote or value) by U.S. persons, each of whom owns directly, indirectly or by attribution at least 10% (by vote or value) of such corporation.
29. IRC §§ 1291-1298.
30. *See*, *e.g.*, *Ball v. Commissioner*, T.C. Memo. 2000-245; *Mayer v. Commissioner*, T.C. Memo. 1994-209; *Holsinger v. Commissioner*, TC Memo 2008-191.
31. IRC § 865(a).
32. *See* IRC § 7201 *et seq*. for tax consequences of not reporting the income.

33. IRC § 512(b)(5).
34. IRC § 512(b)(1).
35. Treas. Reg. § 1.864-2(c).
36. IRC § 475(c)(2).
37. Treas. Reg. §1.864-2(d)(3).
38. PLR 8326013, Dec. 27, 1982.

Mary F. Voce
Tel: +1 212 801 6878 / Email: vocem@gtlaw.com

Mary F. Voce Chairs the Cross Border Tax Planning Practice and concentrates her practice on corporate and international tax. She handles both in-bound and out-bound corporate and international tax planning for U.S. and foreign corporations, U.S. federal taxation of partnerships, limited liability companies, funds and joint ventures. She also handles U.S. federal tax aspects of cross-border corporate mergers, acquisitions and reorganizations, taxation of real estate investments, securities offerings by U.S. and foreign corporations, international projects, equipment leasing and financing. She also handles U.S. federal tax aspects of initial coin offering/first token sales and other tax-related issues on blockchain technology and cryptocurrencies.

Concentrations

- Tax planning for international transactions and investments.
- In-bound and out-bound cross border mergers, acquisitions, reorganizations and joint ventures.
- Aircraft finance and leasing.
- Tax aspects of project finance.
- Investment by foreign investors in U.S. real property.
- Capital markets offerings.
- Global Energy & Infrastructure.

Pallav Raghuvanshi
Tel: +1 212 801 2151 / Email: raghuvanship@gtlaw.com

Pallav Raghuvanshi focuses his practice on U.S. and international tax matters in the context of corporate restructurings and cross-border mergers and acquisitions. He is experienced handling spin-off transactions for large multinational companies, various inbound and outbound transactions involving issues related to foreign tax credits, tax treaties, controlled foreign corporations, and other international reorganization issues. He also handles U.S. federal tax aspects of initial coin offering/first token sales and other tax-related issues on blockchain technology and cryptocurrencies.

Concentrations

- Tax planning for international transactions and investments.
- FATCA.
- Investment by foreign investors in U.S. real property.
- Domestic and international spin-off/split-off transactions.
- Tax planning for initial coin offering/first token sales.
- In-bound and out-bound cross border mergers, acquisitions, reorganizations and joint ventures.

Greenberg Traurig, LLP

MetLife Building, 200 Park Avenue, New York, NY 10166, USA
Tel: +1 212 801 9200 / URL: www.gtlaw.com

Stablecoins:
A global overview of regulatory requirements in Asia Pacific, Europe, the UAE and the USA

David Adams & Jesse Overall, Clifford Chance LLP
Jason Rozovsky, R3

Introduction

A stablecoin is a type of virtual currency or cryptocurrency[1] for which mechanisms are established to minimize price fluctuations and 'stabilize' its value. Historically, stablecoins have been used to pay for purchases of other virtual currencies (e.g., Bitcoin) on cryptocurrency exchanges that did not accept cash, and as a safe-haven asset during periods when other virtual currencies experienced significant price declines. Companies like Facebook, with its recently proposed Libra project, are betting that stablecoins can achieve widespread adoption and change how people make cross-border remittances and payments for consumer goods and services.

To date, the main distinctions among stablecoins have been the mechanisms for maintaining stability (collateralized or uncollateralized) and of governance (centralized or decentralized). Collateralized stablecoins are often backed by fiat currency, commodities (e.g., gold) or other assets, or other virtual currencies held in a reserve. Uncollateralized stablecoins rely on computer algorithms to make monetary policy decisions (e.g., adjusting supply by burning or selling the coins) to maintain a stable value. In either case, governance arrangements – including the role of the issuer or promoter – can vary.

This article describes some of the key legal and regulatory issues raised by the various forms of stablecoins internationally, with a focus on collateralized stablecoins.[2] These issues are receiving greater scrutiny in leading international financial markets, particularly following the announcement of Facebook's Libra project.

Collateralized by fiat currency

Stablecoins collateralized by fiat currencies have predominantly taken one of two main forms to date: either with (1) a fixed redemption value, or (2) a variable redemption value.[3] A stablecoin promising a fixed redemption value (e.g., Tether) has a fixed face value in fiat currency at which it is initially sold (e.g., one U.S. dollar), and the holder can redeem the stablecoin on demand for that amount. Stablecoins offering variable value redemption do not have a fixed redemption amount, instead entitling holders to receive an allocable portion

of the reserve's assets at the time of redemption. The allocable portion of the reserve's assets may differ from the amount initially paid due to fluctuations in the values of the reserve's assets. Facebook's Libra, for example, appears to contemplate variable value redemption,[4] with its reserve consisting of a basket of different fiat currencies and sovereign debt. While most current fiat-backed stablecoins are centralized, Libra aims to outgrow its early dependence on Facebook and other founding members and become governed communally by the projected 100+ members of the Libra Association over time.

Collateralized by commodities

Stablecoins collateralized by commodities or other assets also differ with respect to fixed or variable value redemption. In the former, upon redemption, the holder is entitled to either a fixed quantity of the commodity itself (e.g., an ounce of gold) or a fixed amount of the fiat currency's worth of the commodity (e.g., the amount of gold $1 will buy); while in the latter, the holder receives their allocable portion of the issuer's total commodity reserves at the time of redemption.

Collateralized by cryptocurrency

Stablecoins collateralized by other virtual currencies are increasingly common. MakerDAO, for example, uses two coins, the Dai stablecoin and a MKR token which backs the value of Dai. To issue Dai, a user deposits Ether as collateral, creating a Collateralized Debt Position ("**CDP**"); to retrieve their Ether, users must pay back their Dai together with a variable interest-like fee in MKR tokens, the level of which is set by vote of MKR holders.

Non-collateralized, controlled by algorithm

Certain stablecoins are uncollateralized, with stability instead maintained by algorithm-controlled monetary policy. As proposed in Robert Sams' influential 2014 white paper,[5] a two-coin system would be employed, involving a stablecoin and 'shares' in the monetary system as a whole, with dynamic algorithmic adjustment of the supply of each coin relative to the other, keeping the stablecoin's value consistent.

Stablecoins – applicable regulatory regimes

Although regulation varies significantly between countries, stablecoins potentially raise at least four broad types of regulatory issues in a number of jurisdictions:

- Money movement issues (e.g., money laundering, money services business regulation).
- Investment and trading (e.g., regulation as securities or commodities).
- Banking issues (e.g., deposit-taking, bank registration).
- Virtual currency-specific regulation (e.g., New York's BitLicense, or outright prohibitions in some countries).

United States of America (USA)

While the U.S. legal and regulatory framework for virtual currencies continues to evolve, there are a number of existing laws and regulations that may govern a stablecoin issuance depending on the manner in which such an issuance is structured and the relevant facts and circumstances.

U.S. securities regulatory considerations

From a U.S. securities regulatory perspective, the key issue is whether a stablecoin might be deemed to be a 'security' within the meaning of that term under the federal securities

laws.[6] U.S. Securities and Exchange Commission ("**SEC**") officials have noted that labeling a digital asset a 'stablecoin' does not affect its regulatory status, which instead depends on a facts-and-circumstances analysis of economic reality.[7]

The analysis of whether any given stablecoin is a security[8] would likely employ the so-called '*Howey* test' which is derived from a 1946 U.S. Supreme Court case – *SEC v. W.J. Howey, Co.*[9] – in which the U.S. Supreme Court defined an 'investment contract' as: (i) an investment of money; (ii) in a common enterprise; (iii) in which profits would be expected and derived from the entrepreneurial and managerial efforts of others.

While a stablecoin purchase generally should satisfy the 'investment of money' prong of the *Howey* test, not all stablecoin structures would necessarily satisfy the 'common enterprise' prong of the test. For example, in the case of MakerDAO's Dai stablecoin, each individual user controls whether or not they lose their own 'investment of money' (i.e., their Ether) because they control whether they have deposited sufficient Ether in their CDP as collateral to avoid liquidation. A court might find that their fortunes are not linked to those of any other CDP user[10] or dependent upon the MakerDAO protocol's operator,[11] although it would have to overlook several governance factors, and the fact that Ether collateral belonging to different users is pooled together.

The requirement that there be an 'expectation of profits' from the entrepreneurial or managerial 'efforts of others' may provide a good basis for an argument for stablecoins not being securities under *Howey*. In theory, because the value of a stablecoin is intended to remain 'stable', the absence of value fluctuations should eliminate the ability for a holder to profit from stablecoin ownership, making any 'expectation of profits' unreasonable, a fact the SEC's *Framework for "Investment Contract" Analysis of Digital Assets*[12] (the "**Framework**") explicitly acknowledges.[13] The SEC seems to have further recognized this argument by granting exemptive relief from the securities laws to issuers of stablecoin-like payment tokens that are unlikely to appreciate in value.[14] Where a fixed redemption fiat-backed stablecoin is initially sold by the issuer at $1 and entitles the holder to receive $1 upon redemption,[15] capital appreciation seems impossible, and holders are not typically entitled to distributions.

However, even when a stablecoin is issued at its redemption price, it may trade on cryptocurrency exchanges at a premium or discount, creating opportunities for speculative profit (e.g., if purchased at a discount and immediately redeemed for $1.00, or if sold at a premium without redeeming). A New York court recently stated that Tether's ability to fluctuate in price, notwithstanding its purported stable value, could suggest that it functions as a security.[16] Stablecoin issuers could attempt to eliminate such profit opportunities through selling the stablecoin in unlimited quantities at face value and imposing transfer restrictions, as SEC exemptive relief recently granted to issuers of payment tokens has required.[17] Alternatively, issuers could argue – as in *Noa v. Key Futures* – that any profits from stablecoin trading are due to market fluctuations rather than a promoter's managerial efforts.[18]

The Supreme Court has stated that no profits are expected "when a purchaser is motivated by a desire to use or consume the item purchased."[19] The Framework acknowledges *Howey* is less likely to be met where a 'virtual currency' can immediately be used to make payments in a wide variety of contexts without first being converted to another digital asset or real currency, and substitutes for fiat currency in acting as a store of value that can be saved, retrieved, and exchanged for something of value later.[20] To the extent that a holder's motive is to use stablecoins to make consumer payments, these criteria appear satisfied. In fact,

fixed-redemption fiat-collateralized stablecoins in some instances seem analogous to traveler's checks, functioning as a negotiable medium of exchange and payment mechanism circulating among the general public that can be redeemed for a fixed cash value. Courts have held that American Express traveler's checks are not securities.[21] Furthermore, even though such stablecoin issuers typically maintain cash reserves to back the stablecoin in a bank account, in guidance involving trading stamps redeemable for cash[22] and safekeeping certificates redeemable for gold,[23] the SEC has seemingly not viewed the mere deposit by an issuer/promoter of cash or gold with a bank or other depository for the purpose of meeting customer redemption requests as a 'managerial or entrepreneurial effort' giving rise to an 'expectation of profits'.

However, variable-redemption fiat-collateralized stablecoins and stablecoins relying on stabilization mechanisms other than fiat currency collateral raise difficult issues under the *Howey* test. Redeemable stablecoins backed by a basket of different fiat currencies selected by the issuer, which are capable of appreciating in value, might satisfy the 'expectation of profits from efforts of others' prong unless – as the Framework notes – any value appreciation is truly incidental to the use of the stablecoin for its functionality,[24] or another path outside the securities laws – e.g., the lack of a promoter due to decentralization[25] – is available. As to algorithmic non-collateralized stablecoins, the Framework notes that issuer actions that support a market price for the digital asset, such as by limiting supply or ensuring scarcity, or engaging in token buybacks or 'burning' (removing from circulation) tokens, are likely to constitute 'efforts of others.'[26] Accordingly, where the issuer actively manages monetary policy via algorithmic adjustment of supply, any resulting profits accruing to holders could fall on the wrong side of *Howey*. Further, where monetary policy is managed by distributing new tokens – such as 'seigniorage shares' – to existing stablecoin holders in exchange for stablecoins, not only might such distribution be considered to be a form of 'profit' under the *Howey* test, but – if the new token is a security – then the stablecoin could also be deemed a separate type of statutorily-enumerated security, *even if the stablecoin itself is not an investment contract* – namely, the stablecoin could be a "warrant or right to subscribe to or purchase" a security[27] (i.e., the seigniorage share).

U.S. bank regulatory considerations

Irrespective of the security status analysis, a fixed-redemption fiat-collateralized stablecoin that, for example, is issued in exchange for 1 U.S. dollar and is redeemable for 1 U.S. dollar could be characterized as a 'deposit' within the meaning of that term under U.S. federal and state law, and deposit-taking activities generally trigger bank regulatory licensing considerations. Bank regulatory licensing requirements are triggered in the first instance under the laws of the various states. In New York, for example, the term 'deposit' is not statutorily defined under the New York Banking Law ("**NYBL**").[28] New York case law indicates, however, that a deposit, in the typical banking sense, is the placing of money with a bank to be withdrawn upon the depositor's demand or under rules and regulations agreed upon.[29] Further, New York law generally defines a 'certificate of deposit' as a written acknowledgment by a bank of the receipt of money with an engagement to repay it.[30] Further, despite the lack of a statutory definition of the term 'deposit' under the NYBL, Section 131 of the NYBL sets out "prohibitions against encroachment upon certain powers of banks and trust companies." Among other things, Section 131 prohibits unauthorized persons from issuing notes or other evidences of debts to be loaned or put in circulation as money or receiving deposits.

There is a risk that a stablecoin may be deemed to be an evidence of debt that is put in circulation as money and, accordingly, an issuer of stablecoins in New York most likely

needs to be licensed as a bank or trust company under the NYBL, given Section 131's prohibitions against encroachment upon their powers, or hold the fiat funds received from stablecoin customers in segregated accounts at third party banks. In that regard, it is notable that the issuer of Paxos Standard (PAX), Paxos Trust Company, LLC (the "**Paxos Trust**"), and the issuer of Gemini Dollar (GUSD), Gemini Trust Company, LLC (the "**Gemini Trust**"), are both licensed as limited purpose trust companies under the NYBL. Furthermore, both the Paxos Trust and the Gemini Trust hold the dollar deposits of their customers in omnibus accounts at third-party banks with the intention that they be eligible for Federal Deposit Insurance Corporation ("**FDIC**") 'pass-through' deposit insurance. Other well known stablecoin issuers operating in New York, such as Circle, are not banks or trust companies but have obtained a Bitlicense from the New York Department of Financial Services and maintain U.S. dollars in segregated accounts with third party banks, on behalf of, and for the benefit of, the stablecoin holders. Outside New York, the bank regulatory licensing requirements of other states may vary.

A non-bank issuer of a stablecoin issued in exchange for 1 U.S. dollar and redeemable for 1 U.S. dollar would most likely need to segregate the U.S. dollars it receives in exchange for stablecoins to avoid having to be licensed as a bank. Non-bank financial services entities may hold credit balances on behalf of customers representing cash funds but, generally: (i) may only hold such cash funds for a special purpose; (ii) must obtain a financial services license (e.g., be licensed as a money transmitter, broker-dealer, etc.); and (iii) must segregate such cash funds from their own assets. For example, a U.S. broker-dealer may hold 'credit balances' representing 'customer funds,' but such funds are carried by the broker-dealer in connection with anticipated securities purchases and generally must be segregated from the broker-dealer's funds through deposits at a third-party bank in a 'Special Reserve Bank Account for the Exclusive Benefit of Customers.'[31]

U.S. commodities regulatory considerations

Stablecoins, as virtual currencies, would likely constitute spot commodities subject to the anti-fraud and anti-manipulation authority of the Commodity Futures Trading Commission ("**CFTC**").[32] Provided that they are initially sold at 100% of redemption value, there is no leverage and no periodic margin payments, and physical settlement by actual delivery of fiat currency is always available on demand, typical fiat-collateralized stablecoins are unlikely to constitute derivatives. Accordingly, CFTC registration requirements would not apply to the stablecoins themselves, although derivatives referencing such stablecoins would be fully regulated products. Leveraged products marketed to retail investors would need to consider whether they fall within the ambit of the CFTC's leveraged retail commodity authority.[33]

U.S. money transmission regulatory considerations

At the federal level, money services businesses ("**MSBs**") are subject to registration and regulation as such under FinCEN's regulations, unless an exemption applies.[34] FinCEN was one of the first U.S. federal regulators to assert jurisdiction over transfers of virtual currencies in 2013, when it released guidance identifying certain participants in the digital asset market as 'money transmitters' – a category of financial institution regulated by FinCEN as MSBs. The FinCEN guidance defines the term 'virtual currency' broadly as a "medium of exchange that can operate like currency, but does not have all the attributes of 'real' currency[35] ... including legal tender status."[36] Further, FinCEN guidance states that "convertible virtual currency" ("**CVC**") either has an equivalent value in real currency or acts as a substitute for real currency.[37] Thus, stablecoins generally should be presumed to be CVCs within the meaning of that term under FinCEN's guidance.

An entity that acts as an 'administrator' or 'exchanger' of CVC must register with FinCEN as an MSB, unless it can rely on one of a handful of narrow exemptions.[38] An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency. FinCEN takes the position in its 2019 FinCEN Guidance that CVC issuers generally meet this definition, because at the time of issuance, the seller is the only person authorized to issue and redeem the new units of CVC. This remains true even where the issuer, through contract or otherwise, declines to exercise its authority.

An 'exchanger' is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. Virtual currency exchanges that maintain wallets for their users, or that execute user transactions on a principal or riskless principal basis, would generally meet the 'exchanger' definition. Platforms that merely provide a forum for CVC buyers and sellers to post bids and offers (with or without automatic matching of counterparties) likely would not qualify as 'exchanges,' so long as the users themselves settle any matched transactions through their individual wallets or other wallets not hosted by the trading platform.

The regulatory requirements imposed on MSBs by FinCEN are significant, but far less expansive than those imposed on broker-dealers and other financial institutions regulated by the SEC. In line with FinCEN's statutory mission to combat money laundering, an MSB must: (i) incorporate policies, procedures and internal controls reasonably designed to assure ongoing compliance (including verifying customer identification, filing suspicious activity and other reports, and responding to law enforcement requests); (ii) designate an individual responsible to assure day-to-day compliance with the program and anti-money laundering requirements; (iii) provide training for appropriate personnel, including training in the detection of suspicious transactions; (iv) provide for independent review to monitor and maintain an adequate program; and (v) maintain certain required books and records. FinCEN's authority over MSBs is not comprehensive, however. Instead, its jurisdiction is largely limited to money laundering issues. Unlike the SEC and CFTC, for example, FinCEN does not regulate virtual currency markets, trading, or investment fraud.

At the state level, a stablecoin issuer or exchange may be required to obtain a money transmitter license in the states in which it operates. Money transmitters with a nationwide footprint may need licenses in, and could potentially be subject to examination by regulatory agencies from, all 50 states, although in practice, state authorities may coordinate with one another to reduce redundant examinations. Approximately 38 states participate in the Nationwide Multistate Licensing System, which helps streamline certain regulatory requirements. Notably, U.S. states define 'money transmission' in relation to virtual currencies inconsistently. Some states, like Texas, differentiate between fiat-collateralized stablecoins and those virtual currencies that do not entail ownership claims on fiat currency. While the former constitute 'money' or 'monetary value' for purposes of the Texas Money Services Act, triggering licensure requirements, the latter do not.[39] Other states, like New York, do not differentiate between fiat-collateralized stablecoins and other virtual currencies.[40]

Extraterritoriality of U.S. law: Implications for non-U.S. stablecoin issuers

U.S. laws and regulations relevant to transactions in stablecoins may have an extraterritorial impact, and U.S. regulators and enforcement agencies may seek to apply and enforce such laws where stablecoins are issued to U.S. persons or stablecoin transactions are effected through U.S. intermediaries or IT infrastructure. Thus, non-U.S. stablecoin issuers, brokers,

exchanges, and other market participants must exercise caution if U.S. persons are permitted to transact in stablecoins on their platforms.

Asia Pacific

Australia

In Australia, a range of legislation administered by various regulators (including various license requirements) may apply depending on the characteristics, the legal classification and the related business activities proposed to be carried out in relation to any particular stablecoin.[41] Where a stablecoin falls within the definition of a "financial product", regulations apply, including the requirement to hold an Australian financial services ("**AFS**") license. Analysis will be required on a case-by-case basis, but a stablecoin would most likely constitute a financial product when it has the characteristics of a managed investment scheme, security, derivative and/or non-cash payment (NCP) facility.

If providing advice, dealing, or other intermediary services for a stablecoin deemed to be a financial product, a range of Australian laws apply (including the requirement to hold an AFS license). For example, where a platform deals in stablecoins that are deemed to be financial products, the platform will be considered to be operating a market and a range of Australian laws apply, including the requirement to hold an Australian market license. If transaction processors are part of the clearing and settlement ("**CS**") process for such stablecoins, then a CS facility license may be required. Ministerial exemptions from the applicable regimes may be available on a case-by-case basis.

The development and use of stablecoins in Australia has been limited so far, as has the supply of Australian dollar-linked stablecoins (examples include "AUDRamp", which went live in September 2018 and "TrueAUD" launched in April 2019).[42] Various government agencies including the Treasury, the Reserve Bank and the Australian Securities & Investment Commission (ASIC) continue to study the implications of stablecoins on the Australian economy; however, a tension remains between innovation in traditional centralized payment systems (such as Australia's New Payments Platform) and the innovation of next generation cryptoassets such as stablecoins.[43]

People's Republic of China[44]

Activities relating to virtual or cryptocurrencies[45] are strictly regulated and scrutinized under PRC law. From a PRC legal and regulatory perspective, cryptocurrencies and digital tokens are not currencies issued by competent authorities and therefore may not be circulated or used as currency on relevant markets. Relevant PRC regulations expressly ban licensed financial institutions as well as payment institutions in China from (i) trading virtual currencies, (ii) providing exchange services between any virtual currency and renminbi (RMB), and (iii) providing any financial services in relation to any virtual currency within China. In addition, digital token financing and trading platforms (including private websites and apps) are prohibited from (x) providing conversion services between tokens and fiat money or between different virtual currencies, (y) selling or purchasing (as the central counterparty or otherwise) tokens or other virtual currencies, or (z) providing pricing or information or data intermediary services in relation to tokens.

This means that under the current regulatory environment, stablecoin issuance and usage, together with any other financial activity in relation to stablecoins in China, will be sensitive and subject to close regulatory scrutiny, and thus involve substantial regulatory risks and implications. This will apply whether or not the stablecoin is collateralized. For those who

are considering products with a PRC link, various considerations could be relevant to the regulatory analysis; for example, whether the proposed stablecoin structure could be classed as a blockchain-based payment service rather than a virtual currency issuance, whether the stablecoin could be used within or outside China without any cross-border element, and the identity, licensing status and location of the issuer and other parties.

Hong Kong

The general stance of the Hong Kong Monetary Authority (the "**HKMA**") is that cryptocurrencies, such as Bitcoin, are not 'money' or 'currencies' but 'virtual commodities'. In a similar vein, cryptocurrencies and digital tokens have been, by default, categorized by the Hong Kong Securities and Futures Commission (the "**SFC**") as a 'virtual commodity' or 'virtual asset', which is not a specifically regulated instrument. However, depending on their structure, terms and features, such cryptocurrencies or digital tokens may be considered a regulated instrument.

So far, regulators in Hong Kong have adopted a technology-neutral regulatory approach and are seeking to regulate cryptocurrencies, digital tokens and related activities based on the existing regulatory framework. There are currently neither stablecoin- or cryptocurrency-specific laws or regulations, nor expressed plans to develop new laws or regulations to regulate cryptocurrencies or digital tokens.

Despite this general stance of the HKMA and the SFC, the nature, functionality, rights and structure of stablecoins may not sit neatly within the same classification as the more typical forms of cryptocurrencies and digital tokens. In this respect, a stablecoin issuance could trigger various additional regulatory considerations within Hong Kong, for example:

(i) **Money, certificate of deposit, bill of exchange and/or promissory note** – will the stablecoin resemble the features of such instruments? For example, would there be unconditional orders or promises to pay the bearer of the stablecoin or a specified person the original deposited amount, and is the relevant instrument transferable?

(ii) **Securities (e.g., debentures or collective investment schemes)** – will the stablecoin carry an entitlement or linkage to a certain share of profits, income streams or other returns or rights, options or interests in any shares, stock, debentures, funds, etc.? If not, does it involve participation in profits, income or return from the management of any property?

(iii) **Structured product and/or regulated investment agreement** – will the stablecoin be an instrument with returns/amounts due or whose method of settlement is determined by reference to changes in the price, value or level of any thing or the (non-)occurrence of any specified events?

Moreover, depending on the nature of the stablecoin and the proposed role of the stablecoin issuer, service providers and participants, the following activities relating to the infrastructure, issuance, usage, maintenance and/or transfer of such stablecoin may trigger relevant regulatory licensing, registration or authorization requirements and/or other regulatory compliance considerations:

(i) **Foreign exchange, money remittance and/or money changing services** – is there any element of fiat money exchange (spot or non-spot) or money remittance?

(ii) **Deposit-taking business** – is there any element of taking a deposit (or receiving a loan) from another person?

(iii) **Money broking** – is there any form of negotiation, arrangement or facilitation of currency trading and/or a deposit or loan involving a bank?

(iv) **Stored value facilities/designated payment system** – does it resemble the features of a stored value facility which may be used for storing the value of an amount of money in the context of making payments for goods or services involving the issuer? Could it be a clearing and settlement system or retail payment system that is of such materiality as to be designated for regulatory supervision?

(v) **Moneylending activities** – is there any form of loan, credit or lending facility?

These questions provide an idea of the regulatory considerations but are by no means exhaustive or conclusive. While the relevant stablecoin may or may not fall within the ambit of any one or more of the regulatory areas discussed above (including consideration of various statutory exclusions and exemptions involved), undertaking a detailed factual and legal assessment is a necessary step for issuers to manage their regulatory position and potential risks.

Singapore

In Singapore, offers or issuances of stablecoins may be regulated if they constitute capital markets products (e.g., securities or units in a collective investment scheme) under the Securities and Futures Act (Cap. 289) (the "**SFA**"). The structure and characteristics of a stablecoin would need to be carefully considered to determine whether this is the case. Intermediaries who facilitate offers or issuances of such stablecoins (including operators of platforms on which the stablecoins may be offered, issued and/or traded and those providing financial advice in respect of the stablecoins) may therefore be subject to licensing and other regulatory requirements under the SFA and/or the Financial Advisers Act (Cap. 110) (the "**FAA**").

Further, under the newly introduced Payment Services Act 2019 (the "**PS Act**"), persons who provide e-money issuance services and digital payment token services, among other payment activities, will be regulated. There is a risk that fiat-collateralized stablecoins which are pegged to the value of a currency could be considered as 'e-money' under the PS Act. Digital tokens that are not denominated in or pegged to any currency, such as an algorithm-controlled non-collateralized stablecoin, could potentially be regarded as 'digital payment tokens' under the PS Act. Licensing and other regulatory requirements could apply under the PS Act in these cases. The PS Act is projected to come into operation in late 2019 or early 2020.

While the SFA, FAA and PS Act are key pieces of legislation for activities in respect of stablecoins in Singapore, they are not the only legislative regimes that could apply. Depending on the exact nature of the stablecoin and the related activities proposed to be carried out, other regulatory considerations (such as moneylending and deposit-taking) could also arise.

Japan

In Japan, cryptoasset-related regulations under the Payment Services Act and the Financial Instruments and Exchange Act have been amended to expand the regulations and bring regulatory clarity to those issuing or transacting around cryptoassets. However, as is the case in Hong Kong, stablecoins could, in terms of their legal nature, be different from more typical forms of cryptoassets. For example, fiat-collateralized stablecoins may not be characterized as cryptocurrencies or cryptoassets under Japanese law where their value is pegged to the price of a statutory currency. They may potentially be regarded as prepaid payment instruments, or the function of payment associated with stablecoins could be regarded as money transfer. The necessary license required to issue or otherwise deal with

stablecoins will therefore vary and depend on the legal nature and characteristics of the particular stablecoin.

Various market participants, including banks and tech market players, have announced their intention to issue stablecoins whose value is pegged to the Japanese yen. Also, the Japanese Bankers Association has run a trial of interbank use of stablecoins.

Europe

European Union (EU)

Within the EU, there are no harmonized rules around stablecoins under the existing European legislative framework and most EU Member States do not specifically regulate stablecoins, or cryptoassets more broadly. However, the existence of other (non-cryptoasset-specific) regulatory frameworks creates legal risks and development hurdles for stablecoins within the EU.

Arguably, the EU legal framework that would intuitively apply to stablecoins is the electronic money (e-money) regime set out in the E-Money Directive,[46] given that the EU Commission describes e-money as "the digital alternative to cash, which enables users to store funds on a device (card or phone) or through the internet and to make payment transactions." Under the E-Money Directive, e-money is formally defined as "[1] electronically, including magnetically, stored monetary value [2] as represented by a claim on the issuer [3] which is issued on receipt of funds [4] for the purpose of making payment transactions[47] [...] and [5] which is accepted by a natural or legal person other than the electronic money issuer."

It is likely that any stablecoin would qualify in relation to points 1, 2 and 5 above as electronically stored monetary value which is issued for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer. However, stablecoins do not necessarily represent a claim on the issuer and/or may not be issued on receipt of funds, which would both preclude an e-money classification.[48]

If a stablecoin was created to comply with the definition of e-money, the issuer would have to be licensed under the regulations implementing the E-Money Directive in the EU Member State of the issuer's incorporation. Such license would allow the stablecoin in question to be offered across the EU single market without risking a different categorization and without triggering any marketing restrictions. However, these benefits are quickly outweighed by certain specific requirements that apply to e-money issuers and that may be unsuitable for most stablecoins.

For example, e-money issuers are required to comply with strict safeguarding requirements to protect customers. They must ensure that funds received in exchange for e-money ("**Relevant Funds**") are either (i) placed in a separate account from the institution's working capital and other funds, or (ii) are covered by an appropriate insurance policy or comparable guarantee.[49] When using the first method, it is permissible to invest the Relevant Funds in certain secure liquid assets as determined by the relevant regulatory authority, or retail investment funds licensed in the EU (undertakings for the collective investment in transferable securities or UCITS[50]), but generally speaking there is little flexibility available to the issuer in respect of Relevant Funds. This requirement may be problematic for stablecoins collateralized by commodities or crypto-collateral.

Similarly, e-money holders have the right to redeem the monetary value of their e-money (i.e., the payment from the e-money issuer to the e-money holder of an amount equivalent

to the remaining balance) at any time and at par value.[51] Depending on how local regulatory authorities apply this requirement, this may be problematic for any stablecoin with a variable redemption value calculated by reference to indices, baskets of currencies or any similar formula, but could more easily be complied with for a stablecoin pegged to a particular currency with a fixed redemption value.

The European payment services framework under the Payment Services Directive (the "**PSD**") may also be relevant depending on how a particular stablecoin is used and the environment in which it operates. An example of this is where the stablecoin is used to make payments more effective and efficient or, generally, to provide or facilitate the provision of payment services within the scope of the PSD. These include, among other things, services relating to the operation of payment accounts – for example, cash deposits and withdrawals from current accounts – execution of payment transactions, card issuing, merchant acquiring, and money remittance.[52]

The PSD regulates payment services relating to "funds," which are defined as banknotes, coins, scriptural money and e-money.[53] Therefore, payment services relating to stablecoins that meet the definition of e-money will generally fall within the scope of regulation under the PSD (subject to certain exclusions). Other types of stablecoins may also be used to facilitate the provision of regulated payment services relating to funds; for example, in the context of international money remittance. In this case, the parts of the payment service relating to "funds" (such as fiat currency) would continue to be regulated under PSD2, whilst the other parts of the service involving use of stablecoins may be unregulated, although, the provider would still have to obtain the requisite license for providing the service as a whole.

Where a stablecoin falls outside the scope of the E-Money Directive, there are other EU-wide regulatory frameworks that may apply.

In particular, stablecoins may qualify as units in an alternative investment fund ("**AIF**") under the Alternative Investment Fund Managers Directive ("**AIFMD**").[54] Under the AIFMD, subject to certain exclusions, an AIF is defined as "[1] any collective investment undertaking,[55] including investment compartments thereof, which [2] raises capital from a number of investors [3] with a view to investing it in accordance with a defined investment policy [4] for the benefit of those investors and [5] which does not require authorisation pursuant to the UCITS Directive."

A stablecoin with a redemption value which will vary depending on the performance of a group of underlying pooled assets (which could include fiat-collateralized coins such as Libra) could potentially be classified as an AIF, subject to meeting the various limbs of the definition of an AIF in practice. The effect of this is that the issuance, operation and marketing of such a stablecoin and its infrastructure would be regulated within a legal framework that applies to collective investment undertakings and has not been developed with stablecoins (or cryptoassets) in mind.

Outside the scope of the EU legislative framework, it is also necessary to consider regulatory constraints in each relevant individual EU Member State. While in some Member States, such as the UK and the Netherlands, the position is broadly consistent with the general position outlined above, this is not always the case. For example, in Germany,[56] the regulator has aligned its administrative practice to bring cryptocurrencies into its scope and existing financial services legislation will be extended to cover cryptocurrencies. In Italy, cryptoassets that are not financial instruments may still qualify as 'financial products' (triggering regulation broadly similar to that applicable to financial instruments). The Italian regulator recently launched a consultation proposing the introduction of a bespoke regime

(on an opt-in basis) for cryptoassets that are not financial instruments. Subject to meeting certain requirements (including being offered through licensed platforms), such assets would be exempted from compliance with the 'financial products' framework.

Other jurisdictions, including Malta and Gibraltar, are one step ahead and have already developed bespoke cryptocurrency regimes. In France, the "loi Pacte," enacted in May 2019, introduced a comprehensive new regulatory framework for digital assets. It covers tokens in the primary and secondary markets (i.e., initial coin offerings and digital assets service providers (DASP) respectively), establishing an optional licensing regime alongside a mandatory registration requirement with the French Autorité des marchés financiers (AMF) for providers of custody or fiat/cryptoasset exchange services. It is likely that stablecoins would fall within the scope of the definition of digital assets laid down by the "loi Pacte," thus triggering either the mandatory or optional DASP registration provisions for relevant parties, depending on the type of services being provided in relation to the stablecoins. Bespoke legislation regimes may provide further flexibility than the standard EU position but will need to be considered carefully on a jurisdiction-by-jurisdiction basis.

Russia

For several years, Russia has been trying to adopt a balanced approach to digital assets. Two of the three bills proposed for the regulation of digital assets have recently been passed by the Russian Parliament and signed into law by the President.

The first law, which enters into force on October 1, 2019, introduces the general concept of "digital rights" into the Russian Civil Code but limits those rights to asset-backed and utility tokens, to be issued in an information system, such as a blockchain platform. Both the tokens and the blockchain platform or other information system will have to meet the requirements to be specified in further legislation. The second law regulates crowdfunding platforms, providing for the issuance of "digital utility rights" and enters into effect on January 1, 2020. The third law, which is yet to be adopted, is the key piece of legislation and is expected to introduce a detailed regulation of digital assets in Russia.

Neither the laws that have already been adopted nor the draft law on digital financial assets expressly regulate stablecoins. While it is reasonable to assume that collateralized stablecoins should fall into the category of asset-backed tokens under the Russian Civil Code, they would have to either be expressly referred to, or otherwise satisfy eligibility criteria established by the law on digital financial assets or another specific law.

The attitude of Russian authorities to fiat-collateralized stablecoins may not be favourable as they have historically been negative about payment tokens on the basis that the Rouble must remain the only legal tender in Russia. At the same time, this is a fast-moving area and recently stated opinions of Russian authorities have ranged dramatically from proposing a complete ban on certain categories of digital tokens to giving their full endorsement and affording virtual currencies a status similar to foreign currencies.

Among other issues to be considered in connection with the issue and offering of any particular stablecoin in Russia are relevant regulatory matters (for example, in the case of a collateralized stablecoin, whether storing and managing such collateral is a regulated activity), money transfer and foreign exchange restrictions, as well as restrictions on offering of securities and derivatives established by Russian securities laws.

Middle East – United Arab Emirates (UAE)

In the UAE, there are financial free zones with specific licensing regimes for cryptoassets and payment services activities conducted in these free zones. Outside of such free zones,

'onshore' rules of the Central Bank of the UAE and the Securities and Commodities Authority apply.

The Dubai International Financial Centre ("**DIFC**") and the Abu Dhabi Global Market ("**ADGM**") apply UK-style financial regulations to activities conducted in or from their zones. Therefore, issuing stablecoins would generally be subject to e-money-type payment services licensing in the DIFC and ADGM as is described for the EU above. However, there are additional specific rules to consider in the ADGM.

ADGM financial free zone

The ADGM Financial Services Regulatory Authority ("**FSRA**") published rules and accompanying guidance on June 25, 2018 (amended in May 2019) to create a comprehensive regime for operating a cryptoasset business (the "**OCAB regime**").[57] The OCAB regime covers brokerage, custody, exchange and related activities in respect of specific 'Accepted Crypto Assets' which meet certain criteria (covered below) and are deemed acceptable to the FSRA. It provides a unique bespoke platform for the regulation of cryptoassets, and has been closely followed in approach by the Central Bank of Bahrain in its recent cryptoassets rulebook.

In connection with the OCAB regime, the FSRA has recently issued detailed regulatory guidance specifically in relation to stablecoins, covering how they fit in between its payment services rules and specific cryptoassets rulebook. The FSRA's position is as follows:

(i) It permits only those stablecoins which are fully collateralized 1:1 with fiat, and backed only by the same fiat currency it purports to be tokenizing – therefore other types of stablecoins (such as commodity or crypto-collateralized or non-collateralized stablecoins) may not be permitted.

(ii) Such 'fiat tokens' are to be treated as a mechanism for issuing stored value (e.g., e-money) – similar to the DIFC (see below).

(iii) Issuers of fiat tokens for the purposes of facilitating or effecting payments are treated as money services businesses (i.e., a payment services-type license is required) and will also have to satisfy various cryptoasset-specific rules of the FSRA, including detailed technology standards and acceptance criteria in respect of the stablecoins (see below).

(iv) FSRA license holders must (a) consider which additional FSRA requirements may specially apply to the use of stablecoins, including, for example, what particular risk disclosures may be relevant to investors, and (b) apply the client money rules in the FSRA conduct of business rulebook in respect of fiat tokens.

Of interest, the FSRA also sets out in its guidance various scenarios and how its cryptoasset rules apply on top of traditional payment services rules for stablecoins. In particular, the cryptoasset rules require that the stablecoins themselves must generally comply with a set of criteria for 'Accepted Crypto Assets,' which includes maturity and market capitalisation, security, traceability, reliability of distributed ledger or blockchain network and exchange connectivity. In addition, it is clarified that where a license holder uses a stablecoin purely within its own platform or ecosystem, an additional payment services license will not be required to issue such stablecoin.

DIFC financial free zone

In September 2017, the Dubai Financial Services Authority ("**DFSA**") issued a warning statement to investors that cryptocurrency investments should be treated as high risk. The DFSA clarified that it does not regulate cryptocurrencies, or related initial coin offerings ("**ICOs**"), and that it would not currently license firms undertaking such activities. However,

interest from firms engaging in cryptocurrency business to become licensed in the financial free zones remains high. It is understood that the DFSA is currently considering a licensing regime for cryptoassets. However, it is yet to be determined whether a similar approach to the ADGM would be followed or if, alternatively, a regime tailored towards payments or security tokens (more in line with existing regulated activities within the DIFC) will be adopted.

With respect to stablecoins specifically, DFSA regulations would apply where the activity amounts to 'providing money services,' specifically, money transmission, which means "(a) selling or issuing payment instruments; (b) selling or issuing stored value; or (c) receiving money or monetary value for transmission, including electronic transmission, to a location within or outside the DIFC."

It is likely that most forms of fiat-collateralized stablecoins will fit into the category of selling or issuing stored value. However, other forms of payment services regulation (as well as currency exchange) could apply, depending on the circumstances.

Until now, due to restrictions in its founding law, the DFSA has been restricted in issuing licenses specifically for money services providers (but has permitted existing licensed firms to conduct such activities on an ancillary basis). However, DFSA policy may be changing in this regard. Nonetheless, at present, persons wishing to conduct money services in the DIFC, such as issuing stablecoins to investors, are likely to need to do so as a service ancillary to other regulated activities, such as accepting deposits or arranging investments. This is not inconsistent with most use cases for stablecoins.

Outside the financial free zones

In January 2017, the Central Bank of the UAE established a new licensing framework for persons issuing stored value facilities, which is likely to cover many forms of stablecoin. Currently, the licensing scope is uncertain as implementing rules are awaited (and expected in the coming months) to clarify the rules and permit license applications to be made.

Further, it remains unclear whether the Central Bank intends to regulate virtual currencies. The 2017 Central Bank framework for stored value facilities states that "[a]ll Virtual Currencies (and transactions thereof) are prohibited." Following some confusion in the market, the Governor of the Central Bank issued a statement in February 2017 that clarifying that the regulations "do not cover Virtual Currency" and "do not apply to Bitcoin or other cryptocurrencies, currency exchanges, or underlying technology such as blockchain." Thus far, no public action has been taken in respect of subsequent cryptocurrency activities taking place in the UAE. However, statements from the Central Bank have warned of the risks of dealing with cryptocurrencies and that it may issue future regulations in this area.

In addition, the UAE Securities and Commodities Authority ("**SCA**") regulates derivatives of commodities and, in some cases, 'contracts in commodities' as securities. The SCA has also announced plans to shortly issue a licensing regime for cryptoasset business, focused towards regulating ICOs in the UAE. Whilst most forms of stablecoin will not be covered by such a regime, those which are linked to a basket of reference assets rather than treated as a mechanism of stored value may fall within the remit of the SCA.

Overall, issuing fiat-collateralized stablecoins, as a form of stored value, in the UAE is likely to be regulated as a form of payment services. Where stablecoins fit into other types of cryptoassets, specific restrictions or licensing requirements would apply in the ADGM, but the position is currently unclear in the rest of the UAE. Therefore, in anticipation of additional regulations, a cautious approach should be adopted in the UAE in the absence of engagement with the relevant regulator.

Conclusion

Issuers of stablecoins with a projected global reach (like Facebook's Libra) clearly face a challenging future in navigating this patchwork of international frameworks.

What does this mean for those interested in issuing or marketing stablecoins today? There is no one-size-fits-all solution for designing a regulatory analysis framework for stablecoins. The regulatory analysis will be affected by the laws and regulations of the relevant jurisdictions, the nature and characteristics of the stablecoin, and the activities and/or services relating to such stablecoin. Undertaking a detailed factual and legal assessment is a necessary step for issuers to assess relevant regulatory requirements and potential risks.

Overall, stablecoin issuers must think broadly about what could impact their regulatory position and ask the right regulatory questions. In addition to their home jurisdiction for the initial issuance of the stablecoin, issuers should always consider potentially relevant regulations which have an extraterritorial effect – for example, the regulations of the potential subscribers', users', and other service providers' jurisdictions may affect how an issuer may market to, or accept payments from, such jurisdictions. They should also assess the legal nature of the stablecoin being offered or used in each relevant jurisdiction – the stablecoin may be considered a regulated instrument in one jurisdiction but not another. The issuance, usage, maintenance and/or transfer of the stablecoin by any stakeholder may trigger different regulatory considerations. Furthermore, in light of the potential global operation and usage of successful stablecoins and the increasingly stringent regulatory scrutiny and sanctions around anti-money laundering and counter-financing of terrorism, issuers should also ensure that financial crime concerns are carefully analyzed to comply with applicable regulatory obligations as well as manage reputational risks.

* * *

For more information on Clifford Chance's global fintech capability and resources, or to be added to our weekly global fintech regulatory round-up, please email **fintech@cliffordchance.com**.

Authors and acknowledgments

While market and regulatory developments have dictated that a large focus of this article is on the USA, this article was collaboratively written by a number of lawyers across Clifford Chance's global network of offices. Additional Clifford Chance authors include Thom Beenen in Amsterdam; Kimi Liu in Beijing; Jack Hardman in Dubai, Marc Benzler and Christian Hissnauer in Frankfurt; Rocky Mui in Hong Kong; Diego Ballon Ossio, Peter Chapman, Josephine Chen, Laura Douglas, and Laura Nixon in London; Riccardo Coassin in Milan; Alexander Anichkin, Ekaterina Makarova and Evgeny Soloviev in Moscow; David Felsenthal in New York; Pierre d'Ormesson and Frédérick Lacroix in Paris; Steven Meacher in Perth; Lena Ng and Mae Yen Teoh in Singapore; Kane Barnett in Sydney; Chihiro Ashizawa, Yasuaki Dote, Eiichi Kanda, Naomi Nip and Satoshi Nomura in Tokyo; and Philip Angeloff and Steven Gatti in Washington D.C. Thanks are also due to Ian Macavoy for his careful proofing.

From R3, thanks are due to George Calle and Freeman Lewin, Law and Policy Consultant, for their contributions to this article.

Endnotes

1. The terms virtual currency, cryptocurrency and digital currency are often used synonymously or interchangeably. Use in this article varies depending on regulatory terminology and market practice in the relevant jurisdiction.
2. This chapter reflects legal and regulatory developments up to August 2, 2019.
3. *See* Tobias Adrian and Tommaso Mancini-Griffoli, *The Rise of Digital Money,* IMF FINTECH NOTES: NOTE/19/01, (Jul. 2019), at 4.
4. *See* The Libra Association, *Libra White Paper*, available online at https://libra.org/en-US/white-paper/#introduction, at Section 04: The Libra Currency and Reserve ("one Libra will not always be able to convert into the same amount of a given local currency (i.e., Libra is not a "peg" to a single currency). Rather, as the value of the underlying assets moves, the value of one Libra in any local currency may fluctuate") and Section 05: The Libra Association ("authorized resellers will always be able to sell Libra coins to the reserve at a price equal to the value of the basket").
5. *See* Robert Sams, *A Note on Cryptocurrency Stabilisation: Seigniorage Shares,* (updated April 28, 2015), available online at https://github.com/rmsams/stablecoins/blob/master/paper.pdf.
6. This section does not consider whether stablecoins would be securities under state law (e.g., the 'risk capital' test).
7. Valerie Sczepanik, Senior Advisor for Digital Assets, U.S. Securities and Exchange Commission, *Regulating Blockchain,* Panel at South by Southwest, (Mar. 15, 2019), at 24:35 *et seq.*, https://schedule.sxsw.com/2019/events/PP92908?.
8. A court might also analyze whether stablecoins are "evidences of indebtedness" or "notes" under the federal securities laws. The outcome would likely depend on the extent to which a fiat-collateralized stablecoin is a *bona fide* medium of exchange held for consumer or commercial purposes versus an investment giving rise to an expectation of profits. *See*, *e.g.*, Robert H. Mundheim and Gordon D. Henderson, Applicability of the Federal Securities Laws to Pension and Profit-Sharing Plans, 29 *Law and Contemporary Problems* 795-841 (Summer 1964), at note 45 (noting that, in the context of traveler's checks, trading stamps redeemable in cash or merchandise, and other common products, "not all things which technically might be analyzed as "evidences of indebtedness" are in fact considered "securities" within the meaning of the Securities Act [ ] *The dividing line in these areas between interests which are securities and those which are not might be described as one between media created primarily for exchange and media created primarily for savings or investment.*") (emphasis added).
9. *S.E.C. v. W.J. Howey Co.*, 328 U.S. 293 (1946).
10. *See*, *e.g.*, *Poplar Grove Planting and Refining Co., Inc. v. Bache Halsey Stuart Inc*, 465 F.Supp. 585, 589 (M.D.La. 1979).
11. MakerDAO might argue that it is decentralized and there is no promoter to rely on. *See* Framework, Part II.C.1.
12. Strategic Hub For Innovation and Financial Technology, U.S. Securities and Exchange Commission, *Framework for "Investment Contract" Analysis of Digital Assets,* (Apr. 3, 2019) available online at https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn1.

13. *See* Framework, Part II.C.3 ("[T]he stronger [the] presence [of the following], the less likely the *Howey* test is met [ ] Prospects for appreciation in the value of the digital asset are limited. For example, *the design of the digital asset provides that its value will remain constant* [ ] *over time, and, therefore, a reasonable purchaser would not be expected to hold the digital asset for extended periods as an investment*.") (emphasis added).
14. *See Turnkey Jet, Inc.*, SEC No-Action Letter, (Apr. 3, 2019), available online at https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.
15. *See* Framework, Part II.C.3.
16. Decision and Order on Motion at 23, *In the Matter of the Inquiry of Letitia James, Attorney General of the State of New York, against iFINEX, INC., et al.*, No. 450545/2019 (Sup. Ct. N.Y. County Aug. 19, 2019) ("[T]ether 'goes up and down in value,' 'fluctuat[ing] in price seemingly several cents here and there,' a potentially significant variance in 'dealing with an asset that is supposed to be, quote-unquote, worth a dollar.' [ ] That behavior might suggest that tether actually functions as a security, despite its billing as a 'stablecoin.'").
17. *See*, *e.g.*, *Turnkey Jet, supra*; *see also Pocketful of Quarters, Inc.,* SEC No-Action Letter, (Jul. 25, 2019), available online at https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1.
18. *Noa v. Key Futures, Inc*., 638 F.2d 77, 79 (9th Cir. 1980); *see also Lehman Brothers Commercial Corp. v. Minmetals International Non-Ferrous Metals Trading Co.,* 179 F.Supp.2d 159, 164 (S.D.N.Y. 2001). *But see Balestra v. ATBCOIN, LLC,* 380 F.Supp.3d 340, 357 (S.D.N.Y. 2019).
19. *United Housing Foundation, Inc. v. Forman,* 421 U.S. 837, 852 (1975).
20. *See* Framework, Part II.C.3.
21. *Leighton v. Securities and Exchange Commission*, 221 F.2d 91 (D.C.Cir. 1955).
22. *See*, *e.g.*, *Trading Stamps,* SEC Release No. 3890, 1958 WL 2204 (Jan. 21, 1958); *CMP Corporation*, SEC No-Action Letter, 1978 WL 12200 (Dec. 4, 1978).
23. *See*, *e.g.*, *No-Action Position Relating to Certain Offerings of Gold*, SEC Release No. 5552, 1974 WL 161724 (Dec. 26, 1974).
24. *See* Framework, Part II.C.3.
25. *See* Framework, Part II.C.1.
26. *See* Framework, Part II.C.1.
27. 15 U.S.C. 77b(a)(1).
28. The term "deposit" is defined broadly under the Federal Deposit Insurance Act ("**FDIA**") to include, among other things, the unpaid balance of money or its equivalent received or held by a bank in the usual course of business and for which it has given or is obligated to give credit to an account, or which is evidenced by its certificate of deposit, investment certificate, certificate of indebtedness, or other similar name. The term "deposit" is also defined under Regulation D of the Federal Reserve as, among other things, the "unpaid balance of money or its equivalent received or held by a depository institution in the usual course of business and for which it has given or is obligated to give credit, either conditionally or unconditionally, to an account, including interest credited, or which is evidenced by an instrument on which the depository institution is primarily liable."

29. *See*, *e.g.*, 9 N.Y. Jur. 2d, Banks and Financial Institutions § 219.
30. *See*, *e.g.*, 9 N.Y. Jur. 2d, Banks and Financial Institutions § 266.
31. *See* Rule 15c3-3 under the U.S. Securities Exchange Act of 1934 (17 C.F.R. § 240.15c3-3).
32. *See*, *e.g.*, *CFTC v. Patrick K. McDonnell*, *et al.,* 287 F.Supp.3d 213 (E.D.N.Y. Mar. 6, 2018).
33. *See* Commodity Exchange Act § 2(c)(2)(D).
34. FinCEN is primarily responsible for enforcing the Bank Secrecy Act of 1970, as amended, which generally requires financial institutions to assist U.S. government agencies in detecting and preventing money laundering.
35. FinCEN has defined the term "currency" (also referred to as "real" currency) as "the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."
36. *See Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001* (May 9, 2019) (the "**2019 FinCEN Guidance**"); *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013) (the "**2013 FinCEN Guidance**").
37. *Id.*
38. "Miners," platform users/investors acting for their own accounts, and providers of the delivery, communication, network access, or other services necessary to support the money services business, are not generally subject to regulation as MSBs.
39. Texas Department of Banking, *Supervisory Memorandum 1037: Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act* (rev. Apr. 1, 2019), http://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf.
40. 23 NYCRR § 200.2(p) ("Virtual Currency means any type of digital unit that is used as a medium of exchange or a form of digitally stored value. Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing effort.")
41. See Information sheet 225 from ASIC available online at https://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-crypto-assets/.
42. See Cameron Dark, David Emery, June Ma and Clare Noone "Cryptocurrency: Ten Years On" 20 June 2019 available online at https://www.rba.gov.au/publications/bulletin/2019/jun/cryptocurrency-ten-years-on.html.
43. *Ibid*.
44. "**China**" or the "**PRC**", for the purposes of this article only, excludes Taiwan, Hong Kong and Macau.
45. PRC regulators do not particularly distinguish between digital tokens, cryptocurrency and other concepts related to digital currency under the regulations, and those terms are often used synonymously from a regulatory perspective.
46. Directive 2009/110/EC.

47. The term 'payment transactions' is defined by reference to Directive (EU) 2015/2366, the Payment Services Directive (PSD) and means "*an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing [banknotes and coins, scriptural money or e-money], irrespective of any underlying obligations between the payer and the payee.*"
48. The term 'funds' is not defined in the E-Money Directive. However, it is generally accepted that the definition of funds in the PSD applies and comprises "*banknotes and coins, scriptural money or e-money.*"
49. See Article 7 of the E-Money Directive.
50. Directive 2009/65/EC.
51. See Article 11 of the E-Money Directive.
52. See Annex I to the PSD.
53. See Article 4(25) of the PSD.
54. Directive 2011/61/EU.
55. The term 'collective investment undertaking' is not defined either in the AIFMD or under European law and is *per se* a very broad concept. The European Securities and Markets Authority has specified that it can take any legal form and that a key characteristic is that it "pools together capital raised from investors for the purpose of investment with a view to generating a pooled return for those investors."
56. Germany's Ministry of Finance has provided a draft law to implement Directive (EU) 2018/843 into German law which – among other things – will (i) define cryptoassets as financial instruments, thereby expanding the scope of licensable services under the German Banking Act in relation to cryptoassets, and (ii) implement a license requirement for custodian wallet providers.
57. The ADGM states that it has produced the world's first comprehensive cryptoasset regulatory framework.

David Adams
Tel: +1 202 912 5067 / Email: davidg.adams@cliffordchance.com

David G. Adams is a senior associate in Clifford Chance's Financial Services Regulatory Group. His practice focuses on cross-border financial services regulatory and enforcement work involving both traditional and digital assets. David is also a member of Clifford Chance's US and Global Fintech Groups, and he has authored and co-authored numerous pieces on the intersection of digital assets with existing financial regulatory frameworks.

David's experience in the digital asset space includes advising on US anti-money laundering, data privacy, and securities regulatory issues associated with the establishment of centralized and decentralized exchanges, including SEC broker-dealer and exchange/ATS registration, as well as money transmitter status under FinCEN rules and guidance; and assisting clients in negotiating securities token listing and related agreements.

Jesse Overall
Tel: +1 212 878 8289 / Email: jesse.overall@cliffordchance.com

Jesse Overall is a Capital Markets associate focused on fintech and complex financial transactions. Jesse's experience in the digital asset space includes advising on pioneering security token offerings and real estate tokenization transactions, blockchain M&A deals, crypto lending, virtual currency derivatives, custody, product structuring (including stablecoins) and regulation, technology licensing and service agreements, and membership in open-source protocol consortia. He participates in the Lawyers' Committee of the Chamber of Digital Commerce and the Structured Finance Industry Group's Technological Innovation Committee. During law school, Jesse served as a legal intern at the US SEC and CFTC.

Jason Rozovsky
Tel: +1 347 918 6946 / Email: jason.rozovsky@r3.com

Jason is Assistant General Counsel at enterprise blockchain pioneer R3. Jason joined R3 shortly after its launch and has helped lead the firm's joint software development projects that include financial institutions, technology companies, and regulators for the purposes of testing and launching live applications on Corda, its open-source blockchain platform. Jason further manages critical negotiations and drafting of enterprise blockchain software licensing agreements in the midst of the industry's rapid evolution and changing dynamics.

R3 is an enterprise blockchain software firm working with a broad ecosystem of more than 300 members and partners across multiple industries from both the private and public sectors to develop on Corda, its open-source blockchain platform, and Corda Enterprise, a commercial version of Corda for enterprise usage.

Clifford Chance LLP

10 Upper Bank Street, London, E14 5JJ, UK
Tel: +44 207 006 1000 / URL: www.cliffordchance.com

R3

11 W 42nd Street, 8th Floor, New York, NY 10036, USA
Tel: +1 646 630 7421 / URL: www.r3.com

Blockchain and the GDPR: Co-existing in contradiction?

John Timmons & Tim Hickman
White & Case LLP

Introduction

History is peppered with examples of revolutionary technology fundamentally changing established practices and interactions. These changes present challenges but also create opportunities from a legal perspective. Questions arise as to what extent existing laws are applicable to the technology and whether the new technology should be regulated in a specific manner. There are also often complaints of existing laws inhibiting innovation ushered in with new technology. In the current digital age, these debates have been plentiful[1] and blockchain technology is no exception.

On first appearances, fundamental aspects of blockchain technology seem at odds with certain core principles of European data protection laws. For instance, the permanent record of transactions maintained on the blockchain appears incompatible with an individual's right to deletion of their data as the immutability of data on the blockchain seemingly forgoes the possibility of giving effect to an individual's right to have their data corrected or updated. Similarly, the widespread access to information on the blockchain looks to operate in contradiction with the principle of data minimisation. However, as with a multitude of other matters connected to blockchain technology, the overlap, interaction, tension and compatibility of blockchain technology with European data protection laws is nuanced and complex.

Blockchain is a nascent technology. Advocates of its widespread adoption laud its potential to revolutionise certain industries, common processes and interactions.[2] There can be no doubt that the potential impact of blockchain technology is significant. Whether from a business or societal perspective, the potential for the technology to have a transformative impact is apparent. By way of example, the use of blockchain technology in the electoral system could provide for much greater transparency and assist in establishing confidence in emerging democracies. Similarly impactful is the potential for blockchain technology to provide access to financial products and services to those who have hitherto been excluded from participation in financial markets.

Our focus is on the application of European data protection law (also known as data privacy law) to the use of blockchain technology. The recent adoption of the General Data Protection Regulation (the "**GDPR**")[3] has fundamentally altered the legal landscape in the European Union ("**EU**") and beyond with respect to data protection. The GDPR has created some challenges for the adoption of blockchain technology; however, these challenges are not necessarily insurmountable.

Blockchain technology

It is beyond the scope of our analysis to provide an in-depth technical overview of the

various implementations of blockchain technology. There are more detailed and technically precise explanations throughout this publication and beyond by others who are steeped in the development of this technology.[4]

Blockchain technology is essentially comprised of a distributed digital ledger of transactions that have been cryptographically signed and that are sequentially grouped into blocks. Each block in a blockchain contains a group of transactions. The newest block added to a blockchain refers back to the hash of the previous block, ensuring the immutable nature of the blockchain. Blockchains can be neatly summarised using the following analogy:

> "*In short blockchain technology can be described by comparing it to a spreadsheet in the sky, where each person has the latest version of the document, and everyone can inspect it. Users need to reach a mutual consensus to define its content, and instead of one company […] storing it centrally, every user keeps a copy of the blockchain on their machine.*"[5]

The key components of a blockchain can be summarised as follows:

- **Ledger**: the blockchain is essentially a digital ledger to which new data are continuously appended. The new information records events – often in the form of transactions. Additions do not overwrite the existing content, as can be the case with traditional databases. Instead, the existing content of the ledger is preserved, as new information is added. The impact of this functionality is that all transactions recorded on a blockchain are stored sequentially and in perpetuity. Blockchains grow in size over time as more transactions are recorded, and a record is maintained of every transaction effected on the blockchain.
- **Distributed**: the blockchain is shared amongst all participants (i.e., all machines connected to the blockchain and running the requisite software). It is, in effect, decentralised. Every participant stores a complete copy of the blockchain on their machine (also known as a "*node*"). This functionality creates transparency across the blockchain. The decentralisation of the ledger means that there is no single (centralised) entity that controls the ledger. Through a mechanism embedded in blockchain technology, the ledger can only be appended to following agreement between the various participants.
- **Security**: blockchains are secured using advanced cryptography. The use of cryptography helps ensure that, while new information can be added to the blockchain, information contained in the ledger cannot be altered retrospectively. Since each block refers back to the hash of the previous block, if any information in the previous block changes, the chain will be broken and this will be apparent to all users of the blockchain. As a result, participants can rely on information stored in the blockchain being unaltered. Blockchains are often referred to as "*immutable*" due to the secure way in which information is added to, and protected on, the blockchain.[6]

Blockchains can be either "*permissioned*" or "*permissionless*". In a permissionless blockchain, any person can view and/or add information to the blockchain without authorisation from another person.[7] In a permissioned blockchain, access is restricted according to the persons controlling the blockchain. The distinction between these two types of blockchains is important in the context of compliance with the GDPR as the more unrestricted aspects of the permissionless blockchains present significantly greater challenges for GDPR-compliance.

European data protection law

Data protection law in Europe can trace its roots back to 1953 when the Council of Europe introduced the Convention for the Protection of Human Rights and Fundamental Freedoms, enshrining in law the right to respect for private life.[8] This formed the foundation of data protection law in Europe.

Since then, the law of privacy, and more specifically, data protection, have evolved significantly in Europe. In 1995, the EU adopted a directive for the protection of personal data and established a common standard across Europe with respect to the protection of personal data.[9] More recently, the EU introduced the GDPR, which is the most significant change to data protection law in over 20 years.[10] The GDPR replaced all existing data protection laws in the EU and largely harmonised the law across all EU Member States.[11] It notably updated the existing law and brought much needed clarification. The importance and impact of the GDPR cannot be overstated. It affects almost every organisation within the EU and every organisation that engages with individuals in the EU, even if the organisation itself is based outside the EU.

The GDPR also carries extremely serious penalties for non-compliance. EU legislators and Data Protection Authorities ("**DPAs**") long felt that organisations were not taking their data protection responsibilities seriously. Consequently, the GDPR dramatically increases the maximum penalties for non-compliance to the greater of €20 million, or 4% of global turnover. In 2019, DPAs across Europe have been active in issuing fines for non-compliance, including the UK Information Commissioner's Office, which has issued a notice of its intention to fine an organisation £183 million for alleged breaches of the GDPR.

The bar for compliance has also been significantly raised. The GDPR requires greater openness and transparency, it imposes tighter limits on the use of personal data, and it gives individuals more powerful rights to enforce against organisations that process their personal data.

This is the legal backdrop against which the use of blockchain technology must be considered. Ultimately, the impact of the GDPR on blockchain technology (and vice versa) will depend on how blockchain technology is used, and how it is developed.

The GDPR – key definitions and requirements[12]

Before addressing the ways in which the GDPR and blockchain technology interact with each other, it is important to outline some of the key concepts and requirements underpinning data protection law in the EU.

Data protection law, at its core, is focused on safeguarding the use of information about individuals. Data protection law in the EU is technologically neutral and its application does not depend on the techniques used. The information that is afforded protection under the GDPR is known as "*personal data*" and the individuals about whom personal data are concerned are known as "*data subjects*".

What are "*personal data*"?

The GDPR is concerned with the protection of "*personal data*".[13] The term personal data is defined very broadly. It includes any information relating to an identified or identifiable natural person (i.e., the "*data subject*").

An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online

identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Personal data is interpreted more broadly than the North American concept of "*Personally Identifiable Information*" (or "*PII*") which typically requires that there be some clearly identifiable information present, such as an individual's name. Personal data can include abstract identifiers such as IP addresses.

In the context of blockchain technology, an individual's public key would be considered their personal data[14] and would therefore attract the full range of GDPR compliance obligations. Details of the specific transaction, the associated timestamp, and other information which can be used to single out a specific individual would also be considered their personal data.

What does "*processing*" mean?

The term "*processing*" simply means any use of personal data.

Processing encompasses any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means. It includes actions such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[15] Simply having personal data, or deleting personal data, amounts to processing for the purposes of the GDPR.

Controllers and processors

Beyond data subjects, the other key actors in the context of the GDPR are "*controllers*" and "*processors*".

A controller is the person or organisation that, alone or jointly with others, determines the purposes for which, and means by which, personal data are processed.[16] For instance, an employer would typically be a controller with respect to its processing of employee personal data in the context of the employment relationship (i.e., to pay wages, provide benefits etc.).

A processor is any person or organisation that processes personal data on behalf of the controller.[17] For example, if an employer engages a third party payroll provider, this third party would typically be a processor, acting on behalf of the employer (which is the controller).

The determination of whether an organisation is acting as a controller or processor is a question of fact. Parties to data protection-related contracts often include language purporting to identify the role of each party from a data protection perspective. Whilst this is a common commercial practice, it is not determinative if the facts are contrary to the wording of the contract.[18]

In the context of blockchain technology, identifying the controller and processor presents particular challenges, as discussed in more detail below.

When does the GDPR apply?

In short, controllers bear primary responsibility for GDPR compliance, but both controllers and processors must comply with their respective compliance responsibilities when processing personal data.

The GDPR has a broad territorial scope. It applies to all organisations (both controllers and processors) that are "*established*" in the EU[19] (effectively, all organisations with a corporate seat or permanent presence in the EU). In addition, organisations established outside the EU may also be subject to the GDPR if they: (i) offer goods or services to individuals located within the EU; or (ii) monitor the behaviour of individuals within the EU.[20]

Organisations that have some touch point with the EU, whether in respect of their customer/user base or their physical presence (for example, through an office, branch, or local agent), must be cognisant of the possibility that the GDPR may apply to their personal data processing activities.

There are some exemptions to the application of the GDPR. For example, an individual processing personal data purely in a personal capacity (i.e., for non-business/non-professional purposes) is not subject to the GDPR.[21] This is relevant in the context of blockchain technology, particularly in permissionless blockchains that are used by individuals in a private capacity.

Key requirements of the GDPR

The GDPR requires that personal data be processed in accordance with six key principles:[22]

1. **Lawfulness, fairness and transparency**: processing of personal data must be justified by a valid legal basis.[23] It must also be clear to the relevant individual that their personal data are being processed, and every relevant individual must be provided with information about the identity of the controller and the purposes of the processing.[24]
2. **Purpose limitation**: personal data must only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.
3. **Data minimisation**: personal data collected must be "*limited to what is necessary*" for the relevant purposes. Organisations must be careful not to collect any personal data that are not strictly "necessary" in connection with the relevant purposes.[25]
4. **Accuracy**: personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.
5. **Storage limitation**: personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. **Security**: personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This obligation is not absolute, but takes into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the relevant processing.

It is the responsibility of controllers to comply with these principles and to be able to demonstrate its compliance with these principles.[26]

The GDPR and blockchain technology: Points of conflict

Blockchain technology in itself does not contradict the GDPR. Rather, it is the way in which personal data could be processed when blockchain technology is used that gives rise to points of conflict. Both the GDPR and blockchain technology are concerned with transparency of information usage, and ensuring individuals have control over the use of their information; however, it is fair to say that blockchain technology and the GDPR have divergent approaches on addressing these concerns.

On the one hand, the GDPR envisages clearly defined actors bearing responsibility for compliance with the relevant requirements. Relevant entities are expected to govern their

relationships in accordance with the GDPR and ensure that the rights of individuals with respect to their personal data are being safeguarded. These entities are subject to enforcement of the GDPR by the relevant DPA(s). On the other hand, blockchain technology envisages information (including personal data) being protected through the immutable nature of the distributed ledger, in a transparent manner and through the use of advanced cryptography, with no system of centralised enforcement. These core features of blockchain technology operate to safeguard the information stored on the blockchain and ensure its integrity.

We address some of the key issues with respect to the use of blockchain technology in compliance with the requirements of the GDPR. This is not an exhaustive list of the issues, but instead is focused on the following fundamental points: (i) the scope of personal data; (ii) the identification of controllers and processors; (iii) international transfers of personal data; (iv) giving effect to individual rights in respect of personal data processes in the context of the blockchain; and (v) the need to undertake a data protection impact assessment ("**DPIA**") prior to the use of a blockchain.

Personal data and the blockchain

The GDPR is only relevant where there is processing of personal data. If no personal data are stored on the blockchain, GDPR compliance is unnecessary. However, as set out above, the GDPR adopts a broad and far-reaching approach to the definition of personal data. Unless the blockchain is permissioned, accessible only by corporates, and the information contained on the blockchain relates only to corporate transactions, excluding personal data from a blockchain can be incredibly challenging. Outside of very narrow circumstances, almost all implementations of blockchain technology will involve the processing of personal data, and will therefore be potentially subject to the GDPR.

Blockchains typically include information about: (i) the users carrying out transactions ("**user information**"); and (ii) information about the transactions being carried out ("**transaction information**"). Transaction information can encompass anything that can be recorded digitally. Its content will typically be driven by the purpose of the relevant blockchain. Transaction information may be stored on the blockchain in different formats. For example, it may be open and readable to all who have access to the blockchain, it may be encrypted, it may be hashed, or it may be stored in another form.

User information is the information used to identify particular users carrying out transactions on the blockchain. Typically, blockchains make use of identifiers that do not directly reveal the identity of the user. Where the users of a blockchain are individuals, their user information and transaction information will, in most cases, be considered personal data. This is because it is, in theory, possible to link information on a blockchain back to an individual. Even if such identification is unlikely, and even if it would require the use of information held confidentially by a third party, the fact that identification is possible in principle means that the information would almost certainly be treated as personal data for GDPR purposes.[27]

In effect, this means that where individuals are using a blockchain, even if no personal data are contained within the transaction information, the user information (and therefore any associated transaction information) will likely be considered personal data if it is possible to identify an individual user, even if such identification is unlikely. Accordingly, personal data are being processed in the operation of almost all blockchains.

Due to the nature of blockchain technology, and the requirements of the GDPR, the complexities of compliance with the GDPR will increase significantly when the transaction information contains personal data.

Storing personal data on the blockchain is therefore generally not advisable. On this point, most authorities and experts agree. There are a number of ways of ensuring that personal data as such are not stored on the blockchain and are stored "off-chain" instead. For instance, one solution is to store information on the blockchain that refers to information stored off-chain. This approach (as discussed below in more detail) allows for individuals' rights to be exercised, and will generally make compliance more straightforward. It is worth noting that, even when adopting this approach, the information stored on the blockchain would likely be considered personal data, provided the identifying information stored off-chain continues to exist.[28] Similarly, layering of blockchains can be an effective means of safeguarding personal data to exposure from the risks presented by permissionless blockchain solutions. This involves storing non-personal data on a permissionless blockchain, which is derived from personal data stored in a separate, permissioned blockchain.

Where personal data are to be stored on the blockchain, an approach suggested by some is to apply encryption to such data. Once the personal data are no longer necessary, or for some other reason must be deleted, the keys required to decrypt the information can be deleted and thereafter access to the personal data becomes virtually impossible. There is some debate as to whether this approach can achieve the goal of fully anonymising personal data in the blockchain – if it does, it would mean that the GDPR is inapplicable to the processing of those data. However, this approach has not been tested before courts and regulators and so there remains some doubt as to whether it would be permissible. In addition, it is possible that data that cannot be decrypted with current technology might be decrypted with future technology, meaning that such data would become personal data once more.

Ultimately, where a blockchain has individual users, it is likely that personal data will be processed simply by virtue of the blockchain operating (i.e., as user and transaction information is processed). There are many ways to limit the volume of personal data featured on the blockchain and to obfuscate the personal data which may reduce risk and exposure to the GDPR. However, compliance with the GDPR remains a key consideration, due to the fact that full anonymisation of a blockchain is extremely difficult to achieve, and is subject to being reversed by future technologies.

Identifying the controllers and processors in a blockchain

Controllers

Determining the identity of the relevant controller(s) is fundamental. In the absence of a controller, there is no entity responsible for compliance with GDPR. The GDPR anticipates there being a single identifiable entity (i.e., the controller), or group of entities (i.e., controllers in common, or joint controllers) responsible for the processing of personal data and responsible for compliance with the requirements of the GDPR in respect of such processing.

The decentralised nature of blockchain technology presents challenges in identifying the relevant controller(s). As set out above, in a typical blockchain, each participant (i.e., anyone who joins the blockchain and operates the relevant software) becomes a node.[29] A node is a machine connected to the blockchain that maintains a copy of the ledger. Nodes can also contribute information to the blockchain in the form of completed transactions.

In a permissioned blockchain, the challenge of identifying the controller is more manageable. There will be an entity(ies) responsible for granting or refusing access to the blockchain. That same entity(ies) will also likely be responsible for determining the functionality of the

particular blockchain. As such, this entity(ies) will most likely be considered the controller of the processing of personal data occurring on the blockchain. Other entities granted permission to the blockchain may also be controllers, depending on how the blockchain is used. Through this permissioned model, compliance is generally more straightforward. The key actors are identifiable, and between them, the compliance requirements of the GDPR can be tackled.[30]

In a permissionless blockchain, the challenge of identifying a controller is particularly acute, since there are no restrictions on those who can participate in the blockchain, and therefore anyone can potentially store a copy of the ledger or add to it.

The French DPA (the "**CNIL**") has outlined its opinion of the identity of controllers in both permissioned and permissionless blockchains.[31] The CNIL adopts the position that any blockchain participant that has the right to write on the blockchain, and who can decide to send data for validation to other blockchain participants, is a controller. Although it is questionable whether any participant in a blockchain truly controls the processing, participants do decide to join the blockchain, they run the relevant software and the purposes and means of the processing are clear. The CNIL's approach therefore seems reasonably pragmatic.[32] Whilst this is a neat solution, a further level of analysis is required.

Application of the GDPR

If it is accepted that blockchain participants who have the right to append data to the blockchain, and who can decide to send data for validation to other blockchain participants, can be considered controllers ("**Controller Participants**"), the next issue to resolve is whether the GDPR in fact applies to such Controller Participants.

Firstly, for the GDPR to be applicable, the Controller Participants must be:

(i) established in the EU (for example, a Controller Participant could be a business entity incorporated and headquartered in France, or an individual living in Italy); or

(ii) established outside of the EU, but offering goods or services to individuals inside the EU, or monitoring the behaviour of individuals inside of the EU (for example, a US-based business offering cryptocurrency-related services to individuals on a global basis, but with a website available in EU languages and which accepts payments for services in euros).

A case-by-case analysis will be needed in order to determine whether any given Controller Participant in a blockchain is actually subject to the GDPR. It is possible that where there are multiple Controller Participants, these entities act as joint controllers. This gives rise to additional compliance requirements, including the need to provide information to individuals explaining which of the controllers is responsible for giving effect to the individuals' rights.[33]

Secondly, in respect of Controller Participants that are individuals based in the EU (therefore satisfying (i) above), it must further be resolved whether these individuals are acting in a purely personal capacity or in a business capacity. If acting in a purely personal capacity, these individuals will benefit from the exemption in the GDPR and will fall outside of its application.[34]

It is therefore quite possible in the context of a permissionless blockchain that there will be a combination of Controller Participants, some of whom are who are subject to the GDPR, some of whom are outside of the scope of the GDPR due to their geographic location and processing activities, and some of whom are within the scope of the GDPR but are exempt as a result of their use of blockchain for purely personal purposes.

Processors

Of course, not all blockchain participants are controllers. Some participants act only to validate transactions submitted by other participants and do not contribute new information to the blockchain. In other words, these participant nodes only assess and validate the information submitted by Controller Participants. These entities would likely be considered processors ("**Processor Participants**"), acting on the instructions of the Controller Participants.

Processor Participants may be:

(i) directly subject to the GDPR established in the EU (for example, a Processor Participant could be a business entity incorporated and headquartered in Spain which has multiple nodes participating in a blockchain in a validating capacity only); or

(ii) indirectly subject to the GDPR, by virtue of having to enter into an agreement with the Controller Participant that imposes certain GDPR compliance obligations on the Processor Participant.

The GDPR requires that controllers enter into contractual terms with processors which satisfy particular requirements.[35] Therefore, Controller Participants subject to the GDPR must enter into contractual arrangements with Processor Participants. In a permissionless blockchain, this may be an extremely challenging exercise due to the potential number and geographical distribution of Controller and Processor Participants.[36] In a permissioned blockchain, this issue can be addressed as part of the governance requirements when access is granted to participants.

It should be noted for completeness that Processor Participants established in the EU processing personal data for Controller Participants not established in the EU will only be required to comply with the requirements of the GDPR that are applicable to processors. Furthermore, Processor Participants established outside of the EU processing personal data for Controller Participants not subject to the GDPR will also not be subject to the GDPR themselves (either directly, or indirectly by contractual terms).

International transfers

A further complication for compliance with the GDPR arises in the context of international transfers of personal data.

The GDPR imposes requirements on controllers when transferring personal data to recipients located outside the European Economic Area (the "**EEA**").[37] The rationale for this is that the protection of personal data should not be undermined by a controller in the act of transferring it to a jurisdiction which does not offer a similar level of protection.

Transfers of personal data are permitted without further compliance measures, provided the personal data are transferred within the EEA, or to a recipient located in a non-EEA jurisdiction that the European Commission has determined offers an "*adequate*" level of protection for personal data.[38] Where personal data are transferred to a jurisdiction outside of the EEA, which has not been deemed adequate, the transfer can still be permitted, provided that "*appropriate safeguards*" have been implemented.[39] Although there are a number of options available, the most commonly relied upon solution are a standardised set of contractual obligations which help protect personal data when it leaves the EEA (the "**Standard Contractual Clauses**"). The Standard Contractual Clauses protect personal data by imposing obligations on the controller transferring the personal data and the entity receiving the personal data (which may be a controller or a processor). They also confer

rights on the individuals whose personal data are being transferred, and those rights can be exercised against the transferring or recipient entity.[40]

In a permissionless blockchain, complying with the requirements on international transfers will be extremely challenging, as the blockchain participants could be located in any jurisdiction. Appending data to the blockchain and sending it for verification effectively amounts to a cross-border transfer of data for GDPR purposes. Compliance with the GDPR would require a Controller Participant to have a clear understanding of the location of all other Controller Participants and Processor Participants. A GDPR-compliant international transfer solution would then have to be implemented with each Controller and Processor Participant located outside of the EEA and not in an adequate jurisdiction. Depending on the size and nature of the particular blockchain, this could be an impractically time-consuming exercise.

In a permissioned blockchain, this issue can be tackled in a more straightforward manner. For example, the Standard Contractual Clauses could be incorporated as part of the overall governance strategy. Participating entities in a permissioned blockchain could be required to sign up to an international data transfer agreement incorporating the Standard Contractual Clauses as a condition of participation. This would ensure that all participants were signatories to the relevant agreement and would allow for the free flow of personal data throughout the blockchain and across jurisdictional lines.

Giving effect to individual rights on the blockchain

A key feature of blockchain technology is the creation of a permanent, immutable, transparent ledger of all transactions that have been effected on the blockchain since its inception. This essential feature of blockchain technology is what sets it apart from other technologies and is the reason its many advocates believe it will be so revolutionary.

However, this core functionality of blockchain technology could give rise to GDPR-compliance issues.

Retention and the right to erasure

The GDPR requires that personal data must not be kept longer than is necessary in connection with the purposes for which it is processed.[41] Indefinite retention of personal data runs contrary to the storage limitation principle enshrined in the GDPR.[42]

Complementing this storage limitation requirement is the right of erasure conferred on individuals.[43] Individuals have a right to require controllers to erase their personal data in certain circumstances, such as when the personal data are no longer necessary for the purposes for which they were collected or the individual objects to the continued processing of their data.[44]

Should personal data be stored on the blockchain (which is not advisable from a legal perspective, for the reasons set out above, but is often unavoidable from a practical perspective), it is difficult to reconcile the core features of blockchain technology with the requirements of the GDPR. Whether this can be done will ultimately depend on the nature of the blockchain implementation. For instance, in the context of giving effect to personal data erasure requests, it is not immediately apparent to whom individuals should direct their requests towards. It would be almost impossible (without significant computational power and control of the majority of participating nodes on the blockchain) to give effect to an individual's request for their personal data to be erased on a permissionless blockchain if such personal data is stored on the blockchain. If, however, the blockchain has been designed

to ensure that personal data are stored elsewhere (i.e., off-chain), then the right to erasure could, in principle, be honoured by deletion of the off-chain information.

If personal data are stored on the blockchain in an encrypted form, and the erasure requested relates to such personal data, it has been suggested that the right to erasure could be given effect to by simply deleting the encryption key needed to access the data in question. Although this "moves closer" to giving effect to the right to erasure, it is considered in some quarters to be a compromised solution as it does not lead to the actual erasure of personal data stored on the blockchain.[45] Deletion of the requisite key associated with the encrypted data would place the personal data effectively beyond use at present; however, there are no guarantees that this approach will be suitable as a long-term solution. As computing and processing power continues to increase, the encryption methods used today are likely to become easier to solve therefore making the previously inaccessible personal data accessible once more – turning anonymised data back into personal data, and rendering ineffective any attempt at erasure through deletion of the encryption key.

Controller Participants will need to consider form the outset how they will give effect to the storage limitation and the right to erasure. Ultimately, the optimal approach would be to refrain from storing any personal data on the blockchain. If personal data are to be stored on the blockchain, controllers should give careful consideration to how to delete the personal data in the future, whether to comply with the storage limitation requirements, or whether to give effect to an individual's right to erasure. Alternatively, Controller Participants might decide to run the risk of disregarding the GDPR rights of individuals. However, given the fact that regulators have announced GDPR fines totalling more than £300 million so far this year, this is unlikely to be a wise approach in most cases.

It will be more straightforward to give effect to the right to erasure in a permissioned blockchain where the relevant entities can agree to a technical solution that does not undermine the rights of individuals. There could also be an outright prohibition on storing personal data in a permissioned blockchain, and insistence instead on the use of off-chain information sources.

Data accuracy and the right of rectification

The issues we have outlined above, in connection with data retention and the right to erasure, are similar to the issues that arise in the context of the GDPR requirements for data accuracy and the individual's right to have inaccurate data rectified.[46] One of the key differences between the right to rectification and the right to erasure, is that the right to rectification is absolute. It is not qualified and it is not subject to any exceptions.

Blockchain technology is concerned with creating a permanent and immutable digital ledger, which operates to preserve the data stored thereon. Blockchains do not assess the accuracy of the information appended by participating users. As such, blockchains can operate to preserve inaccurate personal data. For instance, if a Controller Participant operating on a permissionless blockchain stores personal data on the blockchain that is subsequently shown to be inaccurate, such personal data could not, in practice, be updated or be corrected without breaking the blockchain. This creates a problem from a GDPR-compliance perspective: the inaccurate data are enshrined for the lifespan of the blockchain. For the reasons discussed above, in a permissionless blockchain, amending historic data is practically impossible.

Clearly, the most GDPR-compliant approach to these issues is to avoid storing personal data on the blockchain altogether. Using an off-chain data storage approach, as outlined above, would circumvent the issue in many cases. There are alternative solutions where personal data has been stored on the blockchain, such as recording corrections in subsequent blocks

added to the blockchain; however, these do not fully meet the requirements of the GDPR, because the inaccurate data would remain on the blockchain, and would continue to be processed in each subsequent transaction.

Addressing data accuracy and facilitating the right to rectification is significantly more attainable in the context of a permissioned blockchain than a permissionless blockchain.

Is use of blockchain technology necessary?

As the hype around blockchain technology swells, and the pressure to adopt blockchain solutions increases, businesses should first stop to consider whether the use of blockchain technology is necessary, and whether it will bring value to their offering. This is equally true when assessing data protection compliance.

A data protection impact assessment is a tool that is intended to assist controllers in analysing, identifying and minimising data protection risks associated with a particular processing activity. It is a fundamental component of compliance with the accountability requirements of the GDPR.[47] It can also help to support an organisation's compliance with the principle of data protection by design and by default.[48]

In certain circumstances, the GDPR requires organisations to perform a DPIA.[49] Guidance issued on this requirement outlines specific examples of scenarios where a DPIA must be carried out.[50] The use of blockchain technology itself may not trigger the need to conduct a DPIA; however, if there is an intention to process personal data using blockchain technology, a DPIA would be necessary in many cases.[51]

As discussed above, the use of blockchain technology can have a significant impact on the rights of individuals with respect to the processing of their personal data. This, coupled with the fact that new technology is being used, would likely trigger the need to conduct a DPIA, due to the potential for harm to the rights and freedoms of affected individuals. In any event, even if a DPIA is not strictly required, organisations would be well-advised to conduct an assessment so as to identify and minimise any data protection-related risks. A DPIA need not eliminate all data protection-related risks; however, it should assist organisations in identifying and minimising such risks, and in determining whether or not the level of risk identified is acceptable in the circumstances, taking into account the benefits of what the organisation is seeking to achieve.

As noted above, closely tied to the DPIA process and the rationale underpinning it, is the requirement for organisations to give effect to the principle of data protection by design and by default.[52] In essence, data protection by design and by default requires organisations to "*bake-in*" data protection compliance to their processing activities. This would apply to the use of blockchain technology where personal data are being processed.

Organisations must, at the time of determining the means for processing, and when carrying out the processing itself, implement appropriate technical and organisational measures designed to apply the data protection principles enshrined in the GDPR and integrate safeguards into the relevant processing activity so that the requirements of the GDPR are being met and individuals' rights are being safeguarded.

Clearly, the requirement to apply the principle of data protection by design and default to the processing of personal data in the context of blockchain technology, gives rise to compliance risks, particularly in permissionless blockchains.

The GDPR requires organisations to take account of a number of factors when applying the principles of data protection by design and by default. For example, consideration should

be given to: the state of the art, the cost of implementation, and the nature, scope, context and purposes of processing.[53] It is therefore arguable that, in the deployment of a blockchain that will involve the processing of some personal data, the GDPR does not rule out the possibility that an organisation may weigh its interests, and the benefits of using technology such as blockchain, against the interests of the individuals whose personal data are being processed.

Both the requirement to conduct DPIAs and the need to take account of privacy by design and by default present clear challenges in the context of blockchain technology. These challenges may be more readily met in the context of a permissioned blockchain where the identified risks can be managed with a greater degree of control and the technology more readily adapted to take account of changes.

Conclusions

Blockchain technology has the potential to disrupt well-established industries and practices and it may result in fundamental changes in the way in which ordinary persons interact with one another as well as with businesses. Its deployment brings with it a multitude of opportunities, but it also creates complex compliance challenges from a data protection perspective. Some of the fundamental features of blockchain technology sit uncomfortably alongside the requirements imposed by the GDPR.

These challenges are not necessarily insurmountable in all cases. The impact and extent of the compliance challenges depend on factors such as the nature of the blockchain itself, and the information that is processed on it.

At present, permissionless blockchains present the largest challenges in the context of GDPR compliance. Due to the potentially unlimited number of persons with access to the ledger, the proliferation of the ledger across multiple jurisdictions, and the consensus model which applies to the management of information on the blockchain, some requirements of the GDPR cannot be met with current technology. Of course, these issues can be addressed with technical solutions, innovative uses of permissionless blockchains and by limiting the volume of personal data stored on the blockchain, but serious GDPR compliance challenges will remain for the foreseeable future.

The permissioned blockchain model presently offers the best opportunity for compliance with the requirements of GDPR. This model allows the organising entities to establish a governance framework for the participants on the permissioned blockchain. Roles can be clearly defined, contractual provisions satisfying the requirements of the GDPR can be put in place, an international data transfer framework can be implemented, a means to provide individuals with the relevant information can be established and technological solutions giving effect to individual rights can be built into the blockchain.

Organisations considering the use of blockchain technology should:

(i) consider whether a blockchain is necessary to achieve the organisation's goals;

(ii) assess whether, and to what extent, the GDPR applies to the proposed blockchain;

(iii) consider the type of blockchain to be used (such as a permissioned blockchain model);

(iv) undertake a DPIA to identify and address data protection-related risks;

(v) implement data protection by design and by default principles;

(vi) restrict (and where possible, prevent) personal data being stored on the blockchain;

(vii) implement technological features in the blockchain to allow individuals to exercise their rights;

(viii) establish a governance framework for participants in the blockchain that aims at achieving compliance with the requirements of the GDPR; and

(ix) proceed with caution, in the knowledge that many aspects of GDPR compliance have yet to be fully tested in the courts, and an adverse court decision could have major implications for any business that is processing significant volumes of personal data using blockchain technology.

* * *

Endnotes

1. By way of example, see Niels Schaumann, "Copyright Infringement and Peer-to-Peer Technology", *William Mitchell Law Review* (2002), Vol. 28, No. 3, p. 1001.
2. For comparisons between the adoption of TCP/IP which were foundational to the development of the internet, see Marco Iansiti and Karim R. Lakhani, "The Truth About Blockchain", *Harvard Business Review* (January-February 2017 issue) (available at https://hbr.org/2017/01/the-truth-about-blockchain).
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
4. For example, see: "Blockchain Technology Overview", *NIST Interagency/Internal Report (NISTIR) 8202* (available at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.202.pdf); and "How does a blockchain work – Simply Explained" (available at https://www.youtube.com/watch?v=SSo_EIwHSd4).
5. Simon Schwerin, "Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study", *The Journal of The British Blockchain Association*, Vol 1, Issue 1, pp. 1–75.
6. It may be more accurate to describe the blockchain as "tamper resistant" and "tamper evident", as under the normal operation of the blockchain, information cannot be changed once it has been added to the blockchain (although it is technically possible to change the information). See "Blockchain Technology Overview", *NIST Interagency/Internal Report (NISTIR) 8202* (available at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf).
7. Bitcoin is an example of a permissionless blockchain.
8. Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (available at https://www.echr.coe.int/Documents/Collection_Convention_1950_ENG.pdf).
9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

11. There remain some matters which the GDPR defers to Member States, which creates some divergences in approach between EU countries. For example, the following matters must be determined by each Member State: the age of consent for children; the grounds for processing personal data relating to criminal convictions and offences; and the limits that can be placed on individual rights and the scope of processing activities covered by "public interest".
12. For a more comprehensive overview on the GDPR, see Tim Hickman *et al.*, "GDPR Handbook: Unlocking the EU General Data Protection Regulation", *White & Case LLP* (available at https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation).
13. Article 4(1) of the GDPR.
14. The broad approach to the interpretation of the term personal data is emphasised by the European Data Protection Board (formerly, the Article 29 Working Party) in Opinion 4/2007 on the concept of personal data (available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf) and in the case of *C-582/14 – Patrick Breyer v Germany*, where it was declared that IP addresses are personal data.
15. Article 4(2) of the GDPR.
16. Article 4(7) of the GDPR.
17. Article 4(8) of the GDPR.
18. The European Data Protection Board (formerly the Article 29 Working Party) has issued guidance on this topic in Opinion 1/2010 on the concepts of "controller" and "processor" (available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf).
19. Article 3(1) of the GDPR.
20. Article 3(2) of the GDPR.
21. Article 2(2)(c) of the GDPR.
22. Article 5 of the GDPR.
23. As set out in Article 6 of the GDPR, there are six legal bases that can be relied on when processing personal data: (i) consent; (ii) contractual necessity; (iii) compliance with a legal obligation; (iv) protection of an individual's vital interests; (v) public interest; and (vi) legitimate interests.
24. Organisations should provide information to individuals explaining their data processing activities. Most organisation achieve this by providing a privacy notice.
25. By way of example, an online retailer selling clothes does not require an individual's passport details to process the transaction.
26. Article 5(2) of the GDPR.
27. See the case of *C-582/14 – Patrick Breyer v Germany.*
28. The information on-chain in this scenario would be considered "pseudonymous data" and therefore still personal data subject to the GDPR. The reason being that this pseudonymous data can theoretically be used in combination with the off-chain information to identify a specific individual.
29. See the explanation of "*Distributed*" under the heading "*Blockchain Technology*" which discusses "*nodes*".

30. For instance, these entities may be joint controllers under the GDPR and can agree between themselves how best to manage responsibilities with respect to the individuals whose personal data are processed on the blockchain (per Article 26 of the GDPR). Similarly, a permissioned blockchain allows for a governance framework to be established, within which a number of the key compliance issues can be addressed (e.g., processor terms, joint controller terms, international transfer agreements, the provision of privacy notices etc.).
31. See "Solutions for a responsible use of the blockchain in the context of personal data" (available at https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf).
32. This approach is not without challenge. In some debates, it has been suggested that the developers of a particular blockchain solution should be primarily responsible for the compliance requirements in respect of its use.
33. See Article 26 of the GDPR.
34. See Article 2(2)(c) and Recital 18 of the GDPR, and the European Data Protection Board (formerly the Article 29 Working Party) Opinion 1/2010 on the concepts of "controller" and "processor", p.21 (available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf).
35. See Article 28 of the GDPR, which requires that specific matters be addressed in a contract between the controller and the processor.
36. The CNIL acknowledges the challenges in this regard and is undertaking an in-depth analysis of the issue. See "Solutions for a responsible use of the blockchain in the context of personal data", p.4 (available at https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf).
37. The list of countries within the EEA is set out here: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:European_Economic_Area_(EEA).
38. The GDPR permits such transfers pursuant to Article 45. The list of countries deemed to offer an adequate level of protection can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
39. See Article 46 of the GDPR.
40. The Standard Contractual Clauses are a set of contractual terms that have been pre-approved by the European Commission which impose contractual obligations on both the entity transferring personal data and the entity receiving the personal data. The clauses also confer rights on the individuals whose personal data are being transferred and such individuals can bring an action to enforce these rights against either the transferor or the recipient. More information is available here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
41. Article 5(1)(e) of the GDPR.
42. Guidance issued by the UK Information commissioner specifically discourages indefinite retention of personal data (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/).
43. Article 17 of the GDPR.
44. The right to erasure is not absolute and controllers may be able to refuse a request for erasure based on one of the criteria set forth in Article 17(3) of the GDPR.

45. See "Solutions for a responsible use of the blockchain in the context of personal data", p.8 which addresses this issue (available at https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf).
46. See Articles 5(1)(d) and 16 of the GDPR.
47. See Article 5(2) of the GDPR.
48. Article 25 of the GDPR.
49. See Article 35 of the GDPR.
50. See the "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" issued by the Article 29 Working Party (the predecessor to the European Data Protection Board) (available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711).
51. It should be noted that simply using new technology such as blockchain does not automatically trigger the need to conduct at DPIA. This is confirmed on p.10 of the "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679" (available at http://ec.europa.eu/newsroom/document.cfm?doc_id=47711).
52. Article 25(1) of the GDPR.
53. *Ibid*.

Note

ATTORNEY ADVERTISING. Prior results do not guarantee a similar outcome. This publication is prepared for general information purposes only. It is not, and does not attempt to be, comprehensive in nature. Due to the general nature of its content, it should not be regarded as legal advice.

John Timmons
Tel: +44 20 7532 1598 / Email: john.timmons@whitecase.com

John advises on all aspects of UK and EU privacy, data protection and cybersecurity law. John has extensive experience advising a wide range of clients in the EU, the US and Asia on general data protection compliance and providing specific advice on international data transfer solutions, compliance with local privacy and cybersecurity laws, information governance, e-privacy and direct marketing issues and online behavioural/targeted advertising strategies.

John also has experience advising clients in data protection-related litigation under the GDPR and national implementing legislation, and has advised clients on the data protection implications of deploying blockchain technology. John has a detailed knowledge of European data protection law and associated privacy and cybersecurity legislation. John has written extensively on this subject and has recently co-authored a publication detailing UK cybersecurity law.

Tim Hickman
Tel: +44 20 7532 2517 / Email: tim.hickman@whitecase.com

Tim advises on all aspects of UK and EU privacy and data protection law, from general compliance issues (such as implementing privacy policies and consent forms) to more specialised issues (such as managing data breaches, structuring cross-border data transfers, and complying with the 'right to be forgotten'). Tim has a detailed knowledge of the EU's General Data Protection Regulation (GDPR), and co-authored White & Case's Handbook on that legislation (http://www.whitecase.com/eu-gdpr-handbook).

Clients appreciate Tim's ability to find pragmatic and commercial solutions to complex (and frequently multi-jurisdictional) data protection compliance questions.

Tim has significant experience of working with a wide range of clients in the EU, Asia and the US. He has spent time on secondment at Google, advising on cutting-edge privacy and data protection issues. He has also spoken at several events at Harvard Law School, and he delivered the closing address at the Harvard European Law Conference 2019.

White & Case LLP

5 Old Broad Street, London, EC2N 1DW, United Kingdom
Tel: +44 20 7532 1000 / Fax: +44 20 7532 1001 / URL: www.whitecase.com

Smart contracts in the derivatives space

Jonathan Gilmour & Vanessa Kalijnikoff Battaglia
Travers Smith LLP

There is no universally accepted definition for 'smart contracts', but this term is commonly used to refer to legal contracts (or elements of legal contracts) being represented and executed by software. The term 'smart' refers to the fact that some elements of a smart contract are automatic and self-executing pursuant to pre-defined conditions.

The market is evolving to differentiate a 'smart legal contract' from a smart contract code. Smart legal contracts comprise pieces of smart contract code creating a legally enforceable arrangement. A smart contract code, on the other hand, does not necessarily form part of a smart legal contract, but constitutes a piece of code (or programming language) designed to provide for the execution of certain tasks by a machine.

As discussed in more detail below, smart contract code can, in theory, either form the entirety of an agreement between parties, creating a smart legal contract, or can be used alongside a traditional paper contract to form a hybrid arrangement. This is particularly relevant in the derivatives space as it can allow parties to consider and incorporate a variety of terms into what are often highly complex financial instruments. Currently, smart contracts require specific and objective instructions, so their use is relatively simplistic. However, it is the market's expectation that with time we will see an increase in the use of code-heavy smart legal contracts in the derivatives space.

There has been an increased interest from key industry bodies, such as the International Swaps and Derivatives Association (ISDA), in the development of technology-enabled solutions (including the use of smart contracts) which will allow a fundamental reshaping of the derivatives infrastructure. ISDA's view is that these solutions should improve operating efficiency, reduce operating costs and risk, and increase both quality and transparency of data.[1]

Distributed ledger technology and smart contracts

Distributed ledger technology (DLT) refers to the technology of maintaining distributed ledgers on networks of computers, and blockchain is a form of DLT. Essentially, the DLT provides a digital record available to all participants across a network, meaning there is just one central source of data instead of competing records or copies. Nothing within the DLT can be changed without acceptance from all parties. The DLT can also be 'permissioned', essentially meaning access to the data stored within it can be restricted to certain parties – in the case of smart derivatives contracts, this would likely include people such as market participants and regulators. DLT also allows data to be masked to ensure certain parties can only have sight of certain data relating to specific transactions.[2]

The key benefit of using DLT in the context of smart derivatives contracts is the aspect of 'centralisation' of the data source. Where previously a smart contract was possible, but would, in practice, have to be effected by running separate sets of code alongside each other on the systems of each party to a contract, DLT allows the code to be embedded in the distributed ledger, essentially providing a 'centralised' source of data that binds the parties. The DLT also provides security for the parties, granting them the knowledge that neither party can tamper with the code or prevent the contract from performing an action without the consent of the other party.[3] Having a centralised source of data in relation to a derivatives contract should help parties deal with the complexities of automating derivatives contracts and encourage the adoption of smart contract code in the derivatives space.

The benefits of smart derivatives contracts

Many of the benefits that smart derivatives contracts will bring to the industry are addressed throughout this chapter as we discuss the issues and challenges to be considered when adopting these contracts.

Broadly, smart contracts have the potential to create significant efficiencies in the derivatives space by giving the parties the ability to automate performance of obligations and processes under a contract. The ability to automate actions such as calculations and payments upon the occurrence of certain events will speed up the processes and save resources for market participants as the human analysis element will be removed. Ultimately, this should reduce operational costs and allow more parties to participate in the derivatives market.

From a sell-side perspective, these efficiencies are expected to be translated into a decrease in operational and middle-office costs. There has been an increased interest from financial institutions in using automation in various internal processes involving derivatives and structured products – this includes when providing pre-trade (e.g. quoting processes), execution and post-trade services.

In practice, it is ISDA's view that the development of smart derivatives contracts will be beneficial for most market participants by encouraging standardisation. ISDA has recognised that it is not uncommon for entities, as they have grown and merged over the years, to have increasingly complicated internal systems for the processing of derivatives transactions. The ISDA-led standardisation of processes, terms and industry standards for smart derivatives contracts will save resources within the derivatives space and, in turn, open up the market to more participants.[4]

Recent developments in the derivatives market

There is still a long way to go, but some of the key developments involving ISDA's work to facilitate the use of smart contracts across the derivatives industry include:

(i) In 2017, ISDA issued the first version of the Common Domain Model (CDM), known as ISDA CDM 1.0, followed by its second version ISDA CDM 2.0, which was published earlier this year. The CDM is a standardised solution aimed at providing market participants with a common digital representation throughout the lifecycle of a derivatives transaction. In its first two phases, the CDM provides for the representation of certain events in a machine-readable format with a focus on interest rate and credit derivatives, including an initial representation of equity swaps products and the ISDA Credit Support Annex for initial margin. It is expected that in its next phases the CDM will be developed further to incorporate models for foreign exchange

transactions. ISDA has also been working to update the 2006 ISDA Definitions to make them more compatible with the CDM.[5]

(ii) In January this year, ISDA issued a paper entitled *Legal Guidelines for Smart Derivatives Contracts: Introduction*, which sets out the key principles contained in the ISDA documentation framework and raises awareness of the important legal terms that should be maintained when applying technology solutions to derivatives trading. The guidelines are expected to be supplemented from time to time by further papers to deal with specific ISDA documents, including the ISDA Master Agreement, its relevant collateral arrangements and other product-specific documentation.[6]

(iii) On 9 April, ISDA and Digital Asset (a blockchain start-up) announced the development of a smart-contract based tool for derivatives trading and that they are currently working on an open-source reference code library which will facilitate the implementation of the CDM. The combined use of the smart-contract tool with the CDM is expected to allow a superior level of automation of derivatives management.[7]

ISDA has acknowledged the challenges in implementing the use of smart contracts (and other technology-enabled solutions) in the derivatives space and has established internal committees and member working groups to focus on technology-related topics, including:

(a) The ISDA Legal Technology Working Group, which is focusing on exploring the opportunities for further standardisation of ISDA documentation, in particular by overseeing key aspects of the ISDA Clause Library Project, which is discussed later in this chapter.

(b) The Fintech Legal Group, which focuses on the legal, regulatory and governance issues relating to smart contracts and DLT, an approach that will be vital in addressing some of the issues identified in this chapter.

(c) Various CDM working groups, including the ISDA CDM Design Working Group, whose goal is to develop the CDM while identifying how it may be adopted in order to facilitate shared data management and automation of standardised derivatives lifecycle events. Other CDM subgroups look at specific elements of the CDM design, such as collateral, and different asset classes for which it may be used, such as credit or equity derivatives, and reporting.

These groups are currently open to ISDA's membership, and involvement from market participants will be key to the development of smart derivatives contracts in a way that is appropriate for all participants of the derivatives market.[8]

Regulation of smart derivatives contracts

Smart derivatives contracts are expected to be regulated substantially in the same way as traditional paper derivatives contracts.

The derivatives market was subject to extensive global regulatory reform in the aftermath of the financial crisis. This was reflected in the United States with the adoption of the Dodd-Frank Wall Street Reform and Consumer Protection Act and in the European Union (EU) with the European Market Infrastructure Regulation (EMIR).

Overall, the regulatory framework was reviewed with a view to provide further transparency to the derivatives market and reduce systemic risk. EMIR, for example, is built on the basis of three key pillars: (i) risk mitigation; (ii) reporting; and (iii) central clearing. EMIR provides for a set of obligations that apply to market participants depending on how they are classified under the regulation (i.e. broadly, as financial counterparties or non-financial

counterparties), dependent (in some cases) on the volume of derivatives transactions they have in place, and on the types of derivatives transactions that they enter into.

These regulatory regimes would apply to smart derivatives contacts in the same way as it applies to paper contracts.

On one hand, the use of smart contracts will most likely enable parties to comply with certain aspects of EMIR in a more efficient manner. For example, the automation of certain processes, such as the sharing of data in respect of derivatives transactions, could help to facilitate the parties' compliance with regulatory portfolio reconciliation and reporting obligations.

On the other hand, regulations applicable to derivatives contracts have the potential effect of making it more difficult for the derivatives market to adopt the use of smart contracts. As mentioned in further detail below, this is especially true in the context of the development of the automated ISDA collateral documentation, and ensuring that it provides for regulatory-compliant mechanics (e.g. in line with the provisions relating to regulatory variation margin and initial margin requirements).

Smart derivatives contracts would also be subject to the regulation that is directly applicable to smart contracts more generally. Such regulation is less developed than that in the derivatives space, and there are currently no comprehensive international standards on regulatory policy issues concerning smart contracts.[9] It is likely that, should smart contract work continue to develop and become more widely used, regulation of smart contracts would follow, and smart derivatives contracts would have to abide by this regulation.

Issues and challenges to be considered when adopting smart derivatives contracts

There are a number of issues and challenges that will need to be considered by ISDA in its discussions with market participants to facilitate the transition of the derivatives market towards the use of smart contract code and smart legal contracts.

Scope of automation: operational and non-operational clauses

The main payment and delivery obligations in respect of a derivatives contract are dependent on conditional logic, so these would be well placed for being represented into a smart legal contract. However, not all clauses are susceptible to being automated and self-executed. Certain legal terms are subjective in nature and would produce ambiguity if represented in smart contract code.

The materials produced by ISDA relating to the use of smart contracts in the derivatives space suggest that, when determining which parts of a derivatives contract are susceptible to automation, it is helpful to distinguish between operational and non-operational clauses.[10] Operational clauses would generally contain conditional logic that states that, on the occurrence of a specific event or within a given timeframe, a pre-determined action will be taken, so they would be more amenable to automation. Examples of operational clauses include a payment obligation that arises on a particular date and a collateral transfer requirement that arises where certain pre-determined thresholds are met.

Non-operational clauses, on the other hand, do not necessarily contain such conditional logic, and would more likely relate to the wider contractual relationship between the parties, proving to be more resistant to automation. For example, a governing law clause or a representation that a party is validly existing under the laws of its jurisdiction of incorporation. That is not to say, however, that non-operational clauses cannot be automated. Using the example of valid incorporation, a sufficiently developed smart contract code would

be able to check such information on the relevant company registry to ensure the information is correct. Nevertheless, questions still arise as to how the code will be developed and how common standards will be implemented across smart legal contracts and across different jurisdictions and legal systems.

A potential solution to these issues with automation would be for parties to adopt a hybrid form of smart derivatives contract, in which some of the provisions would be automated and others would be set out in traditional paper form. It is intended that the ISDA Clause Library Project will play an important role in enabling parties to use hybrid smart derivatives contracts. The objective of this project, initiated by the ISDA Legal Technology Working Group, is to build an industry-wide clause library for the Schedule to the ISDA Master Agreement in order to standardise ISDA documentation further as parties continue to explore legal technology. ISDA believes the project will encourage development and adoption of technology by providing greater clarity on how smart code can be implemented in practice. Similarly, ISDA's CDM aims to increase automation and efficiency within derivatives markets by providing a blueprint for how derivatives are traded and managed during the lifecycle of a transaction in order to standardise the market as a basis for automation.[11]

It is expected that the development of these projects will play an important role in simplifying the process of creating a hybrid smart contract, and counter the issues concerning the scope of automation. The development of standardised forms (or smart code) for key provisions selected for automation (in this initial stage, with a focus on operational clauses) will encourage and simplify the adoption of smart legal contracts in the derivatives market.

As the industry is still in its early stages of adopting smart contract solutions, when selecting provisions for automation, ISDA's work should, for the time being, focus on provisions that can be used across different types of derivatives products. The ISDA CDM aims to avoid making functions product-specific, so commonality of functions performed by the automated provisions is important. Having commonality in key pieces of smart contract code will also help with legal validation, which is discussed further in this chapter. If a smart legal contract is entirely in smart contract code, knowing that the code has been 'translated' into human language by a significant proportion of the derivatives industry (as this code will be common across the industry) gives parties comfort that it has been properly scrutinised and validated. Nevertheless, this in itself will create the further challenges of ensuring the contract as a whole works, and that the codified contractual elements integrate fully with the paper documentation.

Issues with legal validation

For a smart legal contract to produce its intended legal effect, its automated provisions (or smart contract codes) must be legally validated by a lawyer. This might be challenging as it would require lawyers to understand the programming language. It follows that there is the need for programmers to work in collaboration with lawyers to leverage their legal insight into which parts of the ISDA documentation framework would be legally effective if converted into an automatable form. ISDA is expected to play an important role in facilitating this work.

If lawyers are to be able to validate the legal effect of a smart derivatives contract, lawyers themselves will need to learn the relevant programming language – perhaps from a starting point of having little or no prior knowledge or understanding of programming. Alternatively, if lawyers are to work closely with computer programmers to draft the smart legal contracts, the lawyer's legal drafting will need to be in a form and language that a non-lawyer is able to understand and translate into smart contract code. This would need to take the form of

clear, natural language that is logical and unambiguous, while properly reflecting the legal meaning. Ultimately, both the lawyer and the programmer may have to invest significant resources into learning and using new language if it is intended that smart legal contracts will be legally validated.

It will be challenging for non-operational clauses that include some degree of subjective interpretation (e.g. where a party is required to act in good faith or commercially reasonable manner) or those that are more complex in nature (e.g. when an event of default is linked to the occurrence of a specific event outside the contractual relationship and that is not easily asserted) to be legally validated.

Furthermore, the requirement for programmers and lawyers working in collaboration to create such contracts raises questions concerning liability. The certainty provided by a smart contract can be framed as an advantage – there may be no room for ambiguity and the code can easily be replicated and re-used. However, leaving such little room for nuance could lead to unforeseen and unwanted outcomes. The fact that high-speed code does not necessarily allow for subjective interpretation and human judgment could result in a specific clause being triggered by certain events – such as in an event of default, as explored further below – where a different course of action may have been preferable. A key question arising from this issue is: who takes on the risk of such concerns, and where does the liability fall? This is a question that will need to be considered with caution as the use of smart contracts in the derivatives space increases and develops.

Issues with automation

Not all provisions, when automated, would produce the same effect as if complied with in their original form (i.e. in natural language) without automation.

By way of example, upon the occurrence of an event of default under a derivatives contract, the non-defaulting party would have the right to terminate the outstanding transactions. Under normal circumstances, under a non-automated contract, there are a range of factors that the non-defaulting party would take into account before pulling the trigger – these tend to be subjective and include commercial considerations, the relationship context at the time of the event and the nature of the default. It would be difficult to cater for these factors when translating event of default provisions into programming language. In practice, the occurrence of an event of default under a smart derivatives contract would be self-automated, so it would automatically trigger the termination of any outstanding transactions.

It is unlikely that all counterparties would have the same attitude and response to the occurrence of events of default due to their subjective nature. Therefore, a potential solution is for smart contract code to inform the parties upon the occurrence of an event of default in order to allow the parties to give further consideration to the event (and the then prevailing facts and circumstances) and provide further authorisation as to the consequences that will arise from the occurrence of that event, ideally from a selection of pre-programmed actions to allow for greater efficiency.[12] As the code is developed and the contracts are used, it may be possible for parties to include responses to certain events that are different for each party, or for the code to monitor the level of risk by the frequency of the occurrence of events and use that monitoring to inform its response.[13] However, as the code would be agreed by all parties entering into the contract, this again raises further issues – parties are unlikely to be willing to spell out their intended responses to each event of default, thus opening themselves up to exploitation under the contract.

ISDA has proposed to work with its members to select provisions within the ISDA documentation framework that are best suited for automation – their goal is to select

provisions that can be automated without changing their legal effect, as well as ensuring the work required to standardise the automated format of the selected provisions is cost and time effective.[14]

Drafting precision and automation

The difficulties outlined above regarding automation and flexibility arise because the code, compared to a human user, struggles to understand the subjective considerations – for example, the use of the term 'reasonable'. Without clearly defined parameters within which to work, converting natural language into a codified contract creates the risk that the code would divert from the true legal meaning of the contract.

As ISDA has identified, the human user of a paper contract has the flexibility to fully understand legal drafting, as evidenced by the approach to legal drafting in a court room. Whereas a court will try to give some meaning to ambiguous words to understand what the parties have agreed, a machine is unlikely to be able to take a similar (flexible) approach when 'interpreting' the programming language.[15] However, it is thought that, as the use of smart contract code develops, it could be possible to create software that adds a level of non-determinism to code and that could work out the meaning of non-recognised code by exploring other versions and examples of similar programming.[16] This development could be invaluable in the derivatives space.

Nevertheless, it appears evident that smart derivatives contracts capable of complex subjective interpretation of legal issues are some years away. For most lawyers, deliberate ambiguity can be a vital drafting and negotiating tool. Contracts often contain a mixture of carefully specified language and language which is expressed with a degree of ambiguity – for example, if parties are unable to agree terms, or if a draftsperson wants to improve an unfavourable position for their client. Also, even when the code is capable of applying discretion, for complex derivatives transactions parties may be concerned about the idea of allowing computer code to effectively make commercial decisions following certain events.

There appears still to be some way to go before smart contracts are created with the necessary flexibility and subjectivity for derivatives contracts.

Issues concerning the use of smart contracts in ISDA's collateral documentation

There are a number of legal issues that need to be considered when applying legal technology solutions to the ISDA collateral documentation.

The ISDA collateral documentation includes the credit support documents prepared by ISDA (such as a credit support annex or a credit support deed) providing for the exchange of assets between parties as collateral in respect of underlying derivatives transactions (including for the purposes of compliance with the applicable regulation, e.g. the variation margin and initial margin requirements under EMIR). Broadly, in a derivatives context, collateral is used to support a party's obligations – such as to make payments in certain circumstances – by identifying assets to which the other party can have recourse if the party providing the collateral fails to meet their obligations.

ISDA has identified collateral processes as an area in which opportunities might exist for automation. There is often seen to be a lack of efficiency in many existing collateral processes – for example, differences in reference data (such as for valuation purposes) which may give rise to calculation disputes. Many of these processes use conditional logic which, as discussed elsewhere in this chapter, can be particularly conducive to the use of smart contracts. The benefit of automating these processes is evident as regulation has increased complexity in the area, as automation would add operational efficiency that would save

valuable resources. Nevertheless, legal and regulatory concerns arise when considering the automation of collateral documentation.

When considering the use of smart code in the ISDA collateral documentation, it is important to consider the specifics of the assets to be provided as collateral. Smart contract developers' design choices when it comes to the creation of the smart derivatives contracts, and the use of DLT, will have an effect on the nature of, and the rights to, the collateral, in particular regarding access and restrictions on use. Further, developers must consider the legal *situs* (location) of the assets, and this is an issue explored in more detail later in this chapter.

A party's ability to choose the assets to be posted as collateral might also be affected when its transfer is automated. Under a paper contract, parties may have a choice as to the type of collateral it wishes to post on receipt of a collateral call – for example, where the party is entitled to post either cash or securities, it will consider, from a commercial perspective (including based on liquidity and operational concerns), which type of collateral it wishes to transfer across to its counterparty. This ability to choose may face opposition from a fully automated process. It may therefore be necessary to embed further coding into the mechanics of the smart contract to provide the parties with the ability to elect for specific types of collateral to be transferred upon the occurrence of pre-determined market events (or other commercially agreed triggers).

Also, under applicable derivatives regulation, certain types of collateral are subject to requirements relating to liquidity, credit quality, concentration and wrong-way risks. Smart derivatives contracts will need to be capable of translating these requirements into smart code. ISDA sees this as falling within the realms of smart contract capability, but it will take some time until the code has been developed sufficiently to deal with these complexities.

Finally, the handling of disputes within the context of automated ISDA collateral documentation will have to be considered carefully. Disagreements over collateral valuations will need to be resolved quickly between the parties, especially with regulatory-compliant collateral arrangements, and it will be vital to ensure the smart derivatives contract is designed to allow for suspension of transfer obligations pending resolution of the dispute and, where applicable, the transfer of any undisputed amounts.

While the automation of the ISDA collateral documentation is certainly possible, this in particular will be an area in which lawyers and smart contract developers must work closely together to ensure the resulting smart contract code reflects the many complexities set out in the ISDA collateral documentation and applicable regulation.

Complex and bespoke derivatives contracts

Certain derivatives contracts can be heavily negotiated and customised to apply to bespoke arrangements made between the parties. The level of customisation might vary depending on counterparty type and product complexity. Examples of highly customised arrangements include total return swaps, longevity swaps and other structured finance products that will likely be made under a suite of documents forming the overall derivatives architecture, where various levels of obligations apply across different parts of the documentation. In light of the challenges addressed above, it would be difficult to translate these interlinking obligations into programming language in a straightforward manner. Beyond whether it is possible, it is also not necessarily practical or desirable to pursue the automation of highly complex elements of derivatives contracts. It is extremely difficult, if not impossible, when entering into such an arrangement, to predict all the possible scenarios that may arise from a particular contract and a particular legal relationship between the parties. Indeed, the time and cost involved in attempting to do so may not be worthwhile. Therefore, apart from the issues

raised above that need to be considered before embarking on the development and use of smart derivatives contracts, parties may wish to think carefully about whether it is beneficial to even to try to develop code that is sufficiently intricate to reflect highly complex provisions of certain types of derivatives contract.

The recent regulatory developments in the derivatives space (which follow a global trend post the global financial crisis) have also contributed to the complexity of certain derivatives contracts. For example, there has been an increase in the use of third-party custodians when implementing collateral arrangements to deal with certain margin requirements, and there are additional layers of complexity arising from the need for certain over-the-counter derivatives transactions to be centrally cleared. This only goes to complicate the matter further – as the derivatives market becomes more heavily regulated more generally, and as regulation of smart contracts is further developed, smart derivatives contract code could become ever more complex to develop.

Laws affecting contractual performance

Certain laws might have the effect of interrupting the performance of contracts – for instance, where a provision under a specific contract is rendered void, or where a contractual stay is applied to a party in financial distress under the applicable regulatory regime. Terms can also be implied into a contract, or amended by the courts if found to not reflect the true agreement between the parties. How would smart legal contracts interact with these laws?

The way forward may include the requirement for smart contract code to need human input, to ensure the contract is managed and is kept up-to-date to reflect changes in law. It is impractical and inefficient to include all possible circumstances and imagine responses within the code, and it is legally risky to ignore the consequences of having smart contracts that could potentially be operating outside the law. Therefore, the contract must allow for human intervention to pause its automatic performance – this would not pause the obligations under the contract, but only its automatic operation.

As part of its work in the smart contracts space, ISDA has noted that the right of suspension would be useful in many scenarios.[17] For example, as mentioned above, it would interact well with the idea that smart derivatives contracts could require further authorisation on the occurrence of an event of default. In practice, this would mean that, where appropriate, parties would have the flexibility to suspend the automatic operation of the smart contract and rely on natural language provisions.

Situs

It is often necessary to be able to identify the location of an asset or the location of performance of a contract to be able to ascertain the relevant legal jurisdiction – for example, in the case of disputes, what is to be the governing law. For dematerialised financial assets, ownership is often recorded on a register, and the *situs* is the place in which that register is held or the registrar is situated. Issues might arise when it comes to information relating to smart derivatives contracts (including in respect of assets provided as collateral) on a DLT as the information might be distributed across multiple jurisdictions – and as there is no registered location for the data, *situs* might be indeterminable. It might be that this issue will be resolved over time as the market develops and regulation is enhanced, but for now it is important for industry bodies and market participants to consider this in further detail.[18]

Liquidity concerns

Once the market has moved to address most of the key concerns that are set out in this chapter, it is likely that only the largest and most sophisticated market participants will be

able to start using smart legal contracts. The smaller or less sophisticated players, including many buy-side entities, might find it more challenging and costly to adapt their processes to the new 'reshaped' derivatives market.

What should market participants be doing?

The market is still evolving and is in its early stages of developing a model that works across the derivatives industry. ISDA is playing an important role in the implementation of technology-enabled solutions (with a special focus on smart contracts and DLT). This will have a positive effect on the market, by improving operating efficiency and reducing operating costs and risk.

For the time being, market participants are encouraged to:

- get involved with the initiatives put forward by ISDA, including the working group discussions; and
- have an ongoing dialogue, and compare notes, with their peers, counterparties, legal advisers and other industry bodies on the changes that will need to be implemented into their systems and processes to allow for the use of smart contracts.

It is important for representatives from all different parts of the derivatives market, including buy-side, sell-side, market makers, industry bodies, regulators and advisers, to join efforts in order for considerable progress to be made across the industry and enable the use of smart derivatives contracts and, most importantly, to address the challenges identified in this chapter.

* * *

Endnotes

1. ISDA, *The Future of Derivatives Processing and Market Infrastructure* (2016), available at https://www.isda.org/a/UEKDE/infrastructure-white-paper.pdf, pp. 13-14.
2. ISDA, *Smart Contracts and Distributed Ledger – a legal perspective* (2017), available at https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf, pp. 7-9.
3. *Ibid.*
4. ISDA, *The Future of Derivatives*, p. 13.
5. Further information regarding the ISDA CDM is available at https://www.isda.org/2019/03/20/isda-publishes-cdm-2-0-for-deployment-and-opens-access-to-entire-market/.
6. The guidelines are available at https://www.isda.org/a/MhgME/Legal-Guidelines-for-Smart-Derivatives-Contracts-Introduction.pdf.
7. The press release is available at https://www.isda.org/a/HTSME/Digital-Asset-ISDA-CDM-Adoption-Press-Release.pdf.
8. ISDA has a 'Committee Dashboard' for all members in which members can join committees and working groups, view past and upcoming meetings, and access relevant documentation published for these meetings. The dashboard is accessible at https://www.isda.org/committees.
9. ISDA, *Smart Derivatives Contracts: from concept to construction* (2018), available at https://www.isda.org/2018/10/03/smart-derivatives-contracts-from-concept-to-construction/, p. 6.

10. ISDA, *Smart Contracts and Distributed Ledger*, p. 10.
11. For more information, ISDA have released a Memorandum available to ISDA's membership at https://www.isda.org/a/DZdEE/ISDA-Clause-Library-Project-Memo.pdf.
12. C. Clack and C. McGonagle, *Smart Derivatives Contracts: the ISDA Master Agreement and the automation of payments and deliveries* (2019), p. 23.
13. *Ibid*.
14. ISDA, *Smart Derivatives Contracts*, p. 15.
15. *Ibid.*, p. 21.
16. Clack and McGonagle, *Smart Derivatives Contracts*, p. 24.
17. ISDA, *Smart Derivatives Contracts*, pp. 17-18.
18. ISDA, *Smart Contracts and Distributed Ledger*, p. 9.

Jonathan Gilmour
Tel: +44 20 7295 3425 / Email: Jonathan.Gilmour@traverssmith.com

Jonathan is a partner at Travers Smith and heads its Derivatives & Structured Products Group. He specialises in derivatives and structured products from both a transactional and advisory standpoint and is widely regarded by peers and clients as one of the leading specialists in his field and as a champion of 'buy-side' interests in the UK derivatives market. He counts among his clients some of the UK's largest and most sophisticated occupational pension schemes, investment managers, private equity houses and challenger banks.
Jonathan is a regular speaker on derivatives and spoke at ICLG's Cross-border Fintech: Regulation and the Law 2019. He is a member of a number of ISDA and FIA working groups and sits on the FMLC's High Level Advisory Group on Brexit and its FinTech and Asset Management Scoping Forums. He regularly co-authors articles including for the *Butterworths Journal of International Banking and Financial Law* and the *International Financial Law Review*.

Vanessa Kalijnikoff Battaglia
Tel: +44 20 7295 3150 / Email: Vanessa.Battaglia@traverssmith.com

Vanessa is a senior associate at Travers Smith where she is a member of the Derivatives & Structured Products Group with a developed transactional and advisory practice. She is qualified in New York and Brazil. Vanessa's practice focuses on derivatives, repo, stock lending, custody and collateral arrangements. Vanessa guides clients through regulatory developments such as EMIR and SFTR and their impact on derivatives arrangements. Her clients include asset managers, investment funds, fintech companies, pension schemes, banks and corporates.
Vanessa is a member of key working groups of leading industry bodies including ISDA's Legal Technology Working Group, AIMA's OTC Derivatives Working Group and Invest Europe's Working Group on Derivatives. Vanessa is described in the 2018 edition of *The Legal 500 UK* as "very knowledgeable and responsive". Vanessa has also co-authored articles on the subject of derivatives and associated regulation for the *Butterworths Journal of International Banking and Financial Law*, *International Financial Law Review* and *Funds Europe*.

Travers Smith LLP

10 Snow Hill, London, EC1A 2AL, United Kingdom
Tel: +44 20 7295 3000 / Fax: +44 20 7295 3500 / URL: www.traverssmith.com

Distributed ledger technology as a tool for streamlining transactions

Douglas Landy, James Kong & Jonathan Edwards
Milbank LLP

This chapter will provide a high-level overview of the potential applicability of distributed ledger technology ("DLT") to the transfer of assets represented by "tokens" or other digital assets[1] (which, for the purposes of this chapter, we will call "Transfer Tokens"), and the regulatory environment developing around such tokens. Using a token as a means of representing an underlying asset (colloquially referred to as the "tokenization" of that asset) in order to facilitate transfers of that asset is a relatively new idea, but has its roots in a very old and well understood principle: some things that have value are not easily transferred. Whether because of practical difficulties, regulatory hurdles or imperfect or outdated trading infrastructures, sometimes the easiest way to transfer an asset – whether it be title, an ownership interest, an entitlement, or a beneficial interest in that asset – is by transferring something that represents the asset.[2]

Tokenization has potentially wide applicability to traditional markets. The trading of securities in the United States, for example, is beset with inefficiencies related to existing trading infrastructures. For example, repurchase transactions ("repos," whereby one party agrees to sell securities to another party and then buy them back at a later time) traditionally involve transfers of ownership that are recorded on the books of a clearing bank or the Fedwire Securities Service. Recording these transfers take time and relies on a central intermediary, placing operational bounds on a traditional repo's minimum duration. Using Tokens to represent the underlying securities can potentially streamline this process, as parties could instead transfer (and have such transfer be reflected in a distributed ledger) Transfer Tokens that represent an interest in the securities, rather than the securities themselves.

Of course, tokenization in this manner faces a number of regulatory hurdles – some inherent to the concept itself, and some particular to each specific implementation. For example, as a general matter, it is of particular import that parties not run afoul of the broad reach of the U.S. securities laws:[3] if the purpose of a Transfer Token is to facilitate trading of underlying assets, it is important to establish whether the creation and use of such a token actually creates any of its own barriers – namely, whether the Transfer Tokens could potentially be characterized as "securities," and whether the entity creating such Transfer Tokens could be considered an "issuer" subject to the securities laws. If Transfer Tokens *were* to be treated as securities, the very purpose of their creation and existence (*i.e.*, to facilitate otherwise cumbersome transactions) is challenged. A further challenge is the essential dependence of many securities law analyses on the particular facts and circumstances of each case, precluding a "one-size-fits-all" approach to compliance. Additionally, applying a layer of tokenization to traditional transactions, such as repos, for which the applicable legal regimes are well-established regarding legal certainty, security interest, and enforceability in

bankruptcy, raises the question of whether tokenized transactions that resemble traditional transactions in all substantive respects should necessarily benefit from the same legal treatment as traditional transactions.

Section I of this chapter will provide a basic overview of DLT and how it can be used to create Transfer Tokens that represent underlying assets. Second, we will describe a "generic" implementation of a Transfer Token, and discuss how we believe such a token should be characterized for the purposes of U.S. securities laws. Third, we will provide a number of examples of the potential uses of Transfer Tokens, along with an overview of certain legal issues germane to each implementation.

Background

While a full overview of DLT is outside the scope of this chapter, DLT (commonly implemented in the form of "blockchain" technology) generally refers to a "decentralized peer-to-peer network that maintains a ledger of transactions that utilizes cryptographic tools to maintain the integrity of transactions and some method of protocol-wide consensus to maintain the integrity of the ledger itself."[4] While early implementations of DLT, such as Bitcoin, were limited in scope and intended primarily to facilitate peer-to-peer transfers of value, other implementations of DLT incorporate the ability for parties to "structure and update data on a ledger through robust computer code, known as smart contracts."[5] This allows "any asset or thing [to] be modeled on a ledger," and "parties to run computer functions to interact with the data structures on the ledger."[6]

One potential application of DLT in this context is the ability to "tokenize" a broad range of traditional assets, which, at least theoretically, can encompass nearly anything. In this way, transfers of the asset "can be tracked automatically on a blockchain platform in the same manner as a cryptocurrency such as Bitcoin is tracked using the same technology."[7] By tokenizing an asset and allowing it to be digitally represented on a blockchain or other form of distributed ledger, the process of recording and transferring ownership of the asset can be significantly streamlined. The question of whether such digital assets are "securities" is therefore critical, as the application of the securities laws to the issuance and transfer of digital assets such as the Transfer Tokens would impose onerous, and potentially irrational, requirements on the "issuers" of the Transfer Tokens and hamper the ability of secondary market participants to trade Transfer Tokens amongst each other.

Characterization of tokens under securities laws

Background of treatment of digital assets

Beginning in 2017, the SEC has, through various avenues, articulated its general stance toward the regulatory classification and treatment of digital assets. In April 2019, the SEC issued its *Framework for "Investment Contract" Analysis of Digital Assets* (the "SEC Framework"). As described in the SEC Framework, any person "engaging in the offer, sale, or distribution of a digital asset" must "consider whether the U.S. federal securities laws apply," and a threshold issue is "whether the digital asset is a 'security' under those laws."[8] While the framework is new, its essential underpinning is not: central to the SEC's analysis has been, and continues to be, the well-worn three-prong test articulated by the Supreme Court in SEC v. W.J. Howey Co., 328 U.S. 293 (1946) ("Howey"). The Howey test "applies to any contract, scheme, or transaction, regardless of whether it has any of the characteristics of typical securities," and is meant to determine whether a particular asset or arrangement is an "investment contract" (and therefore a security). Under the test established in Howey,

an "investment contract" exists if there is (i) an investment of money, (ii) in a common enterprise, (iii) with a reasonable expectation of profits derived predominantly from the efforts of others.

In analyzing whether something is a security, "form should be disregarded for substance."[9] The SEC has primarily applied the Howey test to digital assets because such assets do not otherwise fall into any of the enumerated categories of the definition of "security." Accordingly, the Howey test focuses not only on the form and terms of the asset or arrangement itself, "but also on the circumstances surrounding the digital asset and the manner in which it is offered, sold, or resold (which includes secondary market sales)."[10] As a result, the question of whether a hypothetical Transfer Token is a "security" is one that resists blanket classification, and that instead depends on both the form and function of the Transfer Token as well as the particular facts and circumstances surrounding the issuance, offering, and secondary market transfers of the Transfer Token.

While "[no] one factor is necessarily dispositive as to whether or not an investment contract exists,"[11] the SEC Framework articulates a wide range of factors that would be indicative of the presence of an "investment contract," mapping these factors to each prong of the Howey test. These factors include, among others:

- An investment of money:

  Investors purchase or otherwise acquire the digital asset in exchange for value, whether that value takes the form of fiat currency, another digital asset, or another type of consideration.

- A common enterprise:

  While the SEC Framework notes that the SEC does not view the "common enterprise" requirement as a distinct element of the Howey test, the SEC noted that investments in digital assets have generally constituted investments in a common enterprise "because the fortunes of digital asset purchasers have been linked to each other or to the success of the promoter's efforts."[12]

- Reasonable expectation of profits derived from efforts of others:

  An investor has a reasonable expectation of profits derived from the efforts of others if a promoter, sponsor, or other third party (each, an "Active Participant" or "AP") provides essential managerial efforts that affect the success of the enterprise, and investors reasonably expect to derive profit from those efforts. While no one factor is determinative, the SEC Framework lists the following factors as indicative of whether this prong is met:

  - the purchaser reasonably expects to rely on the efforts of an AP;
  - the managerial efforts are significant and affect the failure or success of the enterprise, as opposed to efforts that are ministerial in nature;
  - an AP is responsible for the development, improvement, operation, or promotion of the network;
  - where the network or digital asset is still in development or not yet fully functional, investors would reasonably expect an AP to further develop the functionality of the network and/or digital asset;
  - there are essential tasks or responsibilities performed and expected to be performed by an AP;
  - an AP creates or supports a market for, or the price of, the digital asset;

- an AP has a lead or central role in the direction of the ongoing development or management of the network or the digital asset;
- investors would reasonably expect the AP to undertake efforts to promote its own interests and enhance the value of the network or digital asset, such as where the AP has the ability to realize capital appreciation from the value of the digital asset, the AP distributes the digital asset as compensation to management, or the AP monetizes the value of the digital asset;
- the digital asset gives the holder rights to share in the enterprise's income or profits or to realize gain from capital appreciation of the digital asset;
- the digital asset is transferable or traded on a secondary market or platform;
- purchasers reasonably would expect the AP's efforts to result in capital appreciation of the digital asset;
- the digital asset is offered broadly to potential purchasers or in quantities indicative of investment intent;
- the AP is able to benefit from its efforts as a result of holding the same class of digital assets as those being distributed to the public;
- the potential profitability of the operations of the network or the potential appreciation in the value of the digital asset is emphasized in marketing or other promotional materials; and
- the availability of a market for the trading of the digital asset.

In contrast, the SEC Framework highlights a number of factors that, while not necessarily determinative, would support the notion that the Howey test is not met,[13] including:

- the distributed ledger network and digital asset are fully developed and operational;
- holders of the digital asset are immediately able to use it for its intended functionality on the network;
- the digital assets' creation and structure is designed and implemented to meet the needs of its users, rather than to feed speculation as to its value or development of its network;
- prospects for appreciation in the value of the digital asset are limited;
- any economic benefit that may be derived from appreciation in the value of the digital asset is incidental to obtaining the right to use it for its intended functionality;
- the digital asset is marketed in a manner that emphasizes its functionality rather than the potential for the increase in market value of the digital asset;
- potential purchasers have the ability to use the network and the digital asset for its intended functionality;
- restrictions on the transferability of the digital asset are consistent with the asset's use and not facilitating a speculative market; and
- if the AP facilitates the creation of a secondary market, transfers of the digital asset may only be made by and among users of the platform.

Application of the securities laws and the SEC framework to transfer tokens

As noted above, the question of whether the Transfer Token is a "security" depends on both the form and function of the Transfer Token as well as the particular facts and circumstances surrounding the issuance, offering, and secondary market transfers of the Transfer Token. In general, of course, the aim is to design a Transfer Token such that (i) the hallmarks of a

"security" described in the SEC Framework are generally not present, in either form or substance, and (ii) the factors that would indicate that a digital asset is *not* a security *are* present. For the purposes of this chapter, therefore, we imagine a generic Transfer Token with a number of essential characteristics that we believe should, when analyzed through the prism of the factors articulated by the SEC above, cause that Transfer Token to fall outside the definition of security. These characteristics include:

- The Transfer Tokens are issued to represent a specific underlying asset, and are designed for the express purpose of facilitating a transfer of that asset.

  Discussion: In general, the more narrowly tailored the design of the Transfer Token, the less likely it would be to fall under the auspices of the securities laws. For example, in a hypothetical implementation, a holder of a Transfer Token (a "Token Holder") may deposit assets, such as cash or securities, with a custodian, and receive Transfer Tokens representing those cash or securities in return.[14] The Transfer Tokens could then be used to facilitate transfers of the underlying cash or securities to other market participants who maintain accounts at that custodian. Recipients of Transfer Tokens (or the original acquirer of the Transfer Tokens, in the case of an acquirer who retains the tokens or repurchases them under a repo) could, in turn, "redeem" the Transfer Tokens with the custodian in order to receive the underlying cash or securities. Under this model, the Transfer Tokens' creation and use – tied solely to facilitating a transfer of the underlying assets – would more likely be considered to have been designed and structured to meet the needs of users, rather than to feed speculation.

  Note that given the SEC's broad interpretation of an "investment" of money under the Howey test, such an acquirer of Transfer Tokens may nevertheless be considered to be making an "investment" of value. However, the acquirer is not obtaining the Transfer Tokens for investment *purposes*; rather, the acquirer is *exchanging* some form of property for a Transfer Token that represents that property, and subsequently using the resulting Transfer Token to effect a transfer of that property to another party (who will redeem, and therefore destroy, the Transfer Token). Crucially, the Transfer Token itself is not purchased because of its value; rather, the Transfer Token should be envisioned as having no value in and of itself, and more akin to a book-entry representing some underlying asset rather than an asset itself.[15]

- Because Transfer Tokens are created to represent specific underlying assets and have no value distinct from those assets, there is no "common enterprise" linking the fortunes of the entity issuing Transfer Tokens to Token Holders, or the fortunes of Token Holders to each other.

  Discussion: While the SEC "does [not] view a 'common enterprise' as a distinct element of the term 'investment contract,'" the SEC Framework notes that "investments in digital assets have constituted investments in a common enterprise because the fortunes of digital asset purchasers have been linked to each other or to the success of the promoter's efforts." In particular, the SEC Framework notes that investors in a digital asset that is a security would reasonably expect capital appreciation in the value of the digital asset based on the efforts of an AP. This is not the case with respect to the Transfer Tokens; Token Holders' fortunes are neither linked to the fortune of the "issuer" of the token nor to the fortunes of other Token Holders. Rather, Token Holders' fortunes are tied only to the value of the underlying asset represented by the Transfer Token, which value should not be affected by the tokenization of the asset.

- Additionally, because Transfer Tokens are tied to specific underlying assets and designed to facilitate a transfer of those assets, market participants would not acquire the *tokens themselves* with a reasonable expectation of profits predominantly from the efforts of others.

  Discussion: In contrast to scenarios described in the SEC Framework, there is no AP in the transactions imagined in this chapter that would retain the digital asset, or that would support the price of the digital asset, undertake efforts to enhance the value of the digital asset, or have the ability to realize capital appreciation from the value of the digital asset. The Transfer Tokens are created merely to streamline the process by which market participants may transact in certain types of assets and transfer interests among each other. Participants acquire Transfer Tokens not to profit from the efforts of others, but to more easily effectuate the envisaged transaction(s) in the underlying asset.

- The Transfer Tokens imagined would be issued on a functioning network, be designed to replicate and streamline the process normally associated with transacting in the asset represented, and be distributed only among people or institutions that comprise the existing market for the underlying asset.

  Discussion: As noted above, the Howey test is less likely to be met if a digital asset's creation and structure is designed and implemented to meet the needs of its users and the restrictions on the transferability of the digital asset are consistent with the asset's use. This would generally mean, for example, that to the extent that purchasers of an underlying asset would be limited to individuals or institutions that meet certain criteria, the issuance and transfer of Transfer Tokens should also be so limited.

- Because the Transfer Tokens are meant to replicate "traditional" interests in the underlying assets represented by the Transfer Tokens, one of the primary policy purposes of the securities laws articulated by the SEC – *i.e.*, compelling disclosure in order to reduce informational asymmetries between promoters and investors – would be inapplicable to the use of Transfer Tokens imagined by this chapter, because no informational asymmetry is produced by the tokenization of an asset. No part of the "traditional" transaction in the asset is in substance altered by tokenization, and as noted above, the creation of Transfer Tokens can be more properly envisioned as the creation of an electronic book-entry representing an underlying asset, rather than the creation of a new asset itself.

Potential applications of transfer tokens

Within the model articulated in the foregoing section, Transfer Tokens may be used to streamline transactions in a potentially wide range of assets, although different legal considerations may apply to each. This section reviews the potential applicability of Transfer Tokens to three distinct markets: the repo market; the syndicated loan market; and the market for artwork, and briefly discusses certain relevant considerations with respect to each.

Repos

As indicated in the introduction, one possible application of Transfer Tokens is to the repo market. Typically, repos have been conducted on, at a minimum, an overnight basis, due in part to operational constraints regarding how quickly ownership changes may be reflected on the books and records of a clearing bank or the Fedwire Securities Services. By permitting securities held by a central custodian to be represented by Transfer Tokens,

however, a DLT-based platform could potentially allow market participants to settle repurchase transactions on an intraday basis, in a timeframe that would not otherwise be operationally feasible. Although the application of DLT and Transfer Tokens to these markets is novel, the economic substance of the underlying transactions would be unchanged from that of traditional repurchase transactions conducted on the underlying securities: *i.e.*, a "tokenized" repo would involve a purchase and sale of the underlying securities, except conducted with Transfer Tokens and reflected on a distributed ledger, rather than with the securities themselves and reflected on a set of centrally maintained books.

Under a hypothetical DLT-based implementation, for example, a market participant could obtain Transfer Tokens by transferring securities to an account maintained by a custodian (or alternatively, sending a digital instruction that would effectively "lock" a basket of identified securities already held in that custodial account) and in return receive Transfer Tokens representing the underlying securities. That market participant could then enter into repos on the underlying securities with eligible counterparties, *as represented by* the Transfer Tokens issued with respect to such securities. The holder of the Transfer Tokens would then have the unconditional right to "redeem" the tokens in exchange for receiving the underlying assets from the custodian at any time, thereby allowing a non-defaulting buyer to exercise remedies in the event of the default of the seller. At the conclusion of a successful transaction, the original participant could redeem the Transfer Tokens and receive the underlying assets, or potentially enter into further repo transactions. Any issuance, redemption, or transfer of Transfer Tokens could be reflected and verified in real time on a distributed ledger.

One threshold question with respect to the applicability of DLT to the repo markets is whether this additional layer of tokenization would affect the essential legal characterization of repos – namely, whether the documents governing such tokenized repo transactions would nevertheless be considered "securities contracts" within the meaning of title 11 of the United States Code (the "Bankruptcy Code").[16] Without going into detail, provided the underlying documentation qualifies as a securities contract, a debtor's bankruptcy avoidance rights and the automatic stay of section 362 of the Bankruptcy Code should not apply to the applicable transactions.

Certainty in this area is critical, as market participants may understandably be hesitant to engage in a tokenized repo transaction without assurance that the legal protections afforded to them under traditional repos are present. As defined in section 741(7) of the Bankruptcy Code, a "securities contract" includes, in relevant part:

> (i) a contract for the purchase, sale, or loan of a security, ... or interests therein (including an interest therein or based on the value thereof), or option on any of the foregoing, including an option to purchase or sell any such security, ... or option, and including any repurchase or reverse repurchase transaction on any such security, ... or option (whether or not such repurchase or reverse repurchase transaction is a "repurchase agreement", as defined in section 101);
>
> …
>
> (vii) any other agreement or transaction that is similar to an agreement or transaction referred to in this subparagraph;
>
> (viii) any combination of the agreements or transactions referred to in this subparagraph;
>
> …

> (x) a master agreement that provides for an agreement or transaction referred to in clause (i), (ii), (iii), (iv), (v), (vi), (vii), (viii), or (ix), together with all supplements to any such master agreement, without regard to whether the master agreement provides for an agreement or transaction that is not a securities contract under this subparagraph, except that such master agreement shall be considered to be a securities contract under this subparagraph only with respect to each agreement or transaction under such master agreement that is referred to in clause (i), (ii), (iii), (iv), (v), (vi), (vii), (viii), or (ix);…

One simple argument that tokenized repos should be treated as securities contracts is policy-based: because a tokenized repo mirrors, in practical and economic substance, a traditional repo, it should logically benefit from the same legal treatment. However, ample support for this notion also comes from the text of the statute itself (and in particular, the prong capturing any "repurchase…transaction" and the broad catch-all capturing "any other agreement or transaction that is similar" to any other securities contract) and the Bankruptcy Code's legislative history.

More specifically, it is well-established that the terms "repurchase or reverse repurchase transaction" in section 741(7)(A)(i) should be given their ordinary meaning[17] – that is, an agreement that provides for the sale of a security against the transfer of funds by the recipient of such security, with a simultaneous agreement by such recipient to sell such security on demand or on a date certain against the payment of funds. Notwithstanding the additional layer of tokenization, a tokenized repo facilitates the substantive purchase and sale of *securities* and reflects the parties' intent to engage in such transactions, and should be considered to satisfy this standard. Even if a court were to be unpersuaded by this argument, however – for example, if a court were to characterize the repo as a purchase and sale of *Transfer Tokens* rather than securities – courts have noted that "the text of § 741(7)(A)(vii) . . . expands the definition of 'securities contract' to include 'any other agreement or transaction that is similar to'" an agreement or transaction referred to in Bankruptcy Code § 741(7)(A), and "[f]ew words in the English language are as expansive as 'any' and 'similar.'"[18] Tokenization does not change any of the essential characteristics of the transaction and, in any case, should not be considered to transform the character of the transaction beyond one that remains "similar to" a securities contract.

Syndicated loans

Syndicated term loans are traded by a range of sophisticated financial institutions, including commercial banks, investment banks, hedge funds, broker-dealers, and other institutions. One potential application of DLT using Transfer Tokens involves "tokenizing" an interest in a syndicated loan that has been purchased by a lender or secondary market participant pursuant to an assignment or participation. In this way, "[t]he loans held by lenders in a syndicate can be tracked automatically on a blockchain platform in the same manner as a cryptocurrency such as Bitcoin is tracked using the same technology."[19] By tokenizing an asset and allowing it to be digitally represented on a blockchain or other form of distributed ledger, the process of recording and transferring ownership of the asset should be significantly streamlined.

The syndicated loan market is perhaps an ideal candidate for the application of DLT: loans are currently originated (and trades conducted) pursuant to a complicated suite of documentation, which can theoretically be simplified and made more transparent by reflecting the essential terms of such documentation on a blockchain. Additionally, the underlying assets – loan interests – are generally not considered securities, and so the trading of loan interests among financial institutions has not been considered subject to the securities

laws.[20] The tokenization of loan interests, then, should not be considered to jeopardize that characterization, *provided* that the tokenization is designed solely to facilitate efficient transfer and record-keeping with respect to secondary market transactions in the interests.

For example, a Transfer Token should be designed such that a Token Holder would own an assignment or participation interest in a syndicated term loan in the same manner as the holder of a "traditional" assignment or participation interest, and the rights and obligations of that Token Holder would likewise be identical to that of a lender purchasing a traditional assignment or participation interest. Furthermore, such Transfer Tokens should be subject to certain restrictions on transfer, such that they could be traded only among the same sophisticated financial institutions that currently participate in the secondary market for loans, and transfer should be subject to the same restrictions (*e.g.,* the consent of the borrower) that currently apply to the sale and transfer of loan interests. Lastly, we would expect that the Tokens would be issued by the originating financial institutions (or affiliates thereof), transferred through a fully functioning private or public blockchain (which may be developed, operated, and/or maintained by the financial institutions originating or participating in the loan), and would not be made freely available to the public on a secondary market trading platform in a manner inconsistent with the current marketing and sale process applicable to syndicated loans. Such a design should, consistent with the objectives discussed above, minimize the hallmarks of a "security" described in the SEC Framework.

Notwithstanding the foregoing, the Howey test *may* be met if the Tokens possessed additional characteristics inconsistent with traditional limitations on the marketing and sale of loan interests. For example, if the Tokens were to be freely tradeable on a secondary market platform among the public or participants who did not have the ability to request information from, or conduct due diligence on, the borrower, such transferability would implicate certain of the important policy considerations of the securities laws and may cause the Tokens to be considered securities. As always, the facts and circumstances are crucial.

Artwork

One perhaps novel use of Transfer Tokens would be for the transfer of artwork. Transacting in certain types of property under American law can be a complicated exercise, and artwork falls under a category of property that faces certain practical obstacles to transfer. Contemporary art transfers typically involve a trusted intermediary (such as an art dealer or gallery) who agrees to store and present the artwork to potential buyers for a hefty fee.[21] At the same time, these traditional intermediaries offer a necessary legitimizing function, whether it is in reviewing art pieces for authenticity, evaluating the quality of art presented and sold, or collecting artwork under a centralized clearinghouse which makes it easier for art buyers and sellers to find the pieces they want. As a result, traditional intermediaries create markets for art transactions that otherwise would not exist.

DLT could be used to create more efficient artwork markets. For example, a company dedicated to compiling registries for unique assets recently partnered with a start-up company to auction digital and physical artworks associated with what could be characterized as Transfer Tokens on the Ethereum blockchain platform, with each Transfer Token associated with a unique piece of art.[22] Based on the early success of DLT-facilitated artwork transfers, traditional art houses and galleries have reportedly started experimenting with auctions using blockchain technology to move artwork between interested parties.[23] The benefits of publicly verifiable and secure digital transactions in the art space can be echoed across industries, and the success of DLT as applied to artwork might trigger other innovative uses of Transfer Tokens for other difficult-to-transfer goods.[24]

Conclusion

Transfer Tokens offer a wide range of possibilities when it comes to streamlining transactions in traditional assets. As reviewed herein, there are strong arguments that the model Transfer Tokens described in this chapter are not securities (or even, in themselves, assets), and that tokenizing an asset to facilitate its transfer should not change the legal or economic substance of the transaction. While the potential applicability of Transfer Tokens is vast, however, market participants must carefully review each implementation – especially when highly regulated financial markets are involved – to ensure that the attendant legal issues are properly addressed.

* * *

Acknowledgment

Thank you to **Will Winsett** (Milbank Leveraged Finance associate) and **Travis Gidado** (2019 Milbank summer associate) for their contributions in drafting this article.

* * *

Endnotes

1. It should be noted that the use of the term "digital assets" is somewhat of a misnomer, as assets are typically understood as things which have value. Ideally, the Transfer Token should be conceptualized as akin to a book-entry that has no value in and of itself, but merely represents an underlying asset. Even the use of the word "token" is problematic, as it can both imply value and carry negative connotations associated with the raft of tokens issued pursuant to "initial coin offerings" in recent years. Here, we use the word token to mean that it is *symbolic*.
2. One archetypal example of this concept drawn from traditional markets, of course, is the framework that has developed around the indirect ownership of securities under the Uniform Commercial Code ("UCC"). In response to a "paperwork crisis" on Wall Street during the 1960s and 1970s, when the burden of reconciling trades using the traditional certificate-based system overwhelmed brokerage firms and transfer agents, the Depository Trust Company ("DTC") was created to act as a central securities depository and hold immobilized share certificates on behalf of its participants. The regulatory scheme that governs transfers of interests in the securities held by DTC is Article 8 of the UCC, which provides that persons holding securities through brokers or custodians hold "security entitlements," rather than direct ownership of the underlying securities. Article 8 describes the package of rights held by the holder of a security entitlement (the "entitlement holder"), and provides that an entitlement holder may issue an "entitlement order" in respect of a financial asset that directs an intermediary to transfer or redeem the financial asset to which the entitlement holder has a security entitlement.
3. The use of "securities laws" in this chapter generally refers to the Securities Act of 1933 (the "Securities Act") together with the Securities Exchange Act of 1934 ("Exchange Act") and the regulations and interpretations issued thereunder.

4. *See Blockchain and Distributed Ledger Technology: An Analysis of its Impact on the Syndicated Loan Market, Part One: Generation Considerations and Blockchain Primer*, LSTA (2018).
5. *Id*.
6. *Id*.
7. *See Blockchain and Distributed Ledger Technology: An Analysis of its Impact on the Syndicated Loan Market, Part Three: Application of Blockchain Technology to the Loan Market*, LSTA (2018).
8. SEC Framework, Section I.
9. Tcherepnin v. Knight, 389 U.S. 332, 336 (1967).
10. *Id*.
11. SEC Framework, footnote 4.
12. SEC Framework, footnote 11.
13. The SEC issued, concurrently with the SEC Framework, a no-action letter addressed to an air charter service company proposing to issue "blockchain-based digital assets in the form 'tokenized' jet cards." In that letter, the SEC stated that it would not recommend enforcement against the company for issuing tokens without registration under the securities laws, because (i) the company would not use the proceeds from its token sale to develop a platform or network, which would be fully developed and operational by the time any tokens were sold, (ii) the tokens would be immediately usable for their intended functionality (*i.e.*, purchasing air charter services) at the time of the sale, (iii) transfers of the tokens would be restricted to the company's wallets, (iv) tokens would be sold at one USD per token throughout the life of the program, and each token represented an obligation by the company to supply air charter services at a value of one USD per token, (v) the company would only offer to repurchase tokens at a discount to their face value, and (vi) the tokens would be marketed in a manner that would emphasize their functionality, rather than the potential for increase in its market value. *See* https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm. On July 25, 2019, the SEC issued a second no-action letter to a gaming platform operator that proposed to sell "Quarters" to gamers for use in online video games. In that letter, the SEC noted the presence of factors similar to those cited in its previous letter, including that the platform would be fully operational immediately upon its launch (and before the sale of any Quarters), that Quarters would be immediately usable for their intended purpose and transferable only among other wallets on the platform, that Quarters would be made continuously available at a fixed price, and that Quarters would be sold solely for consumptive use as a means of accessing and interacting with participating games. *See* https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1.
14. A custodian, for these purposes, would be a financial institution licensed or chartered to provide custodial services. However, the token *issuer* may (but is not necessarily required to be) the custodian itself; for example, we envision that token issuances and redemptions may be handled by a third-party company or by a platform maintained and operated by a consortium of institutions. While we generally do not believe the identity of the token issuer should, in itself, alter the analysis or conclusion regarding whether the issued tokens are securities, additional analysis may be required regarding whether the activities of such a company or platform would cause it to fall within the

definition of a "clearing agency" subject to registration with the SEC, and if so, whether an exemption from registration would be available.

15. The model Transfer Tokens described in this Chapter are distinguishable from cryptocurrencies which are purchased because of their value and which are not typically representative of any underlying asset. Such cryptocurrencies do often bear the hallmarks of investment vehicles. The relatively nascent Libra cryptocurrency, however, breaks with the more traditional formulation of blockchain-based cryptocurrencies because it is backed by a reserve of low-volatility assets, which the creators call the Libra Reserve. While a full discussion of the Libra is beyond the scope of the chapter, the Libra is envisioned by its creators as a new type of cryptocurrency which has the potential to bring access to low cost means of transferring money to much of the population currently living with little or no access to financial services. In order to be successful, the creators of the Libra note that it must be more widely adopted than other cryptocurrencies have been to date, citing volatility as one of the major impediments to adoption. In order to alleviate the volatility often associated with blockchain-based cryptocurrencies, it will be backed by assets including bank deposits and short-term government securities. Because of this, the Libra could be errantly described as being representative of the assets which support its value. However, the assets that make up the reserve are merely a tool to decrease volatility and thereby increase rates of adoption. The Libra *itself is* intended to have value, and the underlying assets are merely intended to give comfort to early adopters. The Libra differs in a way that is crucial to the analysis of the applicability of securities law: it is intended to have value in and of itself, while a Transfer Token is intended to be merely representative of an underlying valuable asset. *See* https://libra.org/en-US/white-paper/. Federal Reserve Chairman Jerome Powell has also indicated that the Federal Reserve is concerned the Libra may raise financial stability issues in the United States given the scope of the planned implementation of the cryptocurrency. *See* https://www.wsj.com/articles/feds-jerome-powell-faces-senators-after-rate-cut-signal-11562837403.
16. 11 U.S.C. §§ 101 *et seq*.
17. *See*, *e.g.*, United States v. Hampton, 633 F.3d 334, 337 (5th Cir. 2011).
18. In re Bernard L. Madoff Investment Securities LLC, 773 F.3d 411 (2d Cir. 2014).
19. *See* Blockchain and Distributed Ledger Technology: An Analysis of its Impact on the Syndicated Loan Market, Part Three: Application of Blockchain Technology to the Loan Market, LSTA (2018).
20. *See* Banco Espanol de Credito v. Security Pac. Nat'l Bank, 973 F.2d 51 (2d Cir. 1992).
21. *See* "How to Approach Selling Art as a Collector," Artwork Archive (2019), available at https://www.artworkarchive.com/blog/how-to-approach-selling-art-as-a-collector.
22. *See* R. O'Dywer, "A Celestial Cyberdimension: Art Tokens and the Artwork as Derivative," Circa Art Magazine (accessed July 21, 2019), available at https://circaartmagazine.net/a-celestial-cyberdimension-art-tokens-and-the-artwork-as-derivative/.
23. H. Neuendorf, "Christie's Will Become the First Major Auction House to Use Blockchain in a Sale," ArtNet News (2018), available at https://news.artnet.com/market/christies-artory-blockchain-pilot-1370788.
24. *See* "Blockchain in Oil & Gas," Deloitte (accessed July 21, 2019), available at https://www2.deloitte.com/us/en/pages/consulting/articles/blockchain-digital-oil-and-gas.html.

Douglas Landy
Tel: +1 212 530 5234 / Email: dlandy@milbank.com

Milbank partner Douglas Landy, an expert in US financial services regulation and financial technology issues, is noted for his deep experience in banking and financial technology laws and has published numerous related articles and spoken on related issues. With particular expertise in cybersecurity and financial technology matters, the Volcker Rule, capital requirements, bank insolvency laws, and US-based foreign bank operations, he is widely sought after by clients, representing many of the leading global banks and central counterparties in matters in front of federal and state regulatory agencies. Select highlights include advising: The State of Wyoming on amending banking and UCC laws to encourage Bitcoin/cryptocurrency transactions; Digital Asset in a groundbreaking legal review of a proposed new blockchain product; a multinational bank on a transfer of material business information to cloud services worldwide; a global bank on cyber privacy work; and ongoing regulatory and supervisory issues raised by financial services regulators with respect to technology innovations.

James Kong
Tel: +1 212 530 5244 / Email: jkong@milbank.com

James Kong, a senior associate at Milbank, is highly experienced in bank regulatory, cybersecurity and financial technology matters. Mr. Kong has provided counsel to US and foreign financial institutions on a diverse range of regulatory and compliance matters, including with respect to the US Bank Holding Company Act, the Volcker Rule and other aspects of the Dodd-Frank Act, regulatory expectations regarding vendor risk management and third-party relationships, and anti-money laundering laws and regulations. Select highlights of his recent financial technology work includes advising: The State of Wyoming in its drafting of legislation that would provide legal clarity to financial institutions seeking to custody or secure interests in digital assets; Digital Asset in a groundbreaking legal review of a proposed new blockchain product; a multinational bank on a "first in industry" transfer of material business information from internal data storage facilities to third-party cloud service providers; and a global bank on the Volcker Rule and cybersecurity and data privacy work.

Jonathan Edwards
Tel: +1 212 530 5476 / Email: jedwards2@milbank.com

Jonathan Edwards, an associate at Milbank, represents banks and other financial institutions in a broad range of domestic and international financing transactions and financial technology matters. He has worked for a variety of clients on matters involving acquisition financings, first and second lien financings and other secured and unsecured lending transactions. Jonathan co-authored a chapter on "Regulation and Compliance in a Blockchain World" in Blockchain in Financial Markets and Beyond: Challenges and Applications, and co-authored recent client alerts titled "Bitcoin and the Volcker Rule: Are Banks Banned from Cashing in on the Crypto Craze?" and "Part 2 – Blockchain and the Volcker Rule: Are Cryptocurrency Companies Covered Funds?".

Milbank LLP

55 Hudson Yards, New York, NY 10001-2163, USA
Tel: +1 212 530 5000 / Fax: +1 212 530 5219 / URL: www.milbank.com

Argentina

Juan M. Diehl Moreno & Santiago Eraso Lomaquiz
Marval, O'Farrell & Mairal

Government attitude and definition

In Argentina, the government's attitude towards cryptocurrencies has been limited to the issuance of regulations related to their taxation and the prevention of money laundering and financing of terrorism.

The Argentine government has not implemented specific regulations on the exchange, issuance or, in general, the use of such digital assets, adopting an attitude of observation towards the development of the general impact of cryptocurrencies on the Argentine market.

In Argentina, cryptocurrencies such as Bitcoin are defined by the Financial Information Unit (*Unidad de Información Financiera*, "UIF") as a "digital representation of value that can be digitally traded and functions as a medium of exchange; and/or a unit of account; and/or a store of value, but does not have legal tender status in any jurisdiction and is neither issued nor guaranteed by any government or jurisdiction".

The Argentine Civil and Commercial Code (the "Civil Code") determines that individuals and legal entities are entitled to all the corresponding rights over the assets that are part of their property. In this regard, the Civil Code classifies assets into two categories: (i) tangible; and (ii) intangible.

As opposed to those that have a physical character, intangible assets – such as intellectual property and, in general, rights – do not materialise in the physical sphere. Thus, as a "digital representation of value", cryptocurrencies are intangible assets that are able to form part of individuals' and legal entities' property.

Section 765 of the Civil Code determines that only the Argentine "fiat" currency may be considered as "money" (*dinero*), thus excluding any possibility of including cryptocurrencies in such category.

In connection with the possibility of considering cryptocurrencies as "currency" under Argentine law, section 30 of the Argentine Central Bank's Charter (Law No. 24.144, the "Charter") provides a definition that excludes any type of instruments that: (i) have no legal tender directly or indirectly imposed by its issuer; or (ii) are not issued with nominal values lower than 10 times the amount of the highest national money bill in circulation. Thus, so far, this provision excludes the possibility of considering several cryptocurrencies as "currency" (*moneda*) under Argentine law. Moreover, extensive interpretations of Section 30 of the Charter are prohibited due to its monetary public order nature.

In this regard, the Central Bank issued, in May 2014, a non-binding press communication stating that virtual currencies are neither issued by themselves nor any other international monetary authority and, thus, have no legal tender and are not guaranteed by any government.

Nevertheless, we have not yet seen any local precedents or governmental decisions/communications in connection with any cryptocurrency issued by foreign authorities.

Government backing for cryptocurrencies

In Argentina, there are no cryptocurrencies backed by either the Argentine Government or the Argentine Central Bank.

Cryptocurrency regulation

Cryptocurrencies are not prohibited in Argentina. For the time being, the only specific regulations related to cryptocurrencies are UIF's Resolution 300/2014 (hereinafter, "UIF Resolution"), which implements additional reporting obligations to certain obliged subjects under the Anti-Money Laundering Law No. 25,246 (hereinafter, the "AML Law") (please see "Money transmission laws and anti-money laundering", below), and Law No. 27,430 (hereinafter, the "Tax Reform Law") (please see "Taxation", below).

Sales regulation

There is no specific regulation applicable to the sale of Bitcoin or other tokens under securities laws or commodities laws in Argentina.

Considering the lack of a central issuing authority, bitcoins cannot be classified as securities. Under Argentine law, securities are essentially negotiable instruments to which their issuers incorporate credit rights. Nevertheless, this conclusion may not be extended to other cryptocurrencies (*tokens*) issued by a centralised entity.

Following the example of Securities and Exchange Commissions in other parts of the world, such as those of the United Kingdom, the USA, China, Hong Kong and Brazil, the Argentine Securities and Exchange Commission (hereinafter, the "CNV", after its name in Spanish), issued a communique on Initial Coin Offerings (hereinafter, "ICOs") to warn investors of the potential risks.

The CNV clarified that ICOs would not, in principle, be subject to capital markets' regulations. Nevertheless, it also stated that certain ICOs may be subject to the control of the CNV, depending on their structure and particular characteristics.

The communique also warned investors about the following potential risks associated with ICOs: (a) lack of specific regulations; (b) price volatility and liquidity risks; (c) probability of fraud; (d) inadequate access to relevant information; (e) early stage of the projects; (f) probability of technological and infrastructure failures; and (g) transnational nature of transactions involving ICOs.

Although the CNV states that ICOs are not – in principle – subject to specific CNV control, the communique clarified that claims may be filed with the CNV in those cases where there is a suspicion that an ICO could be fraudulent.

Taxation

Among the amendments introduced by the Tax Reform Law, the taxable income derived from the commercialisation of "digital currencies" was incorporated to the Income Tax Law (hereinafter, the "ITL"). One of the main objectives of the tax reform is to tax financial income.

Neither the Tax Reform Law nor the ITL provide a definition of digital currencies, or the scope that such concept comprises. Please note the corresponding regulations of the Tax

Reform Law have not been issued yet. We understand that the meaning of such concept should be the same as the one of "virtual currencies" defined by the UIF Resolution and, therefore, such Resolution should apply to cryptocurrencies.

The ITL also determined that if the issuer of the cryptocurrencies is domiciled in Argentina, then an Argentine-sourced income would be generated as a consequence of the exchange thereof.

Provided that cryptocurrencies fall within the definition of intangible assets, the exchange of cryptocurrencies should not be impacted by Value Added Tax ("VAT").

In general, and in addition to the aforementioned examples, cryptocurrencies must be taxed like any other intangible asset.

Additionally, the Argentine Congress has recently passed Law No. 27,506 ("KEL") which provides for a promotional regime for the "*Knowledge Economy*" that will be in force between January 1, 2020, and December 31, 2029. Among others, this new tax regime shall benefit the following activities: software, computer and digital services; audiovisual production and post-production and others related to electronic and communications; professional services as long as they are exported; nanotechnology and nanoscience; aerospace and satellite industry; and artificial intelligence, robotic and industrial internet, the internet of things, augmented and virtual reality. Depending on each particular implementation, distributed ledger technologies may fall within several of the categories listed in the KEL.

The following are some of the most relevant tax benefits under the KEL:

- Fiscal stability: As of the moment of the registration and for the term of validity of the Regime. This benefit may be also extended to provincial and municipal taxes, as long as such jurisdictions adhere to the KEL.
- Income Tax: The general corporate tax rate is reduced to 15%, to the extent that the beneficiaries maintain their payroll. In addition, beneficiaries will be allowed to deduct a tax credit derived from any payment or withholding of foreign taxes, if the taxed income constitutes an Argentine source of income.
- VAT: Beneficiaries will not be subject to any withholding and/or collection VAT regimes.
- Employer social security contributions: Beneficiaries will be able to fully detract from their employer social security contributions, in relation to each employee, an amount equal to the maximum established in article 4 of Decree 814/2001 (which currently is ARS 17,509.20).
- Additional benefit: Beneficiaries will be able to obtain a one-time transferrable tax credit bond, which can be used for paying advances and/or balances of income tax and/or Value Added Tax. The bond is equal to 1.6 times the amount of the employer's social security contributions that the beneficiary did not pay due to the benefit mentioned in the paragraph above.

Money transmission laws and anti-money laundering requirements

The AML Law lists a number of persons – including financial entities, broker-dealers, credit card companies, insurance companies, public notaries, and certain government registries and agencies – that have, among other things, specific reporting obligations under the AML Law (Obliged Subjects) and provides for certain general obligations, including: applying

KYC procedures; reporting to the UIF any transaction suspected of money laundering or terrorism financing; and abstaining from disclosing to their clients or third parties the activities performed in compliance with that statute.

As explained above, one of the few regulations on cryptocurrencies in Argentina is the UIF Resolution, which requires most of the Obliged Subjects under the AML Law to report all transactions performed with cryptocurrencies, regardless of their amount.

Following the Financial Action Task Force's guidelines, the UIF also warns Obliged Subjects about the risks involved in transactions with cryptocurrencies. In so doing, the UIF also requires the Obliged Subjects listed in the UIF Resolution to strictly monitor any transactions performed with cryptocurrencies by their clients.

Promotion and testing

There are currently no "sandbox" or other programmes intended to promote research and investment in cryptocurrency in Argentina.

Except for the tax (please see "Taxation", above) and anti-money laundering (please see "Money transmission laws and anti-money laundering requirements", above) regulations, Argentine regulatory authorities have adopted a wait-and-see strategy in connection with cryptocurrencies.

Nevertheless, the Argentine Central Bank has created several research groups – among which there is a group specifically dedicated to cryptocurrencies and blockchain technologies – integrated by members of both public and private entities with the aim of analysing potential regulatory modifications to enable the use of new technologies within the financial services industry.

Ownership and licensing requirements

Although there are no specific prohibitions, given the current lack of certainty in connection with the possibility of considering certain cryptocurrencies as securities under the Capital Markets Law No. 26,831 (hereinafter, the "CML"), regulated entities subject to the CNV's control – such as investment managers, investment advisors and fund managers – tend not to operate with such assets.

Additionally, the formal requirements for the operational activities of such players have not been designed to address cryptocurrencies. Thus, several regulations may act as practical restrictions that hinder the possibility to operate with such digital assets.

Finally, regarding the provision of services through distributed ledger technologies, the Argentine Executive Branch has recently issued Decree 182/2019 (DSD), which regulates the Argentine Digital Signature Law No. 25,506. The DSD creates the new role of "trusted services providers" (*prestadores de servicios de confianza*). Among the services included in this new category, the DSD includes the "operation of block chains for the preservation of electronic documents, management of smart contracts, and other digital services". The role, licensing requirements and scope of activities of trusted services providers is pending regulation by the National Administrative Modernization Secretariat.

Mining

Mining Bitcoin and other cryptocurrencies is permitted in Argentina, although there are currently no specific regulations on such activity.

Border restrictions and declaration

There are no border restrictions or obligations to declare cryptocurrency holdings in Argentina.

Reporting requirements

There are no reporting requirements for cryptocurrency payments made in excess of a certain value.

Currently, the only specific reporting requirements in connection with cryptocurrencies are regulated by the UIF Resolution (please see "Money transmission laws and anti-money laundering requirements", above) and the Tax Reform Law (please see "Taxation", above).

Estate planning and testamentary succession

Following our explanations under "Government attitude and definition" above, cryptocurrencies must be treated as intangible assets for the purposes of estate planning and testamentary succession. Such treatment may potentially change in the future in connection with tokens issued through ICOs, subject to the CNV's view on their legal nature under the CML.

Juan M. Diehl Moreno
Tel: +54 11 4310 0100 ext. 1807 / Email: jd@marval.com

Mr. Diehl Moreno has been a partner of Marval, O'Farrell & Mairal since 2006. He specialises in banking and finance, FinTech, corporate and real estate structuring and financing, and capital markets. Several guides of the legal profession have recognised Mr. Diehl Moreno for several years as one of the leading lawyers in his field of practice in the Argentine legal sector. From 2000 to 2001, he was a foreign associate at Sidley & Austin (New York office). He graduated from the Universidad Católica Argentina in 1993, and he obtained a Master's degree in Business Law from Universidad Austral in 1996 and an LL.M., with honours, from Northwestern University School of Law in 2000. He frequently speaks at seminars and conferences both in Argentina and abroad. In recent years, Juan has been increasingly active in providing a full range of strategic legal advice to financial institutions and FinTech innovators. Many of these need advice while developing and adopting products and services such as crowdfunding, e-payment platforms, cryptocurrencies and digital banking. Juan is a member of the Innovation Group (Mesa de Innovación) of the Argentine Central Bank, which addresses potential regulatory changes aimed to foster the digitalisation of the financial services industry.

Santiago Eraso Lomaquiz
Tel: +54 11 4310 0100 ext. 1374 / Email: seel@marval.com

Santiago Eraso Lomaquiz joined Marval, O'Farrell & Mairal in 2011 and is currently a member of the Information Technology and Privacy and Intellectual Property departments, in which he is in charge of litigation. He has experience advising companies in matters related to information technologies and communication, digital and electronic signatures, e-commerce, intellectual and industrial property and personal data protection. Santiago specialises in legal and regulatory frameworks applied to technologies in the financial sector. He graduated with a law degree from the Universidad Austral in 2014 and has been a member of the High Technology Law Commission of the Colegio de Abogados de la Ciudad de Buenos Aires since 2011. Santiago is member of the Innovation Group (Mesa de Innovación) of the Argentine Central Bank. He has been given awards by the Comité de Abogados de Bancos de la República Argentina and the Colegio de Abogados de la Ciudad de Buenos Aires for his research work in his specialisation. He has also been a speaker at conferences, both locally and internationally, and has written many research papers in his practice area.

Marval, O'Farrell & Mairal

Leandro N. Alem 882, Buenos Aires, Argentina
Tel: +54 11 4310 0100 / Fax: +54 11 4310 0200 / URL: www.marval.com

Australia

Peter Reeves
Gilbert + Tobin

Government attitude and definition

The past few years have seen a sharp rise in the creation and use of cryptocurrencies in Australia, with companies such as Enosi and Havven raising millions through their Australia-based initial coin offerings (**ICOs**). The Commonwealth Government of Australia (**Government**) has shared a broader commitment to facilitate growth and innovation within the technology and cryptocurrency sector whilst also increasing its regulatory involvement.

To date, the Government has taken a largely non-interventionist approach to the regulation of cryptocurrency, allowing the landscape to evolve at a faster rate than its regulatory response. Australian law does not currently equate digital currency with fiat currency and does not treat cryptocurrency as "money".

The Governor of the Reserve Bank of Australia (**RBA**), Australia's central bank, stated during the 2017 Australian Payment Summit that the RBA has no immediate plans to issue a digital dollar akin to money. Terming it an "eAUD", the Governor noted that the rise of new technology associated with cryptocurrencies has the capacity to challenge the role of traditional financial institutions with regard to payments, but that there is currently no public policy case for the RBA to issue an eAUD. Despite this, the Governor indicated that the RBA remains open to considering wholesale applications for a digital Australian dollar and would be continuing to research this area with ongoing studies of the use of a central bank-issued digital dollar in relation to settlement arrangements.

While the Government has not intervened in cryptocurrencies and related activities to the extent that foreign government bodies have done in jurisdictions such as China or South Korea, there has been general clarification of the application of Australian regulatory regimes to the sector. For example, the Government passed the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act* 2017 (**AML/CTF Amendment Act**), which brought cryptocurrencies and tokens within the scope of Australia's anti-money laundering regime. This recognised the movement towards digital currencies becoming a popular method of paying for goods and services and transferring value in the Australian economy, but also posing significant money laundering and terrorism financing risks.

The Government has also been widely supportive of the new technologies in the blockchain and cryptocurrency space. In 2018, the Government committed $700,000 for the Digital Transformation Agency to examine possible blockchain applications within government services.

Cryptocurrency regulation

While there have been recent amendments to various pieces of legislation to accommodate

the use of cryptocurrencies, these have predominantly focused on the transactional relationships, such as the issuing and exchanging process, rather than the cryptocurrencies themselves.

Australia's primary corporate, markets, consumer credit and financial services regulator, the Australian Securities and Investments Commission (**ASIC**), has reaffirmed the view that legislative obligations and regulatory requirements are technology-neutral and apply irrespective of the mode of technology that is being used to provide a regulated service. While there hasn't been any legislation created to deal with cryptocurrencies as a discrete area of law, this does not hinder them from being captured within existing regimes under Australian law.

ASIC's recently updated regulatory guidance informs businesses of ASIC's approach to the legal status of coins (or tokens). The legal status of such coins is dependent on how they are structured and the rights attached, which ultimately determines the regulations with which an entity must comply. A key example is that cryptocurrency which is characterised as a financial product under the *Corporations Act* 2001 (Cth) (**Corporations Act**) will fall within the scope of Australia's existing financial services regulatory regime. This is discussed in more detail under "Sales regulation" below.

There are currently no specific regulations dealing with blockchain or other distributed ledger technology (**DLT**) in Australia. However, in March 2017, ASIC released an information sheet (*INFO 219 Evaluating distributed ledger technology*) outlining its approach to the regulatory issues that may rise through the implementation of blockchain technology and DLT solutions more generally. Businesses considering operating market infrastructure, or providing financial or consumer credit services using DLT, will still be subject to the compliance requirements that currently exist under the applicable licensing regime. There is a general obligation that entities relying on technology in connection with the provision of a regulated service must have the necessary organisational competence and adequate technological resources and risk-management plans in place. While the existing regulatory framework is sufficient to accommodate current implementations of DLT, as the technology matures, additional regulatory considerations will arise.

Various cryptocurrency networks have also implemented "smart" or self-executing contracts. These are permitted in Australia under the *Electronic Transactions Act* 1999 (Cth) (**ETA**) and the equivalent Australian state and territory legislation. The ETA provides a legal framework to enable electronic commerce to operate in the same way as paper-based transactions. Under the ETA, self-executing contracts are permitted in Australia, provided they meet all the traditional elements of a legal contract.

Sales regulation

The sale of cryptocurrency through an ICO is regulated by Australia's existing financial services regulatory regime. Core considerations for issuers are outlined below.

Licensing

Of particular concern to those dealing with cryptocurrencies is whether a cryptocurrency (including those offered during an ICO) constitutes a financial product and therefore triggers financial services licensing and disclosure requirements. Entities carrying on a financial services business in Australia must hold an Australian financial services licence (**AFSL**) or be exempt. The definitions of "financial product" or "financial service" under the Corporations Act are broad and ASIC has indicated in its information sheet, *INFO 225 Initial*

coin offerings (**INFO 225**), that cryptocurrency with similar features to existing financial products or securities will trigger the relevant regulatory obligations.

In INFO 225, ASIC indicated that the legal status of cryptocurrency is dependent upon the structure of the ICO and the rights attaching to the coins or tokens. ASIC has also indicated that what is a right should be interpreted broadly. Depending on the circumstances, coins or tokens may constitute interests in managed investment schemes (collective investment vehicles), securities, derivatives, or fall into a category of more generally defined financial products, all of which are subject to the Australian financial services regulatory regime. In INFO 225, ASIC has provided high-level regulatory signposts for crypto-asset participants to determine whether they have legal and regulatory obligations. These signposts are relevant to crypto-asset issuers, crypto-asset intermediaries, miners and transaction processors, crypto-asset exchanges and trading platforms, crypto-asset payment and merchant service providers, wallet providers and custody service providers, and consumers.

Broadly, entities offering coins or tokens that can be classified as financial products will need to comply with the regulatory requirements under the Corporations Act which generally include disclosure, registration, licensing and conduct obligations. An entity which facilitates payments by cryptocurrencies may also be required to hold an AFSL and the operator of a cryptocurrency exchange may be required to hold an Australian market licence if the coins or tokens traded on the exchange constitute financial products.

Generally, ASIC's regulatory guidance is consistent with the position of regulators in other jurisdictions. For example, the financial regulator in Hong Kong has outlined situations where cryptocurrency may be a financial product. ASIC has also recommended that companies wishing to conduct an ICO seek professional advice, including legal advice, and contact its Innovation Hub (discussed in detail below, "Promotion and testing") for informal assistance. This reflects its willingness to build greater investor confidence around cryptocurrency as an asset class. However, ASIC has emphasised consumer protection and compliance with the relevant laws and has taken action as a result to stop proposed ICOs targeting retail investors due to issues with disclosure and promotional materials (the requirements of which are discussed below) as well as offerings of financial products without an AFSL.

The Treasury has just closed consultation on ICOs and the relevant regulatory frameworks in Australia.

Marketing

ASIC's recognition that an ICO may involve an offer of financial products has clear implications for the marketing of an ICO. For example, an offer of a financial product to a retail client (with some exceptions) must be accompanied by a regulated disclosure document (e.g., a product disclosure statement or a prospectus and a financial services guide) that satisfies the content requirements of the Corporations Act and regulatory guidance published by ASIC. Such a disclosure document must set out prescribed information, including the provider's fee structure, to assist a client to decide whether to acquire the cryptocurrency from the provider. In some instances, the marketing activity itself may cause the ICO to be an offer of a regulated financial product.

Under the Corporations Act, depending on the minimum amount of funds invested per investor and whether the investor is a "sophisticated investor" or wholesale client, an offer of financial products may not require regulated disclosure.

Cross-border issues

Carrying on a financial services business in Australia will require a foreign financial services provider (**FFSP**) to hold an AFSL, unless relief is granted. Entities, including FFSPs, should note that the Corporations Act may apply to an ICO regardless of whether it was created and offered from Australia or overseas. Currently, Australia has cooperation (passporting) arrangements with regulators in foreign jurisdictions (including the United States of America and the United Kingdom), which enable FFSPs regulated in those jurisdictions to provide financial services in Australia without holding an AFSL. However, the passporting relief is currently only available in relation to the provision of services to wholesale clients (i.e. accredited investors), and the FFSP must only provide the services it is authorised to provide in its home jurisdiction. However, ASIC has announced that it will be repealing this passport relief, and instead will implement a new regime requiring FFSPs to apply for a foreign AFSL. It is expected that the new regime will apply from 30 September 2019.

Foreign companies taken to be carrying on a business in Australia, including by issuing cryptocurrency or operating a platform developed using ICO proceeds, may be required to either establish a local presence (i.e., register with ASIC and create a branch) or incorporate a subsidiary. Broadly, the greater the level of system, repetition or continuity associated with an entity's business activities in Australia, the greater the likelihood that registration will be required. Generally, a company holding an AFSL will be carrying on a business in Australia and will trigger the requirement.

Promoters should also be aware that if they wish to market their cryptocurrency to Australian residents, and the coins or tokens are considered a financial product under the Corporations Act, they will not be permitted to market the products unless the requisite licensing and disclosure requirements are met. Generally, a service provider from outside of Australia may respond to requests for information and issue products to an Australian resident if the resident makes the first (unsolicited) approach and there has been no conduct on the part of the issuer designed to induce the investor to make contact, or activities that could be misconstrued as the provider inducing the investor to make contact.

Design and distribution obligations and product intervention powers

The Government has passed the *Treasury Laws Amendment (Design and Distribution Obligations and Product Intervention Powers) Act 2019* (Cth) (**DDO PIP Act**) and released the Corporations Amendment (Design and Distribution Obligations and Product Intervention Powers) Regulations 2018, which may impact the way cryptocurrencies are structured and ICOs conducted in future. The DDO PIP Act introduces new design and distribution obligations in relation to financial products and provides ASIC with temporary product intervention powers where there is a risk of significant consumer detriment. The new arrangements aim to ensure that financial products are targeted at the correct category of potential investors. At the time of writing, ASIC has yet to release guidance on the way it might interpret its powers beyond its initial submission to consultation on the legislation, but ASIC's powers are highly likely to impact marketing and distribution practices in the cryptocurrency sector.

Consumer law

Even if an ICO is not regulated under the Corporations Act, it may still be subject to other regulation and laws, including the Australian Consumer Law set out at Schedule 2 to the *Competition and Consumer Act 2010* (Cth) (**ACL**) relating to the offer of services or products to Australian consumers. The ACL prohibits misleading or deceptive conduct in a range of circumstances including in the context of marketing and advertising. As such, care must be

taken in ICO promotional material to ensure that buyers are not misled or deceived and that the promotional material does not contain false information. In addition, promoters and sellers are prohibited from engaging in unconscionable conduct and must ensure the coins or tokens issued are fit for their intended purpose.

The protections of the ACL are generally reflected in the *Australian Securities and Investments Commission Act* 2001 (Cth) (**ASIC Act**), providing substantially similar protection to investors in financial products or services.

ASIC has also received delegated powers from the Australian Competition and Consumer Commission to enable it to take action against misleading or deceptive conduct in marketing or issuing in ICOs (regardless of whether it involves a financial product). ASIC has indicated misleading or deceptive conduct in relation to ICOs may include:

- using social media to create the appearance of greater levels of public interest;
- creating the appearance of greater levels of buying and selling activity for an ICO or a crypto-asset by engaging in (or arranging for others to engage in) certain trading strategies;
- failing to disclose appropriate information about the ICO; or
- suggesting that the ICO is a regulated product or endorsed by a regulator when it is not.

ASIC has stated that it will use this power to issue further inquiries into ICO issuers and their advisers to identify potentially unlicensed and misleading conduct.

A range of consequences may apply for failing to comply with the ACL or the ASIC Act, including monetary penalties, injunctions, compensatory damages and costs orders.

Taxation

The taxation of cryptocurrency in Australia has been an area of much debate, despite recent attempts by the Australian Taxation Office (**ATO**) to clarify the operation of the tax law. For income tax purposes, the ATO views cryptocurrency as an asset that is held or traded (rather than as money or a foreign currency).

Investors and holders of cryptocurrencies

The tax implications for investors, holders and users of cryptocurrency depends upon the intended use of that cryptocurrency. The summary below applies to investors who are Australian residents for tax purposes.

Investors (including funds) in the business of trading cryptocurrencies are likely to be subject to the trading stock provisions, much like a supermarket treats its goods for sale as trading stock. The gain on the sale of cryptocurrencies will be taxable to such investors on "revenue account", and any losses will be deductible on a similar basis.

Otherwise, the ATO has indicated that cryptocurrency will likely be a capital gains tax (**CGT**) asset. The gain on its disposal will be subject to CGT. Capital gains may be discounted under the CGT discount provisions, so long as the investor satisfies the conditions for the discount. Note that the ATO's views on the income tax implications of transactions involving cryptocurrencies is in a state of flux due to the rapid evolution of both cryptocurrency technology and its uses.

Capital losses made on cryptocurrencies which are "personal use" assets are disregarded. This includes cryptocurrencies acquired or kept for personal use or consumption (i.e., to buy goods or services). Capital gains on personal use assets are only disregarded where the asset was acquired for less than A$10,000.

Issuers of cryptocurrencies

In the context of an ICO, a coin issuance by an entity that is either an Australian tax resident, or acting through an Australian "permanent establishment", will likely be taxable in Australia. The current corporate tax rate in Australia is either 27.5% or 30%. If the issued coins are characterised as equity for tax purposes, the ICO proceeds should not be taxable to the issuer, but all future returns to the token holders will be treated as dividends.

Australian Goods and Services Tax (**GST**)

Supplies and acquisitions of digital currency made from 1 July 2017 are not subject to GST on the basis that they will be input taxed financial supplies. Consequently, suppliers of digital currency will not be required to charge GST on these supplies, and a purchaser would not be entitled to GST refunds (i.e., input tax credits) for these corresponding acquisitions. On the basis that digital currency is a method of payment, as an alternative to money, the normal GST rules apply to the payment or receipt of digital currency for goods and services.

The term "digital currency" in the GST legislation requires that it is a digital unit of value that has all the following characteristics:

- it is fungible and can be provided as payment for any type of purchase;
- it is generally available to the public free of any substantial restrictions;
- it is not denominated in any country's currency;
- the value is not derived from or dependent on anything else; and
- it does not give an entitlement or privileges to receive something else.

Enforcement

The ATO has created a specialist task force to tackle cryptocurrency tax evasion. The ATO also collects bulk records from Australian cryptocurrency designated service providers to conduct data matching to ensure that cryptocurrency users are paying the right amount of tax. With the broader regulatory trend around the globe moving from guidance to enforcement, it is likely that the ATO will also begin enforcing tax liabilities more aggressively.

In relation to mining cryptocurrency, the ATO has also released guidance in relation to how these activities will be taxed. This is discussed in "Mining", below.

Money transmission laws and anti-money laundering requirements

In 2017, the Government passed the AML/CTF Amendment Act, which brought cryptocurrencies and tokens within the scope of Australia's anti-money laundering and counter-terrorism financing (**AML/CTF**) regulatory framework. The amendments came into force on 3 April 2018 and focus on the point of intersection between cryptocurrencies and the regulated financial sector, namely digital currency exchanges.

Broadly, digital currency exchange (**DCE**) providers are now required to register with the Australian Transaction Reports and Analysis Centre (**AUSTRAC**) in order to operate, with a penalty of up to two years' imprisonment or a fine of up to A$105,000, or both, for failing to register. Registered exchanges will be required to implement know-your-customer processes to adequately verify the identity of their customers, with ongoing obligations to monitor and report suspicious and large transactions. Exchange operators are also required to keep certain records relating to customer identification and transactions for up to seven years.

Bringing DCE providers within the ambit of the AML/CTF framework is intended to help legitimise the use of cryptocurrency while protecting the integrity of the financial system in which it operates.

Promotion and testing

Regulators in Australia have generally been receptive to fintech and innovation and have sought to improve their understanding of, and engagement with businesses by regularly consulting with industry on proposed regulatory changes. While there are no programmes specifically promoting research and investment in cryptocurrency, both ASIC and AUSTRAC have established Innovation Hubs designed to assist fintech businesses more broadly in understanding their obligations under Australian law. ASIC has also entered into a number of co-operation agreements with overseas regulators which aim to further understand the approach of fintech businesses in other jurisdictions (as discussed below).

ASIC Innovation Hub

The ASIC Innovation Hub is designed to foster innovation that could benefit consumers by helping Australian fintech start-ups navigate the Australian regulatory system. The Innovation Hub provides tailored information and access to informal assistance intended to streamline the AFSL process for innovative fintech start-ups, which could include cryptocurrency-related businesses.

In December 2016, ASIC made certain class orders establishing a fintech licensing exemption and released *Regulatory Guide 257*, which details ASIC's framework for fintech businesses to test certain financial services, financial products and credit activities without holding an AFSL or Australian credit licence by relying on the class orders (referred to as the regulatory sandbox). There are strict eligibility requirements for both the type of businesses that can enter the regulatory sandbox and the products and services that qualify for the licensing exemption. There are restrictions on how many persons can be provided with a financial product or service, and caps on the value of the financial products or services which can be provided. Businesses may only rely conditionally on the relief for 12 months.

The framework relating to ASIC's regulatory sandbox has been subject to review. The Government recently closed its consultation on draft legislation and regulations outlining an enhanced framework that allows businesses to test a wider range of products and services for a longer period of time. ASIC has also released a consultation paper suggesting that no changes to its existing fintech licensing exemption will be made.

Cross-border business

Beyond this, ASIC has engaged with regulators overseas to deepen its understanding of innovation in financial services, including in relation to cryptocurrencies. In particular, ASIC and the United Kingdom's Financial Conduct Authority have signed an Enhanced Cooperation Agreement, which allows the two regulators to, among other things, information-share, refer innovative businesses to each regulator's respective regulatory sandbox, and conduct joint policy work. ASIC also currently has either information-sharing or cooperation agreements with regulators in Hong Kong, Singapore, Canada, Kenya and Indonesia. These arrangements facilitate the cross-sharing of information on fintech market trends, encourage referrals of fintech companies and share insights from proofs of concepts and innovation competitions.

ASIC is also a signatory to the IOSCO Multilateral Memorandum of Understanding, which has committed over 100 regulators to mutually assist and cooperate with each other, particularly in relation to the enforcement of securities laws.

ASIC has committed to supporting financial innovation in the interests of consumers by joining the Global Financial Innovation Network (**GFIN**), which was formally launched in January 2019 by a group of financial regulators across 29 member organisations. The GFIN is dedicated to facilitating regulatory collaboration in a cross-border context and provides more efficient means for innovative businesses to interact with regulators.

In 2019, a group of fintech associations formed the Asia-Pacific FinTech Network, which is designed to facilitate greater collaboration, cooperation and innovation across the region. The network will focus on sectors including RegTech, Blockchain, Payment Systems, Artificial Intelligence and Financial Inclusion and is expected to accelerate fintech development and lower financial costs both domestically and internationally.

AUSTRAC Innovation Hub

AUSTRAC's Fintel Alliance is a private-public partnership seeking to develop "smarter regulation". This includes setting up an innovation hub targeted at improving the fintech sector's relationship with the government and regulators. The hub will provide a regulatory sandbox for fintech businesses to test financial products and services without risking regulatory action or costs.

AUSTRAC has also implemented a new dedicated webpage providing information about the AML/CTF regime and AUSTRAC's role to assist businesses wishing to create a new financial service product or to understand their AML/CTF obligations. In its annual report for 2016–17, AUSTRAC noted that the webpage had been successful, garnering over 40 direct enquiries from entities developing innovative new approaches to providing "designated services" as defined under the *Anti-money Laundering and Counter-terrorism Financing Act 2006* (Cth) (**AML/CTF Act**). As discussed above, designated services now include the provision of DCE services, and consequently DCE providers may contact AUSTRAC through the webpage to understand their regulatory obligations.

Ownership and licensing requirements

At the time of writing, there are currently no explicit restrictions on investment managers owning cryptocurrencies for investment purposes. However, investment managers may be subject to Australia's financial services regulatory regime where the cryptocurrencies held are deemed to be "financial products".

For example, investment managers providing investment advice on cryptocurrencies held that are financial products will be deemed to be providing financial product advice under the Corporations Act and will need to hold an AFSL or be exempt. ASIC has provided significant guidance in relation to complying with the relevant advice, conduct and disclosure obligations, as well as the conflicted remuneration provisions under the Corporations Act. Further, investment managers may be required to hold an AFSL with a custodial or depository authorisation or be exempt from this requirement if investment managers wish to hold cryptocurrencies that are financial products on behalf of clients.

Against the backdrop of the *Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry* and the broader innovation agenda of the Government, Australia has seen a rapidly rising interest in robo-advice or digital advice models. The provision of robo-advice is where algorithms and technology provide automated financial product advice without a human advisor. For investment or fund businesses seeking to operate in Australia by providing digital or hybrid advice (including with respect to investing in cryptocurrencies), there are licensing requirements under the

Corporations Act. ASIC has released *Regulatory Guide 255: providing digital financial product advice to retail clients*, which details issues that digital advice providers need to consider generally, during the AFSL application stage and when providing digital financial product advice to retail clients. It is intended to complement ASIC's existing guidance including *Regulatory Guide 36: Licensing: Financial product advice and dealing*. Financial product advisers also need to consider their conduct and disclosure obligations. ASIC has released *Regulatory Guide 175 Licensing: Financial product adviser – conduct and disclosure* with respect to this.

Mining

At the time of writing, there are no prohibitions on mining Bitcoin or other cryptocurrencies in Australia.

Cryptocurrency mining taxation

The ATO has released some guidance on its approach to taxation in relation to cryptocurrency mining activities. The summary below applies to miners or business owners who are Australian residents for tax purposes.

Income derived by a taxpayer from "carrying on a business" of mining cryptocurrency must be included in the calculation of their assessable income. Whether or not a taxpayer's activities amount to carrying on a business is "a question of fact and degree", and is ultimately determined by weighing up the taxpayer's individual facts and circumstances. Generally (but not exclusively), where the activities are undertaken for a profit-making purpose, are repetitious, involve ongoing effort, and include business documentation, the activities would amount to "carrying on a business".

Cryptocurrency miners would also be subject to tax on any gains or profits derived from transferring cryptocurrency mined to a third party.

Where carrying on a business, outgoing and losses would be deductible to the taxpayer (subject to integrity measures and the "non-commercial loss" rules).

Whether or not GST is payable by a cryptocurrency miner on its supply of new cryptocurrency depends on a number of factors, including its specific features, whether the miner is registered for GST, and whether the supply is made in the course of the miner's enterprise.

The specific features of cryptocurrency include: it being a type of security or other derivative; it being "digital currency" as defined in the GST legislation (see "Taxation", above); or it providing a right or entitlement to goods or services. If the cryptocurrency is "digital currency", its supply will not be subject to any GST because it will be an input taxed financial supply (assuming the other requirements are satisfied).

A cryptocurrency miner would generally be required to register for GST if its annual GST turnover is $75,000 or more, excluding the value of its supplies of digital currencies and other input-taxed supplies. However, a miner who does not satisfy this GST registration threshold may nevertheless elect to register for GST in order to claim from the ATO full or reduced input tax credits (i.e., GST refunds) for the GST cost of its business acquisitions (but acquisitions that relate to the sales or acquisitions of digital currencies are *prima facie* non-creditable or non-refundable).

Cybersecurity

More generally, with the rise of cloud-based Bitcoin mining enterprises in Australia, mining businesses should carefully consider cybersecurity issues in relation to mining activities.

In its Corporate Plan 2018 to 2022, ASIC signalled that cyber resilience would be a key focus area for the regulator, particularly in relation to monitoring threats of harm from emerging products, the adequate management of technological solutions and misconduct facilitated by or through cyber-based tools. CERT Australia (now part of the Australian Cyber Security Centre) has noted that there has been an increase in cryptomining malware affecting business' resources and processing capacity. ASIC has also released regulatory guidance indicating its expectations for licensees' cloud computing security arrangements. Two reports, namely 429 *Cyber resilience: Health check* and 555 *Cyber resilience of firms in Australia's financial markets*, examine and provide examples of good practices identified across the financial services industry. The reports contain questions that board members and senior management of financial organisations should ask when considering cyber resilience.

Border restrictions and declaration

There are currently no border restrictions or obligations to declare cryptocurrency holdings when entering or leaving Australia.

The AML/CTF Act mandates that both individuals and businesses must submit reports where physical currency in excess of A$10,000 (or foreign currency equivalent) is brought into or taken out of Australia. This requirement is restricted to "physical currency", which AUSTRAC has defined as being any coin or printed note of Australia or a foreign country that is designated as legal tender, and is circulated, customarily used and accepted as a medium of exchange in the country of issue. Although recent discourse indicates that some governments have created or are attempting to issue official cryptocurrencies, the intangible nature of cryptocurrency seems to remain a bar to cryptocurrency being captured by declaration obligations under the AML/CTF Act.

It should be noted that the AML/CTF Act was amended to address some aspects of cryptocurrency transfer and exchange; however, this amendment did not see the scope of AML/CTF regulation widen the border restrictions. At the time of writing, there appears to be no indication that any such further amendment to include border restrictions is being contemplated.

Reporting requirements

The AML/CTF Act imposes obligations on entities that provide "designated services" with an Australian connection. Generally, the AML/CTF Act applies to any entity that engages in financial services or credit (consumer or business) activities in Australia including the provision of DCE services. These obligations include record-keeping and reporting requirements. AUSTRAC has released draft AML/CTF rules, which outline reportable details for matters including but not limited to threshold transaction reports (**TTRs**). TTRs will be required to be submitted where transactions over A$10,000 have occurred.

Reportable information includes, among other details, the denomination or code of the digital currency and the number of digital currency units, a description of the digital currency including details of the backing asset or thing (if known), the Internet Protocol address information of the payee, the social media identifiers of the payee, and the unique identifiers relating to the digital currency wallet of the payee.

In April 2016, the Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations (**AML/CTF**

Report), which contained 84 recommendations to improve Australia's AML/CTF regime, was released. The AML/CTF Report contemplated two phases of consultation of consultation and implementation, with Phase 1 including priority projects completed in 2017, while Phase 2 progresses major, long-term reforms. These reforms should, among other things, clarify record-keeping requirements and reporting obligations for reporting entities.

Estate planning and testamentary succession

To date, there has been no explicit regulation or case law surrounding the treatment of cryptocurrency in Australian succession law. Generally, if estate plans do not cater for cryptocurrency and steps are not taken to ensure executors can access a deceased's cryptocurrency, it may not pass to the beneficiaries.

A will should be drafted to give the executor authority to deal with digital assets. As cryptocurrencies are generally held anonymously, a will should also establish the existence of the cryptocurrency as an asset to be distributed to beneficiaries. A method must also be established to ensure passwords to digital wallets and external drives storing cryptocurrency are accessible by a trusted representative. Unlike a bank account which can be frozen upon death, anyone can access a digital wallet, so care should be taken to ensure external drives and passwords are not easily accessible on the face of the will. This may include providing a memorandum of passwords and accounts to the executor to be placed in a safe custody facility which remains unopened until a will is called upon.

There may also be tax implications arising for the beneficiaries of cryptocurrencies, which are similar to the tax implications for cryptocurrency holders. See "Taxation" above, for further details.

Peter Reeves
Tel: +61 2 9263 4000 / Email: preeves@gtlaw.com.au

Peter Reeves is a partner in Gilbert + Tobin's Corporate Advisory group and is an expert and market-leading practitioner in financial services regulation and funds management. He leads the Financial Services and Fintech practices at G+T. Peter advises domestic and off-shore corporates, financial institutions, funds, managers and other market participants in relation to establishing, structuring and operating financial services sector businesses in Australia. He also advises across a range of issues relevant to the fintech and digital sectors, including platform structuring and establishment, payment solutions, blockchain solutions and global crypto-asset strategies. *Chambers 2019* ranks Peter in Band 1 for Fintech.

Gilbert + Tobin

Level 35, Tower Two, International Towers Sydney, 200 Barangaroo Avenue, Barangaroo, Sydney NSW 2000, Australia
Tel: +61 2 9263 4000 / URL: www.gtlaw.com.au

Austria

Ursula Rath & Thomas Kulnigg
Schoenherr Attorneys at Law

Government attitude and definition

Austrian financial regulators and policymakers are generally receptive to cryptocurrencies, new technologies and fintech.

The Austrian government closely monitors developments in the area of alternative means of financing through distributed ledger technology and other digital assets, such as initial coin offerings ("ICOs"), initial token offerings ("ITOs") or security token offerings ("STO").

Also, the Ministry of Finance has established an advisory board and proclaimed that it aims to foster growth in the fintech sector. Due to current governmental changes and the upcoming elections in fall 2019, it is currently uncertain whether the activities of the advisory board will be continued after the elections and the establishment of a new federal government for Austria.

At the same time, regulators and the government stress that integrity, security and investor protection must not be compromised. While Austrian law does not prohibit cryptocurrencies, the Austrian Financial Markets Authority (*Finanzmarktaufsicht*; FMA) regularly warns investors of the risks of cryptocurrencies, stating in particular that virtual currencies like Bitcoin and trading platforms for such instruments are neither regulated nor supervised by the FMA.

Cryptocurrency regulation

In Austria, no cryptocurrencies or fintech-specific laws or regulations have currently been enacted. Although there is no statutory definition of cryptocurrencies, according to the Austrian regulator, the FMA cryptocurrencies are typically characterised as follows:

- they are not issued by any central bank or governmental authority;
- new units of value are typically created using a predefined procedure within a computer network (commonly referred to as "mining");
- there is no central authority which verifies or manages transactions;
- transactions are recorded on a decentralised, publicly held ledger (commonly referred to as "blockchain") and, once executed, cannot be revoked; and
- electronic wallets may be used to store and manage virtual currencies (commonly referred to as "wallets").

As follows from the above, cryptocurrency is currently not treated as "money" or otherwise given equal status to domestic or foreign fiat currency in Austria. Likewise, there are not yet any cryptocurrencies which are backed by the Austrian government or the Austrian National Bank.

From an Austrian financial services regulatory perspective, cryptocurrencies are currently neither treated as financial instruments (in particular, not as securities or derivatives) nor as currency (domestic or foreign), but as commodities. It is worth noting, however, that derivative instruments referencing cryptocurrencies or tokens will qualify as financial instruments under MiFID II and hence will be covered by financial services regulation under MiFID II/MiFIR.

While commodities as such are not subject to supervision by the FMA, this does not mean that business activities involving cryptocurrencies are entirely outside the Austrian regulatory remit. Depending on their precise features/content, the operation of various business models based on cryptocurrencies may trigger licensing requirements under the Austrian Banking Act (BWG; *Bankwesengesetz*), the Austrian Alternative Investment Fund Manager Act (AIFMG; *Alternative Investmentfonds Manager-Gesetz*), the Austrian Payment Services Act (ZaDiG; *Zahlungsdienstegesetz*), the Austrian Electronic Money Act (*E-Geld Gesetz*) and/or prospectus and other disclosure requirements under the Austrian Capital Markets Act (KMG; *Kapitalmarktgesetz*) and the Austrian Alternative Financing Act (AltFG; *Alternativfinanzierungsgesetz*).

In this respect, the general legal framework also applies to cryptocurrencies and new technologies. The FMA is known to apply a "technology-neutral" supervisory approach, meaning that products and services are subject to the same regulatory framework as 'traditional' products/services. If and to what extent financial services regulation applies, primarily depends on the actual product features/activities.

Innovative business models involving cryptocurrencies may be subject to licensing requirements and governed by:

- the Banking Act – for example, if funds are raised for investment into cryptocurrencies;
- the Payment Services Act 2018 – for example, if information from several accounts is consolidated or if payments are initiated;
- the Securities Supervision Act 2018 – for example, if investment advice or portfolio management are provided in relation to financial instruments referencing cryptocurrencies or if orders are received and transmitted in relation to such instruments;
- the Act on Alternative Investment Fund Managers – for example, if funds are raised for investment into cryptocurrencies according to a pre-defined investment strategy; and
- the Electronic Money Act – when issuing electronic money.

The FMA has published further guidance on the regulatory treatment of certain activities around cryptocurrencies, ICOs/ITOs/STOs and fintech on the fintech navigator section of its website at https://www.fma.gv.at/en/cross-sectoral-topics/fintech/fintech-navigator/.

Key areas to note are the following:

- Purely technical services do not require a licence under financial services regulation. If, however, a technical billing service also includes transfer of funds, this would no longer be considered a purely technical service and would need to be tested against licensing requirements under the Austrian Banking Act, the Austrian Payment Services Act and the Austrian E-Money Act.
- Alternative currencies, payment instruments or means of payment may trigger a licensing requirement if they are intended for payment at third parties, and the network within which they can be used to purchase goods/services is large in terms of

geographical reach, type of products/services and/or number of accepting parties (there is a licensing exception for restricted networks, but this has become increasingly strict following the implementation of Directive 2015/2366/EU ("PSD II")). Also, if accounts are operated in connection with currencies, payment instruments or means of payment through which payments are made, the entity holding the accounts may be obliged to become licensed as a payment service provider.

- If capital is raised in order to invest proceeds into cryptocurrencies or mining, this could be regulated as a banking business (deposits business) or as managing an alternative investment fund under the Austrian Alternative Investment Fund Managers Act if funds are invested in accordance with a defined investment strategy and returns in each case depend on the performance of the underlying investment. If the capital-raising is structured through the issuance of shares or similar participation in a corporation or partnership, this may also trigger prospectus requirements under Austrian securities laws (see "Sales regulation", below).
- Online platforms for acquiring virtual currencies which also settle/process payments in domestic or foreign currency through their own accounts may require a licence under the Austrian Payment Services Act. Generally, if funds pass through the provider's accounts, this will trigger a licence requirement under payment services regulations. Some online service providers therefore cooperate with licensed partners and transfer funds via their accounts.
- Brokers of new or alternative payment methods may need to become licensed if they are considering intermediating deposits or loans/insurance. This would be the case if an app or online platform was linked to a specific deposit/current account. The mere listing of product information, for example, via product comparison portals, would not require a licence.
- While merely buying and selling virtual currencies in one's own name and for one's own account generally does not trigger a licence requirement, the buying and selling of virtual currencies may form part of business models that do require a licence. For instance, the operation of a Bitcoin vending machine may trigger a licence requirement, depending on its features. Also, clearing a Bitcoin vending machine and subsequently transferring any funds collected to a third party may require a payment services licence for money remittance under the Austrian Payment Services Act.
- There is currently no deposit guarantee scheme and no legal investor protection scheme for cryptocurrencies or tokens.

Given the diversity, complexity and rapid evolution of business models in the fintech space, the regulatory treatment of any business models involving cryptocurrencies or tokens will need to be assessed on a case-by-case basis.

The FMA therefore encourages discussion of the regulatory treatment prior to engaging in any business activity. It has set up a dedicated specialist team and fintech contact portal dedicated to those areas, which handles all fintech-related queries.

Sales regulation

There is currently no specific regulation dedicated to the sale of cryptocurrencies or tokens, which are thus covered by general securities and commodities laws.

Depending on a token's terms and conditions/features, certain token offerings/sales may be subject to prospectus requirements under Austrian securities laws, unless an exemption

applies. Each (public) offering must be assessed on a case-by-case basis and the regulatory assessment will depend on the specific technical, functional and economic design of the instruments offered.

For Austrian supervisory law purposes, the FMA has broadly classified tokens as set out below, noting that in practice hybrid forms and overlaps frequently occur and that such classification is subject to any further national and international legal developments:

- Security/investment tokens: tokens that represent assets, in particular payment claims against a specific issuer, e.g. to participate in future earnings or cash-flows or tokens that represent membership rights within the meaning of corporate law. The design of such tokens is often similar to that of "classical securities", in particular bonds or shares. Security tokens are therefore frequently considered as transferable securities pursuant to the Austrian Capital Markets Act and the Austrian Securities Supervision Act. If a token is classified as a transferable security, this has far reaching regulatory implications not only for the token issuer (as this may trigger prospectus requirements under Austrian securities laws) but also for trading platforms on which such token is traded (as they will need to become authorised as stock exchanges or regulated trading venues) or custodial or wallet providers (as they will need to become authorised for safekeeping and administration), amongst others. Even if a security token does not classify as a transferable security (in particular because that token/coin is not-transferable or its transfer is restricted), but provides access to capital or returns for a risk-sharing group of investors, it may classify as a "CMA investment" and its offering may trigger prospectus or disclosure requirements under the Austrian Capital Markets Act or Austrian Alternative Financing Act, unless an exemption applies.
- Utility tokens: There are many designs of utility tokens. While these are often comparable to vouchers, utility tokens occur in many different forms and also fulfil the function of payment tokens or security tokens (hybrid design) making their classification for supervisory law purposes rather difficult. If the token can only be used for designing a product or a service and is not otherwise associated with any claims or if the token only grants access to a product or a service without simultaneously serving a payment purpose, then such token will not be covered by supervisory laws. If on the other hand the token may be redeemed at the issuer or other users of the platform for the use of a product or a service, then it fulfils a payment function rather similar to a payment token.
- Payment/currency tokens: tokens that are accepted as means of payment for the purchase of goods or services, or tokens that serve the purpose of transferring money and value but do not confer any claims against a specific issuer (e.g. Bitcoin or Ripple).

Accordingly, due to their specific content/features, security/investment tokens will typically be subject to prospectus requirements (unless an exemption applies), while other types of tokens, such as utility tokens or payment/currency tokens, usually will not. No prospectus will need to be published if a prospectus exemption applies. This will be the case if the respective tokens are only offered to qualified investors, or if the offering is directed to fewer than 150 persons who are not qualified investors per EEA Member State, or if the minimum investment is at least €100,000 per investor. For offerings of securities below €2,000,000 per year, the Austria Alternative Financing Act applies. The Austria Alternative Financing Act, which uses the same definition for securities as the Austrian Capital Markets Act and thus also applies to public offerings of security tokens, provides for certain disclosure requirements in relation to such offerings. It also regulates the activities of internet platforms that handle such offerings (crowd platforms).

Besides issuers, platform operators may also have the obligation to publish a prospectus, as they may be considered "offerors" for these instruments under the Austrian Capital Markets Act and may, as outlined above, be subject to the requirements of the Austrian Alternative Financing Act.

Breaches of the obligation to publish a prospectus are subject to severe sanctions, including under criminal laws.

Taxation

Income tax treatment of cryptocurrencies

In general, capital gains from the sale of cryptocurrencies held as business assets, and income from commercial activities related to cryptocurrencies (e.g. mining, brokerage), are subject to progressive income tax rates of up to 55% for individuals and 25% for corporations.

Special rules apply to cryptocurrencies treated as investment assets and other (non-business) assets:

Cryptocurrencies are treated as investment assets in case the taxpayer uses them to generate interest income. In this case, capital gains from a subsequent sale are taxed at 27.5% for individuals (taxation at lower progressive income tax rates optional) or at 25% for corporations.

In case cryptocurrencies are not used to generate interest income, are only acquired and sold occasionally (private sales) and are not part of a business (non-business assets), capital gains are subject to taxation of up to 55% for individuals only if they are acquired and sold within 12 months. A tax exemption applies if capital gains do not exceed €440 per calendar year. In case cryptocurrencies are held for longer than 12 months, capital gains are not taxable.

VAT treatment of cryptocurrencies

The exchange of cryptocurrencies (e.g. Bitcoin) into fiat currency (e.g. euro) and *vice versa* is VAT-exempt (CJEU 22 October 2015, C-264/14, Hedqvist; VAT guidelines para. 759). Bitcoin mining as such is not subject to VAT (CJEU 22 October 2015, C-264/14, Hedqvist).

Purchases/supplies of goods or services that are subject to VAT, and which are paid for in cryptocurrency, are treated no differently from payments with fiat currency. The assessment basis for transactions subject to VAT is the fair market value of the units.

Money transmission laws and anti-money laundering requirements

As stated above, money transmission laws may apply to certain business activities involving cryptocurrencies. Cryptocurrencies and tokens used as means of payment may trigger a licensing requirement if they are intended for payment at third parties, and the network within which they can be used to purchase goods/services is large in terms of geographical reach, type of products/services and/or number of accepting parties. Also, if accounts are operated in connection with currencies, payment instruments or means of payment, through which payments are made, the entity holding the accounts may be obliged to become licensed as a payment service provider.

As of today, activities involving cryptocurrencies are only subject to anti-money laundering ("AML") requirements if they require a licence under financial services regulation (e.g. as provision of payment services) or if they are subject to AML requirements under commercial law. Pursuant to the Austrian Trade Code (*Gewerbeordnung*, GewO), commercial operators, including auctioneers, are subject to AML requirements if they make or receive cash payments of at least €10,000.

However, upon implementation of the fifth Anti-Money Laundering Directive, which will amend the current fourth Anti-Money Laundering Directive (2015/849/EU) and will likely enter into force by 10 January 2020, certain providers of crypto-related services will become subject to AML obligations, including KYC checks and AML prevention systems. The current draft bill (which is still under review) would also subject, beside custodian wallet providers (i.e. entities providing services to safeguard private cryptographic keys to hold, store and transfer virtual currencies on behalf of their customers) and providers of exchange services between virtual currencies and fiat currencies, providers of (i) exchange services between virtual currencies, (ii) services in relation to the transfer of virtual currencies, and (iii) financial services in relation to the issuance and sale of virtual currencies to said AML obligations. It remains to be seen if the draft bill, which provides for stricter requirements than the fifth Anti-Money Laundering Directive, will be adopted as currently proposed.

Promotion and testing

True to the government's motto "advice instead of punishment", the Austrian Ministry of Finance has been working on legislative proposals for setting up a dedicated regulatory sandbox programme that could go live in 2019. In such a sandbox, companies that require a financial services licence will be able to swiftly and comprehensively clarify regulatory requirements for innovative business models in a constant dialogue with the regulator and, if necessary, test such business model based on a scaled down licence. The selection criteria for admission to the sandbox and further details are currently still evaluated but will be based on international best practice.

Ownership and licensing requirements

Cryptocurrencies are currently treated by the Austrian regulator as commodities for supervisory law purposes (see "Cryptocurrency regulation", above). Applicable law as well as internal investment policies may restrict investment managers of certain investors to own cryptocurrencies for investment purposes. For example, UCITS funds, real estate investment funds pursuant to the Austrian Real Estate Investment Funds Act, or staff provision funds and their managers, may not invest into commodities. Pension funds and insurance companies are subject to qualitative and quantitative investment restrictions which will typically not permit direct investment into cryptocurrencies. Depending on the relevant investment policy, alternative investment funds ("AIF") and their managers may, however, invest in cryptocurrencies.

There are currently no specific licensing requirements imposed on an investment advisor or fund manager holding cryptocurrency, over and above those set out under the general trade law/financial services licensing framework.

Mining

Mining bitcoin and other cryptocurrencies as such is not yet regulated and thus currently permitted. However, raising capital from the public in order to invest proceeds into mining of cryptocurrencies may be regulated (see "Cryptocurrency regulation" and "Sales regulation", above)

Border restrictions and declaration

There are currently no border restrictions or obligations to declare cryptocurrency holdings.

Reporting requirements

There are currently no reporting requirements for cryptocurrency payments made in excess of a certain value under Austrian law.

Estate planning and testamentary succession

There are no specific rules as to how cryptocurrencies are treated for the purposes of estate planning and testamentary succession. Accordingly, general civil law rules apply. Cryptocurrencies qualify as (intangible) assets (*unkörperliche Sache*) for civil law purposes and as such can be included in estate planning/testamentary succession, or form part of a deceased person's estate.

Ursula Rath
Tel: +43 1 534 37 50412 / Email: u.rath@schoenherr.eu

Ursula Rath is a partner at Schoenherr in its Vienna office, where she specialises in financial services regulation, capital markets, financings and M&A transactions involving the financial services sector. For over a decade, she has advised issuers, selling shareholders, financial institutions and investors on a wide range of equity and debt capital markets transactions, disclosure requirements, inbound and outbound financial services, conduct of business requirements and compliance. She covers the full range of asset management and investment fund work and has advised clients on regulatory changes, such as under PSD II or MiFID II or on Brexit contingency planning. Ursula is a member of the Fintech Board of the Austrian Ministry of Finance, where she consults on priority actions around start-up financing, ICOs and digital assets and is a founding member of blockchain think tank "thinkBLOCK tank", a Luxembourg-based non-profit organisation, bringing together some of the most respected blockchain and distributed ledger experts from currently more than 15 countries (http://thinkblocktank.org/). She regularly publishes on financial services regulation, capital markets and funds.

Thomas Kulnigg
Tel: +43 1 534 37 50757 / Email: t.kulnigg@schoenherr.eu

Thomas Kulnigg is a partner at Schoenherr, where he specialises in M&A venture capital transactions and start-ups, with an industry focus on technology & digitalisation. Thomas also leads Schoenherr's technology & digitalisation industry-group (see: https://www.schoenherr.eu/technology-digitalisation/) and heads the firm's venture capital and start-up practice.
He is a founding member of the think tank "thinkBLOCK tank", a Luxembourg-based non-profit organisation, bringing together some of the most respected blockchain and distributed ledger experts from currently more than 15 countries (http://thinkblocktank.org/) and a member of the advisory board of the Digital Asset Association Austria (https://daaa.at/).

Schoenherr Attorneys at Law

Schottenring 19, 1010 Vienna, Austria
Tel: +43 1 534 37 – 0 / Fax: +43 1 534 37 – 66100 / URL: www.schoenherr.eu

Bermuda

Mary V. Ward & Adam Bathgate
Carey Olsen Bermuda Limited

Government attitude and definition

The current Bermuda government was elected in 2017 having undertaken to create new economic pillars in Bermuda, identify new opportunities for economic diversification, and seek local and overseas investment to develop new local industry and thereby create jobs in Bermuda. Since its election, it has enthusiastically embraced the financial technology ("**fintech**") sector and the potential it offers, and has repeatedly expressed its intention for Bermuda to be a significant centre for this industry.

In furtherance of this goal, the government has implemented a comprehensive regulatory regime aimed at providing legal certainty to industry participants and ensuring that business in the sector conducted in or from Bermuda is done in a properly regulated matter, in accordance with the highest international standards. This regulatory regime is described in more detail below, but, in summary:

- the Digital Asset Business Act comprises a regulatory framework for fintech businesses operating in or from Bermuda; and
- although not covered by the Digital Asset Business Act, initial coin and security token offerings are regulated under a separate regime.

The government has also announced that fintech businesses wishing to set up in Bermuda are to benefit from a relaxed work permit policy, offers through the Bermuda Business Development Agency a concierge service for businesses wishing to establish operations on the island, and has signed a number of memoranda of understanding with fintech businesses, under which these businesses have committed to establishing operations and creating jobs in Bermuda.

Although digital asset offerings and businesses are regulated in the manner described in this article, there is no legislation or other provision of Bermuda law affording official or legal recognition of any cryptocurrency or any other digital asset, or conferring equivalent status with any fiat currency. Nor has the government or the Bermuda Monetary Authority (the "**BMA**"), the jurisdiction's financial regulator and issuer of its national currency, backed any cryptocurrency itself, and the Bermuda dollar remains the territory's legal tender.

Cryptocurrency regulation

While both the Bermuda government and the BMA are on record as being keen to embrace the potential offered by fintech, both recognise that the industry presents tremendous risk, requiring prudent regulation. Bermuda has, accordingly, led the way in introducing a regulatory framework for digital asset business and coin and token offerings.

Digital Asset Business Act

The Digital Asset Business Act (the "**DABA**") came into force in September 2018. Since the DABA's enactment, the BMA has promulgated rules, regulations, codes of practice, statements of principles and guidance in order to supplement the DABA, with the result that the DABA operates in a similar manner to the regulatory frameworks in place for other financial services regulated by the BMA.

In summary, the DABA specifies the digital asset-related activities to which it applies, imposes a licensing requirement on any person carrying on any of those activities, lays out the criteria a person must meet before it can obtain a licence, imposes (and permits the BMA to impose) certain continuing obligations on any holder of a licence, and grants to the BMA supervisory and enforcement powers over regulated digital asset businesses.

At the time of writing, the BMA was engaged in a consultation exercise with a view to amending certain provisions of the DABA to give greater clarity to certain sections and to make other changes that are intended to facilitate more effective administration of its provisions.

Scope of the DABA

The DABA applies to any entity incorporated or formed in Bermuda and carrying on digital asset business (irrespective of the location from which the activity is carried out) and to any entity incorporated or formed outside of Bermuda and carrying on digital asset business in or from within Bermuda. The term "digital asset" in the legislation is defined widely enough to capture cryptocurrencies, representations of debt or equity in the promoter, representations of other rights associated with such assets, and other representations of value that are intended to provide access to an application or service or product by means of distributed ledger technology. "Digital asset business", for the purposes of the DABA, is the provision of the following activities to the general public as a business:

(a) *Issuing, selling or redeeming virtual coins, tokens or any other form of digital asset*

This is intended to regulate any business providing these services to other businesses or to individuals. It does **not** include initial coin offerings or security token offerings (collectively, "**ICOs**") to fund the issuer's or promoter's own business or project. Instead, ICOs are regulated under a separate regime, on which see below.

(b) *Operating as a payment service provider business utilising digital assets, which includes the provision of services for the transfer of funds*

The term "payment service provider" is used globally in anti-money laundering and anti-terrorist financing ("**AML/ATF**") laws, regulations and guidance, and is defined in Bermuda's Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Amendment Regulations 2010 as "a person whose business includes the provision of services for the transfer of funds". The aim here is to ensure that businesses involved in the transfer of digital assets fall within the DABA's ambit.

(c) *Operating as an electronic exchange*

This category captures online exchanges allowing customers to buy and sell digital assets, whether payments are made in fiat currency, bank credit or in another form of digital asset. Exchanges facilitating the offer of new coins or tokens through ICOs are also caught.

(d) *Providing custodial wallet services*

This covers any business whose services include storing or maintaining digital assets or a virtual wallet on behalf of a client.

(e) *Operating as a digital asset services vendor*

This category regulates a person that, under an agreement as part of its business, can undertake a digital asset transaction on behalf of another person or has power of attorney over another person's digital asset, or a person who operates as a market-maker for digital assets. It is intended to capture any other business providing specific digital asset-related services to the public, such as operating as a custodian of digital assets.

In addition to the above categories, the DABA includes an option for the Minister of Finance, after consultation with the BMA, to be able to add new categories or to amend, suspend or delete any of the categories listed above by order.

The DABA specifically provides that the following activities shall not constitute digital asset business:

- contributing connectivity software or computing power to a decentralised digital asset, or to a protocol governing transfer of the digital representation of value (this category exempts mining from the DABA's scope);
- providing data storage or security services for a digital asset business, so long as the enterprise is not otherwise engaged in digital asset business activity on behalf of other persons; and
- the provision of any digital asset business activity by an undertaking solely for the purpose of its business operations or the business operations of any of its subsidiaries.

Licensing requirement

The DABA requires persons carrying on digital asset business to obtain a licence before doing so, unless that person is subject to an exemption order issued by the Minister of Finance. At the time of writing, the Minister had not issued or proposed any exemption orders.

Two classes of licence are available for applicants:

- The **Class M licence** is a restricted form of "sandbox" licence, with modified requirements and certain restrictions, and valid for a specified period, the duration of which will be determined by the BMA on a case-by-case basis. Following the expiry of this specified period, it is generally expected that the licensee will either have to apply for a Class F Licence (as described in further detail below) or cease carrying on business, although the BMA will have discretion to extend the specified period.
- The **Class F licence** is a full licence not subject to any specified period, although it may still be subject to restrictions the BMA may deem appropriate in any given case.

The intention behind this tiered licensing regime is to allow start-ups engaging in digital asset business to do so in a properly supervised regulatory environment, and to engage in proof of concept and develop some sort of track record before obtaining a full licence. The restrictions to which a licensee will be subject will depend on the business model of the prospective licensee (and the risks associated with it), but will almost invariably include an obligation to disclose to prospective customers the fact that the licensee holds a Class M licence and certain limitations on the volume of business the licensee is permitted to conduct, along with other restrictions as the BMA may deem necessary or appropriate on a case-by-case basis.

A prospective licensee may not necessarily receive the licence for which it applies: an applicant for a Class F licence may receive a Class M licence if the BMA decides that a Class M licence would be more appropriate in the circumstances. A licence will further

specify the category (or categories) of digital asset business in which the licensee is permitted to engage.

Carrying on digital asset business without a licence is a criminal offence punishable by a fine of up to US$250,000, imprisonment for a term of up to five years, or both.

Criteria to be met by licensees

The DABA provides that the BMA may not issue any licence unless it is satisfied that the applicant fulfils certain minimum criteria addressing the fitness and propriety of directors and officers, ensuring business is conducted in a prudent manner, the integrity and skill of the business's management, and standards of corporate governance observed by the (prospective) licensee. This is consistent with the position under other regulatory laws applicable to other sectors and is intended to ensure the BMA maintains high standards for the conduct of regulated business. The BMA has also published a code of practice detailing requirements as to, *inter alia*, governance, risk management and internal controls applicable to licensees. The BMA recognises, however, that licensees have varying risk profiles arising from the nature, scale and complexity of the business, so assesses a licensee's compliance with this code in a proportionate manner relative to the business's nature, scale and complexity.

The DABA requires licensees to notify the BMA upon changes in directors or officers, and the BMA has powers to, *inter alia*, object to and prevent new or increased ownership of shareholder controllers and the power to remove controllers, directors and officers who are no longer fit and proper to carry on their role.

Continuing obligations of licence holders

Persons holding a licence issued under the DABA are subject to several ongoing obligations.

Client disclosure rules: the BMA has used powers conferred to it under the DABA to promulgate the Digital Asset Business (Client Disclosure) Rules 2018 in order to mitigate the high degree of risk for consumers owing to the highly speculative and volatile nature of digital assets. These rules require licensees, before entering into any business relationship with a customer, to disclose to that customer: the class of licence it holds; a schedule of its fees and the manner in which fees will be calculated if not set in advance; whether it has insurance against loss of customer assets arising from theft (including cybertheft); the extent to which a transfer or exchange of digital assets is irrevocable and any exceptions; governance or voting rights regarding client assets if the licensee is to hold client assets; the extent to which it will be liable for an unauthorised, mistaken or accidental transfer or exchange; and sundry other matters. The rules also oblige licensees to confirm certain information regarding transactions with clients at the conclusion of each such transaction.

Cybersecurity Rules: alongside the client disclosure rules described above, the BMA has promulgated the Digital Asset Business (Cybersecurity) Rules 2018 (the "**Cybersecurity Rules**"). Under the Cybersecurity Rules, licensees must file an annual cybersecurity report prepared by its chief information security officer assessing the availability, functionality and integrity of its electronic systems, any identified cyber-risk arising from any digital asset business carried on or to be carried on by the licensee, and the cybersecurity programme implemented and proposals for steps for the redress of any inadequacies identified.

The cybersecurity programme itself must include (but is not limited to) the following audit functions:

- penetration testing of its electronic systems and vulnerability assessment of those systems conducted at least on a quarterly basis; and

- audit trail systems that:
  - track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting;
  - protect the integrity of data stored and maintained as a part of the audit trail from alteration or tampering;
  - protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction;
  - log system events including but not limited to access and alterations made to the audit trail systems, and cybersecurity events; and
  - maintain records produced as part of the audit trail.

Licensees must engage a qualified independent party to audit its systems and provide a written opinion to the BMA that the cybersecurity programme and controls are suitably designed and operative effectively to meet the requirements of the Cybersecurity Rules and applicable codes of practice.

Custody and protection of consumer assets: licensees holding client assets are required to have in place and maintain a surety bond, trust account or indemnity insurance for the benefit of their customers. Any such trust account must be maintained with a "qualified custodian", which the DABA defines as a licensed Bermuda bank or trust company or any other person recognised by the BMA for this purpose. A licensee is, in addition, required to maintain books of account and other records sufficient to ensure that customer assets are kept segregated from those of the licensee and can be identified at any time. All customer funds must be held in a dedicated separate account and clearly identified as such.

Senior representative: the DABA imposes an obligation on licensees to appoint a senior representative, to be approved by the BMA, who must be resident in Bermuda and who is sufficiently knowledgeable about both the licensee itself and the industry in general. This senior representative will himself be under a duty to report to the BMA certain significant matters, including: a likelihood of the licensee becoming insolvent; breaches by the licensee of any conditions imposed by the BMA; involvement of the licensee in criminal proceedings, whether in Bermuda or elsewhere; and other material developments.

Head office: the DABA also requires licensees to maintain a head office in Bermuda and to direct and manage their digital asset business from Bermuda. The relevant section goes on to list a number of factors the BMA shall consider in determining whether a licensee satisfies this requirement, together with a number of additional factors to which the BMA may (but need not) have regard.

Annual prudential return: a licensee is obliged to file with the BMA an annual prudential return, with the BMA being granted the power to require more frequent filings or additions to a filing if required in the interest of consumer protection. The annual prudential return should be accompanied by a copy of the licensee's audited financial statements and business plan for the following year, and include information relating to, *inter alia*, business strategy and risk appetite, products and services, the number, risk rating and geographical profile of customer accounts, information on risk and cybersecurity (including a risk self-assessment and policies in these areas), AML/ATF controls, corporate governance, audited financial statements and details on any outsourcing to third parties.

BMA's supervision and enforcement powers

The DABA grants the BMA wide-ranging powers of supervision and enforcement.

It will have the power to compel production of information and documents (with criminal sanctions for non-production or for making false or misleading statements), the power to issue such directions as appear to be desirable to it for safeguarding the interests of a licensee's clients where a licensee is in breach of the DABA or regulations or rules applicable to it, and the power to impose conditions and restrictions on licences. For example, the BMA may:

- require a licensee to take certain steps or to refrain from adopting or pursuing a particular course of action, or to restrict the scope of its business activities in a particular way;
- impose limitations on the acceptance of business;
- prohibit a licensee from soliciting business, either generally or from prospective clients;
- prohibit a licensee from entering into any other transactions or class of transactions;
- require the removal of any officer or controller; and/or
- specify requirements to be fulfilled otherwise than by action taken by the licensee.

In more extreme cases, the BMA may revoke a licence altogether and, if it so elects, subsequently petition the court for the entity whose licence it has revoked to be wound up.

In the event a licensee fails to comply with a condition, restriction or direction imposed by the BMA or with certain requirements of the DABA, the BMA has the power to impose fines of up to US$10,000,000. Alternatively, it may issue a public censure ("naming and shaming"), issue a prohibition order banning a person from performing certain functions for a Bermuda regulated entity, or obtain an injunction from the court. The BMA will use these enforcement powers in a manner consistent with the Statement of Principles and Guidance on the Exercise of Enforcement Powers it published in September 2018, which contains general guidance applicable to all regulated sectors on the BMA's approach to the use of its enforcement powers and the factors it will consider in assessing whether to exercise those powers.

ICO regulation

As noted above, the DABA does not apply to any ICO intended to finance the issuer's or promoter's own business. Instead, the Companies Act 1981 and the Limited Liability Company Act 2016 (collectively, the "**Company Legislation**") were amended in 2018 to include a regulatory framework for ICOs.

The Company Legislation defines an ICO as an offer by a company or a limited liability company (a "**LLC**") to the public to purchase or otherwise acquire digital assets and designates any ICO as a "restricted business activity", requiring consent from the Minister of Finance before any ICO may be made to the public. Private sales and offers of further coins or tokens to existing holders of coins or tokens of the same class are exempted, as are issuances where the offer is made to a limited number of persons (the actual limit depends on the type of company or LLC the issuer is, and is 35 in most cases). Regulations published under the Company Legislation set out key information required to be included with the application for consent, including details as to the proposed project to be funded by the ICO and the persons involved as well as information on the coin or token proposed to be offered and its transferability, and information on compliance features intended to be included in the issuer's systems.

In addition to obtaining consent from the Minister of Finance, a prospective ICO issuer will also have to publish, in electronic form, an offering document and file this with the Bermuda Registrar of Companies. The offering document must contain:

- details regarding any promoter, including its registered or principal office and details of its officers;
- the business or proposed business of the issuer company or LLC;
- a description of the project to be funded by the ICO and the proposed timeline for the project, including any proposed project phases and milestones;
- the amount of money that the ICO is intended to raise;
- disclosure as to the allocation of the amounts intended to be raised amongst the classes of any issuance (pre-sale, post-ICO, etc.);
- any rights or restrictions on the digital assets that are being offered;
- the date and time of the opening and closing of the ICO offer period;
- a statement as to how personal information will be used; and
- a general ICO risk warning containing:
    - information regarding any substantial risks to the project which are known or reasonably foreseeable;
    - information as to a person's rights or options if the project which is the subject of the ICO in question does not go forward;
    - a description of the rights (if any) in relation to the digital assets that are being offered; and
    - information regarding any disclaimer in respect of guarantees or warranties in relation to the project to be developed or any other asset related to the ICO.

If an ICO issuer offers digital assets to the public over a period and any of the particulars in its offering document cease to be accurate in a material respect, the issuer must publish supplementary particulars disclosing the material changes and file these with the Registrar.

The promoter must provide an electronic platform to facilitate communication with prospective investors, and the legislation also grants investors a cooling-off period during which they are permitted to withdraw an application to purchase the digital assets offered.

Any person who makes or authorises the making of a false statement in an ICO offering document is guilty of an offence punishable with a fine of up to US$250,000, imprisonment for a term of up to five years, or both, unless the person proves either that the statement was immaterial or that at the time he made the statement he had reasonable grounds to believe it was true. Officers of the issuer and promoters of the ICO will also incur civil liability to any person who suffers loss as a result of false statements in the offering document, subject to certain defences.

Sales regulation

Issuing, selling or redeeming cryptocurrencies is regulated under the DABA if carried on as a business, and ICOs are regulated under the Company Legislation, in each case in the manner described more particularly above.

Taxation

There are no income, capital gains, withholding or other taxes imposed in Bermuda on digital assets or on any transactions involving them (the potential application of Bermuda's foreign

currency purchase tax is discussed below, under "Border restrictions and declaration"). Moreover, exempted companies or LLCs carrying on digital asset business, including ICO issuers, may apply for, and are likely to receive, an undertaking from the Minister of Finance to the effect that, in the event of there being enacted in Bermuda any legislation imposing tax computed on profits or income or computed on any capital asset, gain or appreciation, then the imposition of any such tax shall not be applicable to such company or to any of its operations.

Money transmission laws and anti-money laundering requirements

Operating a payment service business utilising cryptocurrency or other digital assets (including the provision of services for the transfer of funds) or operating a digital exchange constitutes a regulated activity for the purposes of the DABA (on which see above).

Bermuda has a long-established and well-earned reputation as an international financial centre, and a crucial aspect of this is its robust AML/ATF regime. The jurisdiction made further enhancements to this regime ahead of its fourth round mutual evaluation by the FATF in 2018.

The DABA amended certain provisions of Bermuda's existing AML/ATF laws and regulations in order to ensure that the AML/ATF regime applies expressly to the carrying on of digital asset business, with the BMA subsequently issuing new AML/ATF guidance notes relating specifically to the conduct of digital asset business.

A detailed discussion of the requirements imposed by Bermuda's AML/ATF regime is beyond the scope of this chapter, but in short, digital asset businesses are required to establish policies and procedures to prevent money laundering and terrorist financing. These policies and procedures must cover customer due diligence, ongoing monitoring, reporting of suspicious transactions, record-keeping, internal controls, risk assessment and management, and the monitoring and management of compliance with, and internal communication of, these policies and procedures.

Promotion and testing

As noted at the beginning of this chapter, the Bermuda government is very enthusiastic about the potential offered by fintech for the territory's economy and has launched, or is in the process of developing, a number of initiatives aimed at promoting investment by fintech businesses in Bermuda.

The government has appointed a specialist fintech team with a remit to promote the sector in Bermuda and bring more fintech business to the island. Among its initial success stories is that of Omega One, an agency brokerage for cryptocurrencies, which has opened an office in Bermuda (and received the first licence granted under the DABA), and has committed to hiring at least 20 Bermudians over the next three years, and donating 10% of a planned token sale to philanthropic causes (with 10% of the amount donated going to sports and community clubs in Bermuda).

A further government initiative is a tailored immigration policy for fintech businesses, which allows a company operating in the fintech space and which is new to Bermuda to receive immediate approval of up to five work permits for non-Bermudian staff within the first six months of obtaining its business permit. In order to benefit from this, a business must present a plan for the hiring, training and development of Bermudians in entry-level or trainee positions. A business may not, however, apply for a work permit under this policy in respect

of any job categories which are closed (i.e. reserved exclusively for Bermudians, their spouses and permanent resident certificate holders only) or restricted (in respect of which a permit may only be obtained for one year) under Bermuda's employment legislation, or which are entry-level, graduate or trainee positions.

The government has also entered into a series of memoranda of understandings with various digital asset businesses. Under these memoranda:

- Binance Holdings Limited, the parent company of the Binance Group, the world's largest digital exchange, has committed to develop its global compliance base in Bermuda, creating at least 40 jobs, and to develop a digital asset exchange in Bermuda. It has also undertaken to sponsor university scholarships for Bermudians in blockchain technology development and regulatory compliance, and to make capital available for investment in new Bermuda-based blockchain companies.
- Medici Ventures LLC, a subsidiary of overstock.com (the world's first major enterprise to accept Bitcoin), will create at least 30 jobs in Bermuda over three years, develop a security token trading platform in Bermuda, support the training of Bermudians in software development, and collaborate with the government, the BMA and other stakeholders in developing and improving Bermuda's legal and regulatory framework applicable to digital asset businesses.
- Shyft, a blockchain AML/ATF and identity startup, will invest up to US$10 million over the next three years into Bermuda's economy, support the training of Bermudians in blockchain technology and software development, and collaborate in the development and improvement of Bermuda's digital asset legal and regulatory framework. Shyft has also signed a separate MOU with Trunomi, a Bermuda-based consent and data rights platform, which aims to leverage Shyft's blockchain technology with Trunomi's expertise in consumer consent frameworks to support Bermuda in the implementation of an electronic ID scheme.

Ownership and licensing requirements

Under current Bermuda law, and under the ICO Act and the DABA, no licensing requirements are imposed on any person merely by virtue of that person holding any form of digital asset, unless that person does so in the course of its business and on behalf of another, in which case that person will likely be regarded as a digital asset services vendor and thus subject to regulation under the DABA. The BMA is consulting on proposals to require Bermuda trust companies which hold digital assets as trust property to obtain a licence to do so under the DABA.

An investment fund incorporated or formed in Bermuda which proposes to deal in digital assets as part of its investment strategy or programme may fall within the ambit of the Investment Funds Act 2006. This requires open-ended funds to apply to the BMA for authorisation prior to commencing business, and subjects such funds to the ongoing supervision of the BMA. It does not apply to closed-ended funds, such as private equity funds.

Mining

Mining is specifically exempted from the scope of the DABA. It therefore remains an unregulated activity.

Although mining is not prohibited by any Bermuda law of which we are aware and is not subject to regulation under the DABA, Bermuda's high energy costs will, it is anticipated, operate as a practical deterrent to the establishment of any mining operations in Bermuda.

Border restrictions and declaration

Bermuda imposes a foreign currency purchase tax of 1% whenever a Bermuda resident purchases a foreign currency from a Bermuda-based bank. This tax will not apply to most (if not all) purchases of cryptocurrency or other digital assets, on the grounds that these are purchased almost exclusively from digital exchanges, whereas the foreign currency purchase tax applies only to purchases from banks in Bermuda. This renders immaterial the question of whether "foreign currency" in this context would include a cryptocurrency (the BMA has not, to date, expressed a view).

There are no other border restrictions on cryptocurrencies or other digital assets; the only obligation to make a customs declaration in respect of any form of money arises in respect of cash or negotiable instruments in excess of US$10,000.

Reporting requirements

Digital asset businesses and their senior representatives are subject to certain reporting obligations under the DABA, as described in more detail above. The DABA does not impose any reporting requirements in respect of individual digital asset payments, irrespective of their value, although licensees are required to include anonymised details on transaction volume, value and geographical spread in their annual returns.

Estate planning and testamentary succession

There is no particular regime of Bermuda law which deals specifically with the treatment of cryptocurrencies or other digital assets upon the death of an individual holding them. This means that, in principle, digital assets will be treated in the same way as any other asset and may be bequeathed to beneficiaries in a will, or, if a person dies intestate, will fall to be dealt with under the Succession Act 1974.

The main potential difficulty that may arise is practical and is by no means unique to Bermuda; namely that anyone inheriting any kind of digital asset will, on the face of it, only be able to access that digital asset if the beneficiary has, or can obtain or access, the private key to the wallet in which it is stored. Most exchanges have policies in place to transfer digital assets to next of kin but these policies, and the transfer requirements, will vary between the exchanges.

Mary V. Ward
Tel: +1 441 542 4507 / Email: mary.ward@careyolsen.com

Mary V. Ward advises on all aspects of commercial and corporate law, with extensive experience in securities law, mergers and acquisitions, restructuring of private and public companies and private equity. She has also advised on insurance matters, including incorporation and ongoing regulatory requirements of commercial insurers, equity and debt financings of insurers and insurance groups including private placements, listed debt offerings and IPOs.

Mary is recognised as an expert in her field by both *Chambers* and *The Legal 500* with market sources recognising her considerable experience in securities and insurance work.

Mary is rated as a Leading Lawyer – Highly regarded in *IFLR1000*.

Adam Bathgate
Tel: +1 441 542 4500 / Email: adam.bathgate@careyolsen.com

Adam is counsel in the Bermuda office and advises on all aspects of Bermuda corporate law. His particular specialisms lie in debt finance transactions, the formation and maintenance of investment funds, and the fintech sector.

Adam has considerable expertise in the areas of fund finance, leveraged and acquisition finance and general lending, whether secured or unsecured. He has also worked on asset finance and structured finance transactions.

In the funds sphere, Adam's practice is largely focused on the formation and maintenance of private equity, infrastructure and real estate funds, including related downstream deal work, although he also has experience in hedge funds and hybrid funds.

Adam is ranked as a "rising star" in *IFLR1000*.

Carey Olsen Bermuda Limited

Atlantic House, 11 Par-la-Ville Road, Hamilton HM 11, Bermuda
Tel: +1 441 542 4500 / URL: www.careyolsen.com

Brazil

Martim Machado & Julia Fontes Abramof
CGM Advogados

Government attitude and definition

Brazilian authorities do not consider cryptocurrencies as legal tender nor do they afford them the same status as fiat currencies of other countries. They also do not specifically regulate the creation, use, trading or circulation of cryptocurrencies. The "Real" is the only legal tender recognised and accepted in Brazil. However, Brazilian authorities have not ignored cryptocurrencies.

The Brazilian Central Bank, through statements issued in 2014 and 2017, commented on the risks associated with the use of cryptocurrencies, pointing out, among other things, that cryptocurrencies were not issued nor backed by the Brazilian government, were not pegged to any fiat currency or asset nor had their conversion into "Real" or other fiat currencies guaranteed by the Brazilian government.

The Brazilian security and exchange commission – Comissão de Valores Mobiliários (CVM) – in several opinions issued during 2017 and 2018, expressed concerns about initial coin offerings (ICOs). According to CVM, ICOs could be subject to prior registration with CVM (as the securities offerings generally are) as many cryptocurrencies have features that could result in their characterisation as securities. In addition, in 2018, CVM banned the direct acquisition of cryptocurrencies by Brazilian investment funds. It is important to point out that CVM did not rule out investments in cryptocurrencies because it believes that cryptocurrencies are unlawful. CVM only prohibited direct acquisitions of cryptocurrencies by Brazilian investment funds because it understood that cryptocurrencies were not included in the classes of assets in which funds are allowed to invest under current regulations (funds are only allowed to invest in "financial assets" and CVM believes that cryptocurrencies do not meet the definition of financial assets under current regulations). However, Brazilian investment funds are still able to make indirect investments in cryptocurrencies (via cryptocurrency-based derivatives or third party vehicles directly investing in cryptocurrencies or their derivatives and which are incorporated in jurisdictions where they are allowed to hold cryptocurrencies or their derivatives).

Since 2016, the Brazilian federal tax authorities have required taxpayers to declare cryptocurrencies in their annual tax returns, as well as to pay income tax on capital gains derived from the use or disposition of cryptocurrencies. Furthermore, in May 2019, federal tax authorities created reporting obligations applicable to Brazilian-based exchanges, as well as on Brazilian legal entities and individuals holding cryptocurrencies. These reporting obligations are discussed in greater detail under "Reporting requirements" below.

Despite these statements, opinions and regulations, nothing currently prevents legal entities and individuals in Brazil from creating cryptocurrencies or from using them to purchase

goods or services. Cryptocurrencies can be exchanged for goods or services in Brazil if the parties involved in the transaction so agree.

Cryptocurrency regulation

The creation, use and trading of cryptocurrencies are not specifically regulated in Brazil. However, there are two bills of law currently under discussion in the House of Representatives that could change that landscape.

The first bill of law (PL 2,303, dated July 7, 2015) originally intended to include cryptocurrencies in the definition of "payment schemes". The Brazilian Central Bank defines "payment schemes" as the set of rules and procedures that govern the provision of certain payment services to the public, such as credit and debit cards. The inclusion of cryptocurrencies in the definition of payment schemes would make it subject to the regulation and oversight of the Central Bank. A Special Commission in the House of Representatives was appointed to analyse the bill and, during discussions, such bill underwent substantial changes. At one point, the proposed changes ended up subverting the original bill and banned the issuance, circulation, and even the use or acceptance of cryptocurrencies as means of payment. Subsequently, new changes were proposed not only to generally allow cryptocurrencies to be issued and used, but also to prohibit regulatory bodies from creating rules that could ban or hinder the issuance, circulation and use of cryptocurrencies, or the activities of exchanges.

The second and more recent bill of law (PL 2,060, dated April 4, 2019) aims at defining cryptocurrencies, clarifying that they are not securities, and allowing cryptocurrencies to be freely issued, transferred and used.

Because both bills of law are somewhat overlapping, it is likely that they will be jointly vetted by the House of Representatives. However, both bills of law are still in their initial phases of discussion and no assurance can be given that they will be eventually approved by Congress and passed into law. Furthermore, the bills may be substantially amended during their review process.

Sales regulation

There are no specific laws or regulations concerning the sale of cryptocurrencies in Brazil. However, cryptocurrencies, depending on their characteristics, could be classified as securities under Brazilian law. If that happens, the public offering of cryptocurrencies may be subject to prior registration with CVM, the Brazilian security and exchange commission. In this regard, CVM has already expressed concerns about initial coin offerings (ICOs). Although CVM has not specifically regulated ICOs, it has understood that such offers may be subject to the rules currently applicable to traditional securities offerings.

In CVM's opinion, many cryptocurrencies offered through ICOs could be "securities" or, more specifically, "collective investment agreements", which are securities that generate participation, partnership or renumeration rights (including those resulting from the rendering of services) whose income originates from the efforts of an entrepreneur or a third party. The characterisation of a cryptocurrency as a security means that its public offering to investors in Brazil, even by means of the Internet or from abroad, must be preceded by registration with CVM (except when registration exemptions apply). In addition, such characterisation also requires that the distribution of cryptocurrencies be carried out by entities duly authorised to operate by CVM.

Taxation

Federal tax authorities understand that cryptocurrencies are financial assets and should be taxed accordingly. In this regard, cryptocurrencies must be declared in income tax returns as "other assets". Furthermore, individuals are obliged to pay income tax on any capital gains obtained with the disposition of cryptocurrencies, provided that the total value of cryptocurrencies disposed of during any given month exceeds BRL 35,000.00. Tax rates vary from 15% to 22.5%.

Money transmission laws and anti-money laundering requirements

Brazilian anti-money laundering laws and regulations establish a series of obligations applicable to individuals or legal entities that operate in various markets, such as real estate, luxury or high value goods, financial services, broker-dealers, and credit card companies. Such persons are required to keep detailed records of their operations and to report suspicious transactions and other transactions that meet certain pre-defined criteria to the Financial Activities Control Council (COAF), a federal government agency in charge of enforcing anti-money laundering laws and regulations.

Even though Brazilian authorities have already expressed concerns about the use of cryptocurrencies for money laundering purposes, they have not yet amended existing regulations nor enacted new regulations to deal specifically with cryptocurrencies. Nonetheless, in spite of the non-existence of anti-money laundering laws and regulations dealing particularly with cryptocurrencies, existing anti-money laundering laws will apply to transactions involving the use of cryptocurrencies whenever they have been entered into for money laundering purposes.

Furthermore, reporting obligations recently created by federal tax authorities (discussed in greater detail under "Cryptocurrency regulation" above) will enable Brazilian authorities to have access to information that may allow them to identify suspicious transactions from a money laundering perspective.

There are no specific laws or regulations concerning money transmission laws in Brazil applicable to cryptocurrencies.

Promotion and testing

No government-sponsored promotion and testing programmes regarding cryptocurrencies are currently in place in Brazil. However, the Brazilian Central Bank has been studying the use of distributed ledger technology in the financial system by analysing potential use cases and developing working prototypes.

In addition, in May 2019, the Central Bank launched an initiative called the "Financial and Technological Innovation Lab (Lift)", which provides incentives to projects that may bring technological innovations to the finance arena. Out of 12 projects selected by the Central Bank, one third relies on blockchain technology.

Ownership and licensing requirements

The only restriction on the ownership of cryptocurrencies is set by Circular Notice No. 1/2018/CVM/SIN, issued by CVM, the Brazilian securities and exchange commission. The aforementioned Circular Notice bans the direct acquisition of cryptocurrencies by Brazilian investment funds as, according to CVM, cryptocurrencies are not qualified as financial assets under current regulations. There is no restriction on the ownership of cryptocurrencies by any other persons or entities.

Legal entities, including exchanges, and individuals are not subject to any licensing requirements in Brazil in order to issue, own or transact with cryptocurrencies. However, as explained under "Sales regulation" above, if any person offers cryptocurrencies that are classified as securities under Brazilian law, such person may have to obtain a proper licence from CVM to act as a securities broker/dealer.

Mining

The mining of cryptocurrencies is not prohibited in Brazil and has not been the subject-matter of any specific statement, warning, opinion or regulation by any Brazilian authority.

Border restrictions and declaration

There are no border restrictions or declarations specifically applicable to cryptocurrencies in Brazil. However, Brazil does have foreign currency exchange controls in place, which require conversions of Brazilian currency – the Real – into other currencies, and *vice versa*, to be carried out with the involvement of authorised financial institutions (including traditional banks) and reported to or registered with the Brazilian Central Bank, as the case may be. In certain cases (such as capital contributions made by foreign investors into Brazilian legal entities and foreign loans granted by foreign lenders to Brazilian legal entities or individuals), prior registration with the Central Bank is required.

These foreign currency exchange controls require international transfers of funds in connection with a wide variety of transactions to be carried out only as specified in Central Bank regulations, which normally require such transfers regarding foreign currency exchange contracts to be with authorised financial institutions and the presentation to such financial institutions of supporting documentation regarding the transfers to be made, including information on the nature/purpose of the transfers, and on the beneficiaries.

Even though there are no laws or regulations expressly addressing the use of cryptocurrencies to effect international transfers of funds to or from Brazil and despite the fact that one could find a reasonable legal basis to support the use of cryptocurrencies for that purpose, the Brazilian Central Bank has already stated (in a brief statement that has not discussed the issue in depth) that it sees the use of cryptocurrencies to effect international transfers of funds as not permissible since such use would circumvent existing foreign currency controls.

Reporting requirements

Since 2016, federal tax authorities have required taxpayers to report their cryptocurrencies in their income tax returns as "other assets", regardless of the number of cryptocurrencies owned and their respective value.

In May 2019, federal tax authorities enacted Normative Instruction No. 1,888/19, which created specific reporting obligations for Brazilian-based exchanges, as well as for Brazilian legal entities and individuals transacting with cryptocurrencies through exchanges located outside Brazil or transacting with cryptocurrencies without using any exchange.

Brazilian-based exchanges are legal entities organised under Brazilian law that offer services related to cryptocurrency transactions, such as brokerage, trading or custodial account services, and that are authorised to accept any means of payment, including other cryptocurrencies, as consideration for their services. Reportable transactions include purchases, sales, donations, issuances and any other transfers of cryptocurrencies (including transfers to and from exchanges). The regulations broadly define cryptocurrencies to include

any digital representation of value that does not qualify as legal tender, is electronically transacted with the use of cryptography and distributed ledger technologies, and is used as an investment (store of value) or an instrument to transfer value or to access services.

The specific reporting obligations set forth in Normative Instruction No. 1,888/19 consist of the following:

- Legal entities and individuals must report, on a monthly basis, data concerning any transactions carried out by them whenever the monthly value of such transactions exceed BRL 30,000.00 (in a single transaction or in a series of transactions).
- Exchanges, on the other hand, must report, also on a monthly basis, all transactions carried out in their platforms in the relevant month, regardless of their amount.

In each case, reportable information includes the dates and types of transaction (purchase, sale, donation, etc.), name of exchanges involved (when the information is not being reported by an exchange), names of the parties, types and characteristics of the cryptocurrencies transacted, transactions amount, and wallet addresses (if any). Parties must be identified by their full names, addresses, tax residency information and taxpayer identification numbers.

In addition to these monthly reporting obligations, Normative Instruction No. 1,888/19 requires exchanges to provide to federal tax authorities annually the following information about their clients: (a) total amount, in Brazilian Reals, of the cryptocurrencies held; (b) the quantity of each cryptocurrency held; and (c) the cost, in Brazilian Reals, of each cryptocurrency held (when that information is reported to the exchange by the relevant client).

Failure to timely comply with these reporting obligations will subject exchanges, entities or individuals, as the case may be, to fines of between BRL 100.00 and BRL 1,500.00 per month of delay. The submission of incomplete, inaccurate or incorrect information will carry fines ranging between 1.5% and 3% of the respective transaction amount.

Estate planning and testamentary succession

There are no special estate and succession rules applicable to cryptocurrencies in Brazil. As long as the private keys that ensure control of the cryptocurrencies remain accessible after death, cryptocurrencies, like any other assets, will become part of the estate and will have the destination provided under general estate and succession laws.

Martim Machado
Tel: +55 11 2394 8960 / Email: martim.machado@cgmlaw.com.br
Martim Machado is a lawyer with over 25 years of experience representing international companies and their Brazilian subsidiaries in connection with a variety of legal matters in Brazil. He specialises in corporate law, commercial contracts, foreign direct investments and M&A. Martim is a graduate (LL.B.) from the Catholic University of São Paulo Law School – PUC/SP (1994) and holds a Master of Laws degree (LL.M.) from Georgetown University Law Center in Washington, D.C. (1998). Prior to founding CGM Advogados, Martim was a partner at major Brazilian law firms, an attorney with the Inter American Development Bank – IDB in Washington, D.C., and a foreign associate at Mayer, Brown & Platt (currently, Mayer Brown) in New York, NY.

Julia Fontes Abramof
Tel: +55 11 2394 8965 / Email: julia.abramof@cgmlaw.com.br
Julia Fontes Abramof is an associate specialising in corporate law, commercial contracts, foreign direct investments and M&A. Julia is a graduate (LL.B.) from the Catholic University of Rio de Janeiro Law School – PUC/RJ (2014) and attended a postgraduate course in Business Management, Export/Import, and International Marketing at the University of California in Los Angeles – UCLA.

CGM Advogados

Avenida Brigadeiro Faria Lima, 1,663, 5th floor, São Paulo, 01452-001, SP, Brazil
Tel: +55 11 2394 8900 / URL: www.cgmlaw.com.br

British Virgin Islands

Clinton Hempel & Mark Harbison
Carey Olsen

Government attitude and definition

The British Virgin Islands ("**BVI**") regulator, the Financial Services Commission ("**FSC**"), recognises Bitcoin- and Ether-focused funds. This has resulted in leading Fintech companies such as Bitfinex, Finamatrix and Football Coin being incorporated in the BVI. The primary focus of the service providers in the jurisdiction relates to initial coin offerings ("**ICOs**") and initial token offerings ("**ITOs**"). The challenge for the BVI, along with all other jurisdictions, is how to regulate the fundraising for such offerings. Most ICOs and ITOs established in the BVI use the structure of a business company incorporated under the BVI Business Companies Act 2004 (the "**BCA**"). This provides corporate flexibility, relative free-flow of funds, and low comparative establishment costs associated with a BVI company.

At the present time neither the FSC nor the BVI Government have given any form of regulatory advice or guidance in respect of ICOs or ITOs, nor have they issued any guidance for cryptocurrencies, blockchain or financial technology more generally. The BVI Government has indicated its intention to establish a legal framework that is supportive of the cryptocurrency and financial technology sectors in the BVI, but no draft legislation or consultations have been announced. In the meantime, the consensus view is that the BVI are following a 'wait and see' approach to the development of how ICOs and ITOs will be regulated.

In the meantime, an indication of the BVI government's forward looking and crypto-friendly approach is reflected in the fact that is has entered a partnership with blockchain company LifeLabs. This was an initiative following the devastation of Hurricane Irma, to strengthen their emergency planning through the use of a crypto-wallet. LifeLabs makes a wallet (which supports Ethereum, Bitcoin, and the firm's own crypto tokens). The idea behind the partnership is that in the event of a natural disaster disrupting traditional fiat currency systems, British Virgin Islanders will be able to use LifeLabs wallet to receive government assistance. The BVI Government has also indicated that it will utilise blockchain technology in such an event.

Some ICOs and ITOs have been promoted as an unregulated form of investment, relying on the argument that tokens do not constitute a security for the purposes of the different investor protection laws around the world. As a result, some token issuers have used ICOs and ITOs as a means of avoiding regulation. However, depending on the nature of an investor's rights that attach to a token, it is possible that a token may represent a form of security, particularly if those rights entitle the investor to a share of the profits of the token issuer and the investor is not involved in the day-to-day management and control of the token issuer. Tokens that give investors other rights, such as licences to products and services, could fall outside the

scope of being classed as a security. However, token issuers and investors still need to proceed with caution because it is possible that those types of tokens could be classed as a security, depending on the facts and circumstances of each case and the investor protection laws that apply to the tokens. Further, how the gains on tokens are taxed in different countries may also influence how they are recognised for regulatory purposes.

While the consensus is that ICOs and ITOs will not be subject to securities legislation in the BVI, whether or not the legislation applies will be fact-specific and driven by the nature of the underlying assets of the respective offering. In particular, if a company wishes to: (a) collect and pool investor funds for the purpose of collective investment; and (b) issue fund interests that entitle the holder to receive, on demand or within a specified period after demand, an amount calculated by reference to the value of a proportionate interest in the whole or in a part of the net assets of the company, then it will be deemed open-ended and need to be licensed. There are a number of fund options in the BVI, including public funds, professional funds, private funds, approved funds and incubator funds.

With regard to cryptocurrencies, these are not treated as money in the BVI and do not enjoy equal dignity with domestic or foreign fiat currencies. Pursuant to the Legal Tender (Adoption of the United States Currency) Act 1959 and the Coinage and Legal Tender Act 1973, the US dollar is the legal tender of the BVI. BVI legislation is silent regarding the definition of what is money and currency and the existing regulatory framework does not contemplate cryptocurrencies.

There are no government-backed cryptocurrencies and the BVI's constitutional and currency system means it does not have a central bank.

Cryptocurrency regulation

As discussed above, there is no current regulatory framework for cryptocurrencies in the BVI, similarly there is no express prohibition. The government has indicated a willingness to establish a supportive legal framework but the industry is still in its early stages in the BVI. The regulation of cryptocurrencies, ICOs and ITOs will be determined by how the framework for such transactions fits into the existing regulatory framework in the BVI which, as noted, above was drafted without contemplating cryptocurrencies.

Sales regulation

The Securities and Investment Business Act 2010 ("**SIBA**") regulates, amongst others, the provision of investment services from within the BVI. SIBA provides that any person carrying on, or presenting themselves as carrying on, investment business of any kind in or from within the BVI must do so through an entity regulated and licensed by the FSC (subject to the safe harbours in SIBA). Investment business is widely defined and covers: (i) dealing in investments; (ii) arranging deals in investments; (iii) investment management; (iv) investment advice; (v) custody of investments; (vi) administration of investments; and (vii) operating an investment exchange.

"Investments" is also widely defined and may include: (i) shares, interests in a partnership or fund interests; (ii) debentures; (iii) instruments giving entitlements to shares interests or debentures; (iv) certificates representing investments; (v) options; (vi) futures; (vii) contracts for difference; and (viii) long-term insurance contracts.

Cryptocurrencies in general, and tokens under an ICO or ITO, do not fall immediately within any of the above criteria and therefore do not fall under the SIBA regime. Where they may

fall under the SIBA regime is where the token that is subject to the ICO or ITO is viewed as security or derivative. This will be fact-specific to the relevant ICO or ITO that is being undertaken and would require a level of detailed analysis in each case.

Anti-money laundering

BVI AML legislation must be carefully considered with respect to an ICO or ITO. AML legislation primarily focuses on regulated entities in the BVI and requires certain policies and procedures to be established by "relevant persons" conducting "relevant business". Both the terms "relevant persons" and "relevant business" are strictly defined terms. The requirements seek generally to provide for regulatory rules to minimise and eliminate any form of money laundering or terrorist financing through the BVI. If the company is deemed to carry out "relevant business" (e.g. it is a fund, provides money transmission services, advises on money brokering, etc.) then it has to obtain and maintain client KYC and have internal systems and controls and provide the FSC with a copy of such internal policies for approval.

ICOs of standard utility tokens would not be caught within the definition of "relevant business", and therefore the company is unlikely to be a "relevant person". However, the company and its directors should nevertheless be aware of the BVI AML obligations as a way of future-proofing the business.

Taxation

There are no specific taxes levied against cryptocurrencies in the BVI. The BVI is a tax-neutral jurisdiction and does not have any withholding tax, capital gains taxes, income tax or corporate taxes at the time of writing. In the unlikely event that a BVI entity owns BVI situate land, the entity may be responsible for stamp duties.

Where there is an ICO or ITO, the exchange operators will need to be cognisant of the impact of the Foreign Account Tax Compliance Act ("**FATCA**") and Common Reporting Standards, which will be relevant to determining the ultimate beneficial ownership of the BVI entity issuing the ICO or ITO. While these pieces of legislation will not be immediately relevant at the launch of the ICO or ITO, they will need to be considered as the BVI business company acting as the issuer starts to conduct business more generally.

Money transmission laws and anti-money laundering requirements

The relevant money transmittal law in the BVI is the Financing and Money Services Act, 2009 ("**FMSA**") which regulates money services business. FMSA defines money services as including:

- money transmission services;
- cheque exchange services;
- currency exchange services; and
- the issuance, sale or redemption of money orders or travellers cheques or other such services.

The regime under FMSA is broadly equivalent to the Payment Services Directive. As set out above, the consensus is that for the purposes of BVI legislation, "money" and "currency" refer to fiat currencies rather than cryptocurrencies. It is therefore unlikely that ICO or ITO transactions solely involving cryptocurrency or digital tokens would be viewed as falling

with the definition of money services and the FMSA regime. Where a cryptocurrency transaction is used to facilitate currency exchange services, then this may be viewed as the provision of money services and therefore fall within the remit of FMSA.

Promotion and testing

There are no "sandbox" or other programmes intended to promote research and investment in cryptocurrency in the jurisdiction at present.

Ownership and licensing requirements

As discussed above, there are no specific regulatory requirements in respect of cryptocurrencies; set out below is the framework for the approved financial manager regime under BVI law.

For persons wishing to act as an investment manager or investment advisor in the BVI, regulatory approval from the FSC may be obtained under: (1) SIBA; or (2) the Investment Business (Approved Managers) Regulations, 2012 (the "**Approved Manager Regulations**"). The Approved Manager Regulations were implemented in 2012 with a view to offering a significantly simplified approval process and a lighter regulatory framework than that provided under SIBA.

An Approved Manager's licence authorises you to act as manager or advisor to: (1) BVI incubator funds; (2) BVI approved funds; (3) BVI private funds; (4) BVI professional funds; (5) funds domiciled in certain recognised jurisdictions; and (6) closed-ended funds domiciled in the BVI or in certain recognised jurisdictions, if they have the key characteristics of a private or professional fund. However, an Approved Manager cannot offer services to public funds.

The Approved Manager can be set up as a BVI company or a BVI partnership. The Approved Manager licence is fairly easy to obtain, provided that the directors of the Approved Manager can demonstrate expertise and experience in the area of investment business. The main restriction is that an Approved Manager must not manage assets exceeding US$400m if managing regulated investment funds (such as professional and private funds) or US$1 billion if managing unregulated funds. The Approved Manager licence can also be used for the provision of asset management to individuals. The limit on assets under management for the provision of asset-management services depends on the type of asset management to be provided, but will not be below US$400m.

There are no capital requirements for the Approved Manager and there is no need to appoint a compliance officer. In contrast, a holder of a licence under SIBA will have to submit audited financial statements, appoint a compliance officer, provide employees with compliance training, etc. That said, the advantage of having a licence under SIBA is that there is no limitation on the value of assets under management. For eligible investment managers or investment advisors, the advantage of becoming licensed as an Approved Manager, as opposed to becoming licensed under SIBA, is that the ongoing obligations owed by an Approved Manager are less onerous than those owed by an investment business licensee under SIBA, namely:

An Approved Manager must:

- at all times have at least two directors, one of which must be an individual. However, directors can be resident in any jurisdiction;
- have an authorised representative appointed;
- submit financial statements annually, which need not be audited; and

- submit an annual return which has to contain certain prescribed information such as that the directors continue to be fit and proper, details of the persons to whom the manager provides service, complaints received, etc.

Mining

Mining Bitcoin in the BVI is permitted and there are no current regulations in respect of mining activity.

Border restrictions and declaration

Further to the earlier distinction between cryptocurrency holdings and fiat currency, there are no border restrictions or obligations currently in place in the BVI in respect of cryptocurrencies.

Reporting requirements

There are no reporting requirements or thresholds for payments made by cryptocurrency currently in place in the BVI. The Beneficial Ownership Secure Search System Act 2017 ("**BOSS**") requires BVI companies and their registered agents to record information about the beneficial ownership of a BVI company on a central government-controlled, but confidential, database. Beneficial ownership is determined by reference to control tests, i.e. share ownership, voting rights, the right to remove a majority of the board of directors, and the exercise of significant influence and control over a company.

Estate planning and testamentary succession

Cryptocurrencies have not been widely used for the purposes of estate planning and testamentary succession under BVI law. If, in the unlikely event that the cryptocurrency is regarded as an asset actually situated in the BVI, then a deceased's cryptocurrency could not be validly transmitted to his/her heirs or beneficiaries until an application is made to the BVI High Court Probate Registry (the "**Registry**"). To deal with the deceased's cryptocurrency, a person would need to be appointed as legal personal representative of the deceased, by obtaining the appropriate grant from the BVI Probate Registry. There are two types of grant that may be obtained: (1) Grant of Probate (where the deceased left a will which expressly deals with the BVI cryptocurrency); and (2) Grant of Letters of Administration (where the deceased did not leave a will expressly covering the BVI cryptocurrency). In respect of the latter, the deceased would be deemed to have died "intestate" in relation to the BVI cryptocurrency – even if they had a valid will covering assets in other jurisdictions.

Clinton Hempel
Tel: +27 76 412 6091 / Email: clinton.hempel@careyolsen.com

Clinton is the managing partner of Carey Olsen's British Virgin Islands practice group.

Clinton has practised law for over 20 years and has significant experience in advising financial institutions, public and private businesses, high-net-worth individuals and their onshore advisers on the laws of the British Virgin Islands. He advises on a wide range of corporate and commercial transactions, financings and investment structures, including takeovers, joint ventures, mergers and acquisitions and public and private equity transactions. Clinton also advises on all aspects of BVI regulatory compliance and risk management.

Mark Harbison
Tel: +1 284 394 4034 / Email: mark.harbison@careyolsen.com

Mark is an associate in Carey Olsen's British Virgin Islands office. Mark focuses on a broad range of corporate, commercial and finance transactions. Mark has acted for a wide variety of clients in respect of mergers and acquisitions, cross-border debt finance, corporate restructurings and voluntary liquidations. Mark has also worked on a number of BVI regulatory compliance projects.

Carey Olsen

Rodus Building, PO Box 3093, Road Town, Tortola, British Virgin Islands
Tel: +1 284 394 4030 / Fax: +1 284 494 4155 / URL: www.careyolsen.com

Canada

Simon Grant, Kwang Lim & Matthew Peters
Bennett Jones LLP

Government attitude and definition

The general attitude of the Canadian government (including regulatory agencies) to cryptocurrencies has been a mix of caution and encouragement: caution in terms of protecting investors and the public, but encouragement in its support of new technology. For example, as early as 2015, the Standing Senate Committee on Banking, Trade and Commerce produced a report entitled, "Digital Currency: You Can't Flip This Coin", in which the committee stated:

> *…the Committee strongly believes that a balanced regulatory approach is needed in the digital currency sector. On one hand, the Committee is mindful that the government has the responsibility to protect consumers and root out illegal activity. On the other hand, it is critical that government action does not stifle innovation in digital currencies and its associated technologies that are in an early and delicate stage of development.*
>
> *Having completed the study, the Committee is of the opinion that the opportunities presented by digital currencies, technologies and businesses outweigh the challenges. The Committee is confident that the implementation of our recommendations will have positive outcomes for consumers, merchants, digital currency-related businesses, Canada's financial services sector and others. The Committee looks forward to timely government action designed to maximise the opportunities and manage the challenges facing the digital currency sector.*

This attitude is generally consistent with the position that has been put forward through working papers and speeches from senior members of the Bank of Canada. These have highlighted that the main area for optimism and innovation revolve around the technology that underlies cryptocurrency. According to one paper, it is distributed ledger technology (DLT, or "blockchain") that has the potential to make financial services and other industries more efficient. This technology could bring "important efficiency gains for users in many applications within and outside the financial system by removing redundancy in current record-keeping mechanisms that are often fragmented and require multiple points of input and verification by intermediaries".[1] Therefore, senior Bank of Canada officials have stated that "even if the products themselves ultimately fail, they advance the development of technologies that are likely to be useful for a range of other purposes".[2] However, they caution that at present, cryptocurrency would be unlikely "to form the basis of a stable or desirable monetary policy regime".[3]

The Canadian government itself is also experimenting with blockchain technology throughout different departments. The National Research Council is testing blockchain to

publish research grant and funding information in real time.[4] Canada Border Services Agency is participating in a pilot project designed to improve data quality and facilitate the movement of goods with blockchain-based technology.[5] As well as this, the Bank of Canada is actively conducting research to assess the effects of introducing a central bank digital currency.[6]

For federal income taxation purposes, cryptocurrencies are generally treated as akin to commodities, not as money. Under securities laws, many cryptocurrencies or "tokens" are classified as securities.

Cryptocurrencies are not treated as legal tender in Canada. According to section 8 of the *Currency Act*, legal tender is coins issued by the Royal Canadian Mint under the *Royal Canadian Mint Act*, and notes issued by the Bank of Canada under the *Bank of Canada Act.*[7] For this reason, the Bank of Canada prefers to refer to cryptocurrency as "cryptoassets", as the use of "currency" is somewhat misdescriptive.[8]

Despite cryptocurrency not being recognised as legal tender, the Bank of Canada tested Digital Depository Receipts ("**DDRs**") as a digital representation of Canadian currency in 2016 and 2017. DDR is a way to transfer central bank money on to a DLT Platform. DDRs are issued as digital tokens on a blockchain and act as a claim on central bank reserves.[9] This was tested in Project Jasper in the form of "CADcoin" where the Bank of Canada issued DDR, just like it would Canadian currency,[10] "in order to better understand the potential impacts of blockchain technology on Financial Market Infrastructure" ("**FMI**").[11]

Project Jasper was a joint initiative between the public and private sector, conducted by the Bank of Canada and Payments Canada with the help of banks and corporations (such as R3). Together, they built and tested a closed, simulated payment system to better understand the potential for blockchain to augment or displace FMI. Project Jasper marked the first-ever DLT experiment in which a central bank partnered with private financial institutions.[12]

To date, there have been four phases of the project. Phase One was developed on an Ethereum platform. Ethereum uses a Proof-of-Work ("**PoW**") consensus protocol to operationally settle transactions. Phase Two was built on the Corda platform. In this test, the Bank of Canada served as a notary, accessing the entire ledger and verifying the transactions.[13]

The Bank of Canada also considered legal settlement finality. Project Jasper was designed so that a transfer of DDR equalled a full and irrevocable transfer of the underlying claim on central bank deposits.[14] While using DDR requires significant Bank of Canada involvement in a system that many hope will be decentralised, it can provide certainty regarding legal settlement finality rarely found in blockchains.

The Bank of Canada partnered with Payments Canada and TMX in Phase Three of Project Jasper. In this test, the participants – the Bank of Canada, the Canadian Depository for Securities ("**CDS**"), Large Value Transfer System ("**LVTS**") banks and CDS members – experimented in broadening the DLT ecosystem beyond wholesale payments to include securities settlement for TSX-listed equities.[15] The proof-of-concept platform operated on a private Corda peer-to-peer DLT network that used open source Corda V2.0. Securities and cash were brought on ledger and could immediately be redeemed after their transfer by the issuance of DDRs by the Canadian Depository for Securities and the Bank of Canada. As well as this, the proof-of-concept also introduced a credit extension process in which LVTS members were able to extend credit to non-LVTS members in the form of DDR transfers. The Bank of Canada noted that several features of the DLT platform showed promise. Namely, the proof-of-concept created a shared ledger for token interactions with

cash and equities over a single distributed network, and the Corda DLT platform effectively integrated FMIs by enabling "loose coupling" of the components controlling the cash, equities and positions in the ecosystem.[16] This model ultimately achieved "DvP1 settlement with only DvP2 input of liquidity", and the loose integration framework left the Bank of Canada and CDS fully in control of their respective tokens for cash and equities.[17] Although the scope of the project was not broad enough to demonstrate whether DLT would yield significant cost savings or efficiency gains, the report stated that an "expansion of the scope across a number of possible dimensions" would likely provide such insight.[18]

In Phase Four, the Bank of Canada partnered with the Monetary Authority of Singapore to explore the use of DLT in cross-border payments.[19] The purpose of this phase of the project was to remedy some of the current issues to cross-border payment arrangements (such as lack of transparency of payment status, limited service availability, processing time, costs, and operational risks) by introducing a tokenised form of wholesale central bank currency for use by commercial banks.[20] This experiment marked the first successful trial wherein two central banks exchanged digital currencies using blockchain technology. By using Hash-Time Locked Contracts across the two DLT platforms to synchronise all actions making up a transaction (so that either all actions or no actions happen), the teams "successfully demonstrated a cross-border, cross-currency, cross-platform atomic transaction without the need for a third party that is trusted by both jurisdictions".[21] Once again, this experiment was a fairly specific proof-of-concept, and the report acknowledges that many opportunities for in-depth research remain open.

Cryptocurrency regulation

In Canada, cryptocurrencies are primarily regulated under securities laws as part of the securities' regulators mandate to protect the public.

Sales regulation

In Canada, securities laws are enacted on a provincial and territorial basis rather than federally. The securities rules throughout the provinces and territories have largely been harmonised. The Canadian Securities Administrators (the "**CSA**"), an unofficial organisation, represents all provincially and territorially mandated securities regulators in Canada.

Defining a "security"

The securities laws of a province or territory apply to people and entities: (a) distributing securities in that jurisdiction; or (b) from that jurisdiction. "Security" is broadly defined in Canadian securities legislation and covers various categories of transactions, including "an investment contract".[22] The test for determining whether a transaction constitutes an investment contract, and therefore a security, for the purposes of Canadian securities laws was established by the Supreme Court of Canada, referring to United States jurisprudence.[23] This test, the "**Investment Contract Test**", requires that in order for an instrument to be classified as a security, each of the following four elements must be satisfied:

1. there must be an investment of money;
2. with an intention or expectation of profit;
3. in a common enterprise (being an enterprise "in which the fortunes of the investor are interwoven with and dependent upon the efforts and success of those seeking the investment, or of third parties"[24]); and

4. the success or failure of which is significantly affected by the efforts of those other than the investor.

The application of the Investment Contract Test has been the subject of judicial and regulatory consideration that is beyond the scope of this overview. That being said, where the elements of the Investment Contract Test are not strictly satisfied, securities regulators in Canada are mandated to consider the policy objectives and the purpose of the securities legislation (namely, the protection of the investing public by requiring full and fair disclosure) in making a final determination. This acts a little like a legislative "basket clause". The Supreme Court of Canada has stated that substance, not form, is the governing factor in determining whether a contract (or group of transactions) is an investment contract.[25]

Regulator guidance

In addition to the law in Canada as set out in the Investment Contract Test, certain securities regulators in Canada have issued notices and statements regarding the potential application of securities laws to cryptocurrency offerings ("**ICOs**"). These notices and statements confirm that Canadian securities regulators, while receptive to innovation and development, continue to carefully monitor investment activity in this space.

In March 2017, the Ontario Securities Commission issued a press release[26] warning that ICOs may trigger certain Ontario securities law requirements (including registration or prospectus requirements), even if the coins or tokens do not represent shares or equity in an entity.

In August 2017, the CSA issued Staff Notice 46-307 *Cryptocurrency Offerings* ("**SN 46-307**").[27] Currently, this is the most comprehensive guidance regarding the applicability of existing securities laws to cryptocurrency offerings in Canada. In SN 46-307, the CSA stated that it was aware of businesses marketing their coins or tokens as software products, and taking the position that the offerings are exempt from securities laws, but cautioned that "in many cases, when the totality of the offering or arrangement is considered, the coins/tokens should properly be considered securities", including because they are investment contracts.[28] In line with Canadian jurisprudence and the Investment Contract Test, the CSA affirmed that it will consider substance over form in assessing whether or not securities laws apply to an ICO.

The CSA further cautioned that, depending on the facts and circumstances, coins or tokens may be considered derivatives and subject to applicable legislative and regulatory requirements.

In June 2018, the CSA issued Staff Notice 46-308 *Securities Law Implications for Offerings of Tokens* ("**SN 46-308**").[29] In SN 46-308, the CSA generally reiterated the position it took in 46-307. Importantly, it again confirms that an ICO may involve a distribution of securities not covered by the non-exclusive list of enumerated categories of securities in the OSA if the offering otherwise falls within the policy objectives and purpose of securities legislation. In addition, the CSA indicated that it had found that most offerings of tokens purporting to be utility tokens involved the distribution of a security, and specifically an investment contract.

In March 2019, the CSA and Investment Industry Regulatory Organization of Canada ("**IIROC**") published a joint Consultation Paper 21-402 Proposed Framework for Crypto-Asset Trading Platforms ("**CP 21-402**").[30] The purpose of CP 21-402 is to seek feedback to establish tailored regulatory requirements for platforms that facilitate the buying and selling or transferring of crypto assets ("**Platforms**") to address the novel features and risks of Platforms that are not addressed by the existing regulatory framework. CP 21-402 confirms the guidance set forth in SN 46-307 and SN 46-308, and states that a Platform on which

crypto assets that are securities and/or derivatives are traded would be subject to securities and/or derivatives regulatory requirements. It further clarifies that if an investor's contractual right to a crypto asset that is classified as a commodity constitutes a security or derivative, securities legislation could still apply to the Platform on which the crypto asset is traded. Examples of heightened areas of risk compared to other regulated entities, such as marketplaces, are outlined by the CSA and IIROC, and include investors' crypto assets not being adequately safeguarded, a lack of transparency of order and trade information, and the potential for manipulative and deceptive trading.

CP 21-402 outlines a Proposed Platform Framework (the "**PPF**") that will apply to Platforms that operate in Canada and Platforms with Canadian participants, and is based on the regulatory framework for marketplaces. The PPF incorporates requirements relevant for dealers and is structured to account for the different marketplace and dealer functions that Platforms may perform. Furthermore, the PPF also considers Platforms becoming IIROC dealer and marketplace members and becoming registered as investment dealers. If a Platform does business as an exchange, the CSA and IIROC suggest contacting the relevant securities regulatory authority to determine if recognition is appropriate. The CSA also anticipates that the requirements may need to be tailored for Platforms that trade or deal in crypto assets that may be classified as derivatives.

Securities law requirements

In Canada, absent an available exemption, a prospectus must be filed and approved with the relevant regulator before a person or entity can legally distribute securities. A prospectus is a comprehensive disclosure document which seeks to satisfy the public protection aim of securities laws by disclosing information about the securities and the issuer to prospective investors. Exemptions from the prospectus requirement are principally set out in National Instrument 45-106 – *Prospectus Exemptions* ("**NI 45-106**"). Generally, securities sold pursuant to a prospectus exemption are subject to resale restrictions and, particularly in the case of a non-reporting issuer (i.e. an issuer that is not a public entity and is not subject to ongoing securities compliance and disclosure obligations), may never be freely tradeable. Resale restrictions rules are set out in National Instrument 45-102 – *Resale of Securities* ("**NI 45-102**").

In addition to the prospectus requirement, an individual or entity engaged in the business of distribution of securities, or advising others with respect to securities, is required to register with Canadian securities regulators. The requirements for registration, and exemptions from registration, are set out in National Instrument 31-103 – *Registration Requirements, Exemptions and Ongoing Registrant Obligations* ("**NI 31-103**"). Once registered, the person or entity is subject to various reporting and compliance obligations. NI 31-103 covers various other categories of registration in addition to dealers and advisers, such as investment fund managers.

Legal status of ICOs in Canada

The present Canadian regulatory trend is to apply and adapt existing securities laws, including the Investment Contract Test, to transactions involving blockchain or cryptocurrency which resemble traditional securities, without regard to the use of new technology.[31] In order to make a determination on whether or not an ICO constitutes a distribution of securities, Canadian securities regulators will perform a case-by-case, highly fact-dependent analysis, focusing on the substance and structure of the ICO rather than its form.[32] Even if an ICO cannot be said to fall within the specific definition of a "security" provided by legislation, as discussed above, it may nonetheless be found to involve the sale

of securities if it otherwise triggers the policy objectives and purposes of securities legislation.

Applying the investment contract test to ICOs

As discussed above, there is presently no caselaw or legislation in Canada definitively addressing when an ICO or other sale of cryptocurrency will constitute a distribution of securities. However, statements from the CSA offer guidance regarding certain elements of an ICO that may increase the likelihood of the coins or tokens being found to be securities.[33] While each offering of coins or tokens should be analysed based on the particular circumstances of the offering and the features of the coin or token, these statements, together with statements by United States securities regulators on the subject,[34] offer insight into how the Investment Contract Test may be applied to ICOs.

Coins or tokens as securities

If an ICO is found to constitute a distribution of securities, it will trigger Canadian securities law requirements, including prospectus and registration requirements, unless an exemption from the same is available. Individuals or businesses intending to rely on prospectus exemptions in connection with an ICO will need to ensure that they satisfy the conditions for such exemption as set out in NI 45-106, including any applicable resale restrictions in NI 45-102. Resale restrictions will be of particular concern if coins or tokens begin trading on cryptocurrency exchanges or otherwise in the secondary market following their initial sale. Issuers of a cryptocurrency that is found to be a security will also need to ensure that they comply with any applicable registration requirements, including dealer registration, or that the conditions for an exemption from registration are fully satisfied. Failure to comply with securities laws may result in regulatory or enforcement action by securities regulators against the parties behind the ICO, including fines and potential incarceration.

Taxation

Background

The Canadian tax treatment of cryptocurrencies remains uncertain, with little legislative authority or administrative guidance. The Canadian federal tax authority (the "Canada Revenue Agency", or "CRA") has expressed high-level views regarding the characterisation of certain payment tokens (*i.e.*, Bitcoin) and the potential income and sales tax implications of transacting in such tokens; however, these views are extremely limited (some would argue outdated) and not particularly helpful in the rapidly evolving cryptocurrency landscape.[35] Moreover, while the Canadian federal government has recently made strides to address the void, particularly concerning the sales tax implications of certain "virtual payment instruments", much work remains to be done in order to solidify the underlying tax regime.

Accordingly, much of the analysis thus far concerning the potential tax treatment in Canada of cryptocurrency transactions is founded in an extrapolation of these administrative positions and thin legislative framework to scenarios upon which Canadian legislators and tax administrators have not expressly considered. It is hoped that greater clarity will be provided in the near future, which will not be limited to Bitcoin/payment instruments, but that will also consider more recent developments in cryptocurrency technologies and their evolving distribution to, and usage by, the public, including ICOs.[36]

Characterisation of cryptocurrency for income tax purposes

The CRA currently adopts the position that, despite its nomenclature, a cryptocurrency (specifically, a payment token such as Bitcoin) is not a "currency" for income tax purposes.

Rather, such a cryptocurrency is akin to a commodity (albeit an "intangible"), the value of which will fluctuate based on external factors driven largely by investor sentiment and basic supply/demand. Based on this view, this type of cryptocurrency could potentially be analogised as the virtual equivalent of a precious metal such as gold or silver. Such a characterisation, if appropriate, could have significantly different tax implications under Canadian tax law as compared to "normal" cash (even foreign currency) transactions. Note that the CRA has generally been silent on its views concerning cryptocurrencies other than payment tokens (*i.e.*, Bitcoin). Accordingly, references below to "cryptocurrency" are generally restricted to payment tokens unless otherwise indicated.

(a) Acquisition of cryptocurrency

The threshold question is whether the initial acquisition of a cryptocurrency is a taxable event that potentially triggers a Canadian income tax liability to the person acquiring the cryptocurrency. The answer depends on the manner, purpose and circumstances in which the cryptocurrency is acquired.

If the cryptocurrency is acquired through "mining" activities of a commercial nature (*i.e.*, mining carried out generally for business purposes or in connection with a business), the current published administrative position of the CRA is that the acquirer will be required to report business income for the year determined with reference to the value of the mined cryptocurrency. For this purpose, the mined cryptocurrency will generally be treated as inventory of the business. Such a holder will have a myriad of tax issues distinct from the acquisition of cryptocurrency from non-mining activities, and must be reviewed on a case-by-case basis.

The acquisition of cryptocurrency as a pure speculative investment, similar to physical gold or a publicly-traded security, is generally not a taxable event to the person acquiring the cryptocurrency. However, the acquisition will establish the holder's "cost" in the cryptocurrency for Canadian tax purposes, which is relevant in the determination of the tax consequences that will be realised later when the cryptocurrency is eventually sold or otherwise exchanged.

This is to be contrasted with the acquisition of cryptocurrency as consideration for the provision of goods or services, or as compensation for some other right of payment. Such transactions are generally governed at this time by the CRA's position regarding "barter transactions", which is described in greater detail below under the heading "*Using cryptocurrencies in business transactions – Barter transaction*".

(b) Determining a holder's tax cost in cryptocurrency

Once a cryptocurrency has been acquired, it will be important to determine its cost for Canadian tax purposes, which is a fundamental concept for determining the future income tax consequences on an eventual disposition of the cryptocurrency.

Where a cryptocurrency is purchased in exchange for Canadian currency, the cost of the cryptocurrency for income tax purposes will be equal to the amount of cash paid, plus any directly related acquisition expenses. If foreign currency is used, the holder will generally be required to convert the foreign currency into the Canadian-dollar equivalent at the applicable rate, pursuant to Canadian tax rules.

Cryptocurrencies can obviously be acquired by several alternative means, including commercial business transactions and other forms of "barter" exchanges. The particular facts surrounding any such acquisition could have meaningful distinctions regarding the determination of the holder's tax cost upon the acquisition of the cryptocurrency (see below, under the heading "*Using cryptocurrencies in business transactions – Barter transaction*").

(c) Tax on disposition of cryptocurrency

A person will realise taxable income (or loss) on an eventual disposition of a cryptocurrency. This includes a sale of the cryptocurrency for cash and the use of the cryptocurrency to pay for goods or services, or as consideration under other contractual rights/obligations (*i.e.*, a "barter transaction", described below).

If the cryptocurrency has a value at the time of its disposition in excess of its tax cost, it will be critical to determine whether the holder should report such excess as being on capital account (*i.e.*, a capital gain) or whether the proceeds should be reported as business income. This is a material distinction for tax purposes.

Generally, the buying and selling of a commodity can be regarded as being on capital account unless it is carried out in the context of a business of buying and selling such commodities, or such buying and selling otherwise amounts to an "adventure or concern in the nature of trade". This is a factual, case-by-case determination requiring a detailed review of the holder's dealings with such commodities.

If a person acquires cryptocurrency as payment for goods or services in the normal course of the person's business (even if the person is not, *per se*, in the business of buying and selling cryptocurrencies as part of a speculative investment business), there is a risk that any appreciation realised when the person disposes of the cryptocurrency will be fully taxable as business income. Again, this issue is fact-dependent, should be reviewed on a case-by-case basis, and is described in greater detail below.

Using cryptocurrencies in business transactions

(a) Barter transaction

A person can accept a commodity in exchange for the provision of a good or service or as consideration for some other form of right of payment, with such transaction being subject to tax treatment under Canada's "barter transaction" tax rules.

In a barter transaction using cryptocurrency, the following must be considered by the person (referred to below as the "provider") that accepts a cryptocurrency as consideration in exchange for a good, service or other right:

- The provider will generally realise business income for Canadian income tax purposes equal to the fair market value of the goods, services or other rights provided (the "**Business Income Inclusion**"). For this purpose (but not for other purposes – see, *e.g.*, the sales tax implications described below), the value of the cryptocurrency at the time of the exchange is generally not the determining factor.
- The provider will generally acquire the cryptocurrency with a cost for Canadian income tax purposes equal to the Business Income Inclusion.
- The provider is now the owner of the cryptocurrency and must (eventually) do something with it, such as sell it to an investor or use it to purchase goods/services/rights in connection with its own business. Any gain or loss realised by the provider on an eventual disposition of the cryptocurrency (*i.e.*, the difference between the provider's cost in the cryptocurrency, and the amount received on the eventual disposition) will be taxable at such time to the provider. The issue then becomes whether such gain/loss is treated as being on full income account or on account of capital (the income tax treatment being materially different as between the two) (see the discussion above under the heading "*Characterisation of cryptocurrency for tax purposes – Determining a holder's tax cost in cryptocurrency*"). Managing the provider's exposure to fluctuations in the value of the cryptocurrency post-acquisition will be a material and practical concern.

Another type of increasingly prevalent transaction (which may or may not be properly characterised as a "business transaction") is the acquisition by a person of one cryptocurrency ("crypto #1") in exchange for a different cryptocurrency ("crypto #2"). Such a transaction will also be considered a barter transaction involving the exchange of one commodity for another commodity. The person will generally be considered to have acquired crypto #1 with a tax cost equal to the fair market value of the crypto #2 given up in exchange, computed as of the time of the barter transaction. The additional complication in this scenario is that the person acquiring crypto #1 will also be considered to have disposed of crypto #2, and will have to report any income/gain in respect of crypto #2 for Canadian income tax purposes (the person must therefore know his/her tax cost in crypto #2, which depends on the manner in which crypto #2 was originally acquired by such person).

(b) Sales tax implications

Canada imposes a federal sales tax (the goods and services tax, or "**GST**") on the supply of many goods and services, subject to detailed exemptions. Most Canadian provinces and territories also levy sales tax, which is often "harmonised" with the federal sales tax to effectively create one blended federal/provincial (or territorial) rate. Persons that are required to charge and collect federal GST (or harmonised sales tax) in respect of a business activity can generally claim a rebate in respect of such tax that the person directly incurs in the course of carrying on such business (generally referred to as an input tax credit or "**ITC**"). The ITC mechanism is generally intended to mitigate the duplication of sales tax throughout a supply chain, and is designed to ensure that the cost of sales tax is ultimately borne solely by the end consumer of any particular good or service.

As with any provision of goods or services subject to federal and provincial/territorial sales taxes, a provider of goods/services that accepts cryptocurrency in lieu of government-issued currency must charge, collect and remit the appropriate sales tax. This may prove easier said than done in the context of cryptocurrency.

In this respect, the provider must be careful not to use the Business Income Inclusion amount (which is relevant under the Canadian tax authorities' current administrative policy to determine the provider's income tax associated with the sale) in determining the applicable amount of sales tax. For federal GST purposes, the Canadian tax authorities require that the provider charge, collect and remit GST based on the value of the cryptocurrency at the time of the sale. Presumably, the purchaser would be entitled to claim an input tax credit (if available) in respect of the full GST charged, if incurred in the course of a business activity.

While this may sound manageable at a high level, a few practical issues arise for the provider:

- How does the provider determine the value of the cryptocurrency at the precise moment of sale, particularly when cryptocurrencies are traded in non-traditional marketplaces and the value can swing wildly from day to day (possibly minute-by-minute)? What record-keeping is required by the service provider to justify the amount upon which it charges sales tax?
- How does the provider charge, collect and remit the sales tax in a transaction entirely handled in cryptocurrency, namely where the sales tax portion is also paid in cryptocurrency? The provider must remit to the Canadian tax authorities in Canadian currency (not cryptocurrency), meaning that the provider will be forced to either remit an equivalent amount of cash from other sources, or sell a sufficient amount of the

cryptocurrency to generate the cash to satisfy the remittance. Given the volatility of most cryptocurrencies, an inherent risk is borne by the provider in collecting the sales tax in cryptocurrency.

Corporate directors are personally liable for any deficiencies in collecting or remitting sales tax. It is therefore critical for the provider of goods/services to take reasonable measures to ensure full compliance and mitigate any associated risk.

Another sales tax issue associated with transactions involving cryptocurrencies is whether the person disposing of the cryptocurrency (*e.g.*, the person using the cryptocurrency to purchase goods or services or trading one cryptocurrency for another) is required to charge and collect sales tax on the value of the cryptocurrency. In this respect, if the disposition of a cryptocurrency is a barter transaction akin to a disposition of a commodity, should such disposition be treated as a taxable supply of the cryptocurrency much in the same way as a commodity? If that were the case, compliance obligations and costs associated with routine cryptocurrency transactions could become exceedingly complex and beyond the reasonable abilities of many holders/users of cryptocurrency. In May 2019, the Canadian Department of Finance released draft legislation aimed at simplifying the federal sales tax on certain transactions involving "virtual payment instruments" ("**VPI**"). In this respect, a VPI generally includes payments tokens such as Bitcoin, but expressly excludes tokens that operate in a manner similar to gift cards or that have functionality on a gaming or affinity/rewards program platform. Pursuant to these proposals, transactions involving VPI would generally be exempt from federal sales tax as a "financial instrument". These proposals demonstrate a willingness of the Canadian federal government to begin to tackle the difficult tax and compliance issues associated with cryptocurrencies, albeit in only a fairly narrow and targeted manner at this time.

Money transmission laws and anti-money laundering requirements

Canada was the first country to approve regulation of cryptocurrencies in the context of anti-money laundering. In 2014, the Parliament of Canada passed Bill C-31. This bill amends Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* to include virtual currencies. The bill laid out a framework for regulating entities "dealing in virtual currencies", treating them as money services businesses ("**MSBs**"). As MSBs, those dealing in digital currencies are subject to the same record-keeping, verification procedures, suspicious transaction reporting and registration requirements as MSBs dealing in fiat currencies.[37] As of May 2019, the amendments resulting from Bill C-31 had not been proclaimed in force.

Promotion and testing

The CSA Regulatory Sandbox was set up to encourage the development of innovative products and services. The Sandbox allows companies engaged in cryptocurrency matters to register or seek exemptive relief (generally on a time-limited basis) in order to test products and services in the Canadian market.

Ownership and licensing requirements

As noted above, an individual or entity engaged in the business of distribution of securities, or advising others with respect to securities, may be required to register with Canadian securities regulators. Similarly, investment fund managers are required to be registered.

On December 11, 2017 the Investment Industry Regulatory Organization of Canada ("**IIROC**"), the organisation that governs persons and companies registered under securities law, issued a notice to its members regarding margin requirements for cryptocurrency futures contracts that trade on commodity futures exchanges. According to the notice, members are required to market and margin crypto futures contracts daily at the greatest of: (a) 50% of market value of the contracts; (b) the margin required by the futures exchange on which the contracts are entered into; (c) the margin required by the futures exchange's clearing corporation; and (d) the margin required by the Dealer Member's clearing broker.

Mining

Because mining converts electrical energy (typically drawn from the power grid or a private power source) into waste heat in proportion to the difficulty of the underlying mathematical problem, it can result in large quantities of power being used for what may be perceived as a socially undesirable purpose. Furthermore, because mining enables the operation of a variety of cryptocurrencies (e.g. Bitcoin), it functions as a convenient point for regulatory intervention. For those reasons, many official bodies have started to explore, or in some cases implemented, laws or policies that contemplate cryptocurrency mining. In Canada, governmental regulators appear to have adopted a largely "hands-off" approach for the time being.

However, Hydro Quebec (a Quebec Crown entity) recently announced the implementation of higher power prices for users involved in cryptocurrency mining, the effect of which may be to discourage such activities in that Province. We expect to see further intervention by government actors, as the quantity of power used by cryptocurrency mining operations, along with the use of various cryptocurrencies to facilitate illegal activities, continues to grow. To counteract the deleterious effects of such regulations on their operations, we additionally expect to see Bitcoin miners move to private power sources as time goes on.

Border restrictions and declaration

There are no border restrictions or declaration requirements as such.

Reporting requirements

See "*Money transmission laws and anti-money laundering requirements*", above. MSBs are required to send a large cash transaction report to the Financial Transactions and Reports Analysis Centre of Canada ("**FINTRAC**") upon receipt of an amount of $10,000 or more in cash in the course of a single transaction, or receipt of two or more cash amounts of less than $10,000 each that total $10,000 or more, if the transactions were made by the same individual or entity within 24 hours of each other.

Estate planning and testamentary succession

Canada levies no separate estate tax, unlike many countries. However, a deceased is deemed to dispose of their property on death for its fair market value, which can result in income taxes being payable by the estate. Although it is far from settled, the Canada Revenue Agency currently takes the view that cryptocurrencies are generally commodities rather than currency, and that trading in cryptocurrencies will usually (with some possible exceptions) be regarded as being on capital account. In such circumstances, the estate will have to pay tax on any capital gains accrued as of the date of death. For a more detailed discussion of tax issues, see "Taxation" above.

In terms of estate planning, given the anonymous, decentralised nature of cryptocurrencies held on a blockchain, it will be imperative to include instructions on where to locate a copy of the private key related to the cryptocurrency. It would be unwise to include a private key in the will itself, since wills generally become public documents following probate.

* * *

Endnotes

1. Bank of Canada Staff Discussion Paper, *Crypto "Money": Perspective of a Couple of Canadian Central Bankers*, February 2019, p. 9 https://www.bankofcanada.ca/wp-content/uploads/2019/02/sdp2019-1.pdf.
2. Remarks by Timothy Lane, *Decrypting "Crypto",* October 1, 2018, p. 5, https://www.bankofcanada.ca/2018/10/decrypting-crypto/.
3. *Crypto "Money"* at p. 22.
4. https://globalnews.ca/news/3977745/ethereum-blockchain-canada-nrc/.
5. http://nexus.gc.ca/new-neuf/articles/blockchain-chaine-blocs-eng.html.
6. *Crypto "Money"* at p. 22.
7. *Currency Act*, RSC 1985 c. C-52.
8. *Decrypting "Crypto"* at p. 2.
9. https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf.
10. https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf.
11. https://www.coindesk.com/project-jasper-lessons-bank-of-canada-blockchain-project/.
12. Payments Canada, Bank of Canada, and R3, *Project Jasper White Paper*, June 2017, p. 8. https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf.
13. https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf.
14. https://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf.
15. Payments Canada, TMX Group, Bank of Canada, Accenture, and R3, October 22, 2018, *Jasper Phase III: Securities Settlement Using Distributed Ledger Technology,* p. 5, https://www.payments.ca/sites/default/files/jasper_phase_iii_whitepaper_final_0.pdf.
16. *Jasper Phase III,* p. 18.
17. *Jasper Phase III,* p. 29.
18. *Jasper Phase III,* p. 29.
19. Bank of Canada, Monetary Authority of Singapore, Accenture, and JP Morgan, *Jasper-Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technology,* May 2, 2019, p. 6, http://www.mas.gov.sg/~/media/ProjectUbin/Jasper%20Ubin%20Design%20Paper.pdf.
20. *Jasper-Ubin Design Paper*, p. 6.
21. *Jasper-Ubin Design Paper,* p. 7.
22. *Securities Act*, RSO 1990, c S.5 ("**ONSA**"), s. 1(1). See also *Securities Act*, RSA 2000, c S-4 ("**ABSA**"), s. 1(ggg)(ii), (v) and (xiv).
23. *Pacific Coast Coin Exchange v Ontario Securities Commission*, [1978] 2 SCR 112 [*Pacific Coast*].

24. *Ibid.* at p. 129, quoting *SEC v. Glen W. Turner Enterprises, Inc.*, 474 F. 2d 476 (1973) at p. 482.
25. Pacific Coin para 43. A flexible approach to defining an investment contract has also been promoted by the Ontario Securities Commission in *Bluestream Capital Corp, Re* (2015), 38 OSCB 2333.
26. See Ontario Securities Commission, News Release, "OSC Highlights Potential Securities Law Requirements for Businesses Using Distributed Ledger Technologies" at http://www.osc.gov.on.ca/en/NewsEvents_nr_20170308_osc-highlights-potential-securities-law-requirements.htm.
27. See Canadian Securities Administrators, Staff Notice 46-307 *Cryptocurrency Offerings* at http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm.
28. See SN 46-307 at 3.
29. See Canadian Securities Administrators, Staff Notice 46-308 *Securities Law Implications for Offerings of Tokens* at http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20180611_46-308_securities-law-implications-for-offerings-of-tokens.htm.
30. See Joint Canadian Securities Administrators/Investment Industry Regulatory Organization of Canada Consultation Paper 21-402 – *Proposed Framework for Crypto-Asset Trading Platforms* at https://www.osc.gov.on.ca/documents/en/Securities-Category2/csa_20190314_21-402_crypto-asset-trading-platforms.pdf.
31. SN 46-307, p. 3.
32. *Ibid*.
33. See SN 46-307 and Canadian Securities Administrators, Staff Notice 46-308 *Securities Law Implications for Offerings of Tokens* [SN 46-308].
34. See United Stated Securities and Exchange Commission, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, SEC Release No 81207 (July 25, 2017).
35. Certain provincial tax authorities, namely Revenu Quebec, have also published their own administrative positions on certain narrow issues (i.e., provincial sales tax) dealing with cryptocurrencies.
36. The taxation of ICOs is beyond the scope of this chapter, due to: (i) the significant differences in potential ICO structures and legal characterisation of the underlying transactions; (ii) the speed at which ICO structure and cryptocurrency "technology" and forms of offerings are evolving; and (iii) the lack of meaningful legislative, judicial or administrative guidance from a Canadian tax perspective. However, the fundamental "building block" tax concepts discussed in this chapter likely form the basis of the analysis underpinning certain of the discrete transactions and legal relationships created in many current ICO structures.
37. https://research.osc.gov.on.ca/c.php?g=699050&p=4969862.

Simon Grant
Tel: +1 416 777 6246 / Email: GrantS@bennettjones.com

Simon Grant is a co-head of Bennett Jones' cross-disciplinary Fintech & Blockchain practice group. Simon practices corporate and commercial law, with an emphasis on financing transactions and financial regulation.

Simon regularly advises clients on financial regulation and compliance, including foreign financial institutions and fintech companies doing business in Canada.

He also routinely acts for credit providers, borrowers and sponsors on loan facilities, acquisition financings, project financing and capital markets transactions.

Kwang Lim
Tel: +1 604 891 5144 / Email: LimK@bennettjones.com

Kwang Lim is a member of the Fintech & Blockchain practice group. His business law practice includes corporate finance and M&A. He focuses on offering practical and strategic advice and facilitating opportunities for entrepreneurs, start-ups, scale-ups, public companies, agents/underwriters and other advisors across various industry sectors (including blockchain and fintech, energy, mining, real estate, technology, biotechnology, and finance) that are involved in domestic and international financings and transactions. Kwang also advises on securities law compliance and corporate governance issues.

Kwang has been a guest lecturer for the Capstone Business Law course at the Faculty of Law, University of British Columbia. Kwang has also lectured on topics such as key provisions in technology agreements and the essentials of contract drafting.

Kwang obtained his Master of Laws at UCLA with a specialisation in business law.

Matthew Peters
Tel: +1 416 777 6151 / Email: PetersM@bennettjones.com

Matthew Peters advises clients in various industries, including natural resources, manufacturing, financial services, telecommunications, pharmaceuticals and technology, in connection with international tax planning, domestic and cross-border mergers and acquisitions, corporate reorganisations, corporate finance, executive and employee compensation and various other tax matters. He has also represented clients before the Tax Court of Canada and the Federal Court of Appeal.

Matthew is a frequent speaker on international and domestic tax matters, and has written and presented papers at conferences and seminars across Canada and the United States. He is a member of the Canadian and Ontario Bar Associations, Canadian Tax Foundation, New York State Bar Association, American Bar Association and International Fiscal Association.

Bennett Jones LLP

3400 One First Canadian Place, P.O. Box 130, Toronto, ON, M5X 1A4, Canada
Tel: +1 416 777 4801 / Fax: +1 416 863 1716 / URL: www.bennettjones.com

Cayman Islands

Alistair Russell & Dylan Wiltermuth
Carey Olsen

Government attitude and definition

The Cayman Islands is a leading global financial centre and has, over the course of several decades, developed a reputation as one of the world's most innovative and business-friendly places to operate. The jurisdiction offers a stable society and political system, judicial and legislative links to the United Kingdom, tax neutrality, many sophisticated service providers, and a proportionate regulatory regime that focuses closely on the financial services industry, and in particular those catering to sophisticated and institutional investors based elsewhere.

It is this reputation and these attributes that have helped the jurisdiction become an obvious choice for many of those proposing to establish fintech-related structures, whether it be in the form of a fund vehicle investing into Digital Assets,[1] an exchange for the same, an initial coin offering ("**ICO**"), or otherwise.

Each of the Cayman Islands Government, the Cayman Islands Monetary Authority ("**CIMA**"), and industry bodies such as Cayman Finance, acknowledge the importance of continuing to attract fintech business to the jurisdiction and ensuring the further growth of the sector. They are also aware, however, of the need to balance this approach with maintaining the Cayman Islands' commitment to the highest standards of financial probity and transparency and the specific considerations that can accompany Digital Assets.

Consequently, there has been no precipitous introduction of new regulation of the Digital Asset space, but rather a more judicious review of the sector and existing regulatory framework. Currently, the Cayman Islands Government is in the process of considering the proposals of an industry working group convened by CIMA regarding the adoption of any additional regulatory measures or governance standards for the marketing or trading of Digital Assets within and from the Cayman Islands. It is anticipated that the conclusion of this review will be made public shortly, but our expectation is that the results of the process are unlikely to lead to a wholesale or dramatic change of the current regulatory burdens, and will instead maintain the existing pro-industry approach while providing welcome clarification on certain areas of potential ambiguity.

In advance of the publication of such review and any steps to implement the same, however, this chapter sets out the current legal position in the Cayman Islands.

Cryptocurrency regulation

Save for certain aspects of the Cayman Islands anti-money laundering regime (as further detailed below), the Cayman Islands has not enacted any law or imposed any regulation that specifically targets Digital Assets.

As such, whether any activity involving a Digital Asset is subject to regulation will largely be determined in accordance with: (a) the nature of the activity being conducted; and (b) how the relevant Digital Asset would best be classified within the existing legislative framework.

Although a detailed analysis of each is outside the scope of this chapter, a summary of the statutory regimes that are most likely to be of relevance are as follows:

The Mutual Funds Law

Pursuant to the Mutual Funds Law of the Cayman Islands, an entity formed or registered in the Cayman Islands that issues equity interests and pools the proceeds thereof, with the aim of spreading investment risks and enabling investors to receive profits or gains from the acquisition, holding, management or disposal of investments, may come within the ambit of that statute and be required to obtain a registration or licence from CIMA.[2] The particular nature or classification of the Digital Assets will not generally be of relevance, provided they are being held as an investment.

As such, any pooling vehicle that is investing into the Digital Asset space or accepting Digital Assets by way of subscription and then investing into more traditional asset classes, would be advised to seek Cayman Islands legal advice on the point.

The Securities Investment Business Law

Pursuant to the Securities Investment Business Law of the Cayman Islands, an entity formed or registered in or that is operating from the Cayman Islands which engages in dealing, arranging, managing or advising on the acquisition or disposal of Digital Assets, may come within the ambit of the Securities Investment Business Law and be required to obtain a registration or licence from CIMA. This will, however, only apply to the extent that such Digital Assets constitute "securities" for the purposes thereof. The statute contains a detailed list of assets that are considered securities thereunder. Although such list does not currently make specific reference to any Digital Asset, in our view, certain types of Digital Asset are likely to constitute securities. Consequently, consideration will need to be given on a case-by-case basis as to whether the Digital Asset in question falls within one of the existing categories; for example, instruments creating or acknowledging indebtedness, options or futures. Equally, however, it seems clear that certain Digital Assets are likely to fall outside the definition, and thus outside the scope of the law (for instance, pure utility tokens and some cryptocurrencies).

The Money Services Law

Please see below for further details.

Anti-money laundering regulations

Please see below for further details.

Sales regulation

There are no securities or commodities laws in force in the Cayman Islands that apply specifically to Digital Assets (although please see the requirements of the Securities Investment Business Law as detailed above), whether in relation to their marketing and issuance by a Cayman Islands entity (e.g. pursuant to an ICO), or their sale by an existing holder.

In relation to the offering of securities or interests more broadly, where issuances or sales are targeted at investors based outside of the Cayman Islands, Cayman Islands law does not

generally impose any prohibition or regulatory burden; it will instead look to the local authorities where such investors are based, to restrict or regulate the same as they see fit. With that said, this is one area in which the Cayman Islands Government's review may lead to further regulation; specifically, in circumstances where structures are established in order to offer Digital Assets to retail investors based elsewhere. Whether or not this is seen as a suitable step will, however, likely depend in part on the speed with which the major on-shore jurisdictions clarify their approach to Digital Assets under their own securities law regimes.

In relation to the offering, sale, or issuance of interests *within* the Cayman Islands, however, certain regulatory provisions should be borne in mind. For example, the Companies Law prohibits any exempted company formed in the Cayman Islands and not listed on the Cayman Islands Stock Exchange from offering its securities to the Cayman Islands public. The Limited Liability Companies Law includes a similar prohibition in relation to LLCs. Even persons based, formed or registered outside the Cayman Islands should be careful not to undertake any activities in relation to a sale or issuance of Digital Assets that would constitute "carrying on a business" in the Cayman Islands. To do so may entail various registration and licensing requirements and financial and criminal penalties for those who do not comply. There is no explicit definition of what will amount to "carrying on a business" for these purposes, and consequently, persons who propose to undertake concerted marketing to the Cayman Islands public, particularly if it involves engaging in any physical activity in the Cayman Islands, are encouraged to seek specific legal advice on the point.

In practice, however, these restrictions do not generally pose much of a practical concern for issuers given that:

(i) the "public" in this instance is taken to exclude other exempted companies, exempted limited partnerships, and LLCs (which together comprise the majority of Cayman Islands entities); and

(ii) issuers' target investors tend not to include other persons physically based in the Cayman Islands themselves.

For completeness, and as detailed further above, Cayman Islands persons, or those operating from within the Cayman Islands, arranging for the sale or issuance of Digital Assets by another, may come within the ambit of the Securities Investment Business Law regardless of where the activity takes place, or the ultimate investors are based.

Taxation

There are no income, inheritance, gift, capital gains, corporate, withholding or other such taxes imposed by the Cayman Islands government, including with respect to the issuance, holding, or transfer of Digital Assets.

Stamp duty may apply to original documents that are executed in the Cayman Islands (or are brought into the Cayman Islands following execution). However, the sums levied are generally of a nominal amount.

Entities formed or registered in the Cayman Islands may also apply for and, upon the payment of a fee of approximately US$1,830, receive a tax exemption certificate confirming that no law enacted in the Cayman Islands after the date thereof imposing any tax to be levied on profits, income, gains or appreciations shall apply to such entity or its operations. Such certificates will generally apply for a period of between 20 and 50 years (depending on the type of entity).

Money transmission laws and anti-money laundering requirements

Money transmission laws

Pursuant to the Money Services Law, any person carrying on a "money services business" in or from the Cayman Islands must first obtain a licence from CIMA. Any breach of this requirement will constitute a criminal offence.

For the purposes of the foregoing, a "money services business" means the business of providing (as a principal business), among other things, money transmission or currency exchange services.

Although there is no clear authority on the extent to which the foregoing would be seen to include such transactions in cryptocurrency or other Digital Assets, a cautious and substantive reading of the statute may, in some cases, warrant it. In particular, if the Digital Assets in question are primarily used to facilitate the transfer of fiat currency from one party to another, or the conversion between fiat currencies, the legislation may well apply. Consequently, persons wishing to establish such businesses are encouraged to consider closely the application of the Money Services Law and consult appropriate advisors.

Although a consideration of the requirements of the licensing application and approval process under the Money Services Law is beyond the scope of this chapter, it will generally require:

(i) the maintenance of specified capital levels;

(ii) the appointment of approved auditors;

(iii) the provision of audited financials to CIMA;

(iv) the maintenance of proper records; and

(v) the payment of an annual fee.

Anti-money laundering requirements

The very nature and, in some cases, the intended features of Digital Assets can present heightened compliance risks and, moreover, practical hurdles to addressing the same. Such features may include the lack of a trusted central counterparty, increased anonymity, and ease of cross-border transfer without any gating or restriction.

Consequently, the Cayman Islands authorities have maintained a keen focus on balancing the jurisdiction's long track record of innovation and the promotion of a business-friendly environment with its commitment to the prevention of crime and maintaining robust standards of transparency. To date, this has been done, not by establishing an entirely separate regime for Digital Assets, but by applying the purposive approach enshrined within the existing framework which focuses on the specific activity and the nature of the assets in question so as to properly quantify the risk that the same may be used to facilitate illegal activity. With that said, we anticipate that the Cayman Islands authorities will continue to provide clarifying guidance and updates to address any ambiguities or uncertainties that arise in relation to the current regime.

Pursuant to the provisions of the Proceeds of Crime Law, the Anti-Money Laundering Regulations, and the guidance notes thereon (together the "**AML Laws**"), any persons formed, registered or based in the Cayman Islands conducting "relevant financial business" are subject to various obligations aimed at preventing, identifying, and reporting money laundering and terrorist financing.

"Relevant financial business" is defined in the Proceeds of Crime Law, and encompasses a broad variety of activity, including the following which may be of particular relevance in the context of Digital Assets:

- money or value-transfer services;
- issuing and managing means of payment (specifically including electronic money);
- trading in transferable securities;
- money broking;
- securities investment business; and
- investing or administering funds or money on behalf of others.

As such, the relevant requirements may depend on the type of Digital Asset in question; for instance, whether it can best be classed as a currency or money substitute, a security, a utility token or something else. We would thus generally expect businesses that engage in the operation of cryptocurrency exchanges, cryptocurrency issuances, brokering transactions in cryptocurrency, the trading and management of Digital Assets that are properly classed as securities, and the investment of funds (whether in the form of fiat currency or cryptocurrency) on behalf of others into Digital Assets, to come within the scope of the AML Laws. Notably, Digital Assets that are purely in the nature of utility tokens may fall outside of the ambit of the regime. However, specific legal advice on such distinctions is vital to ensure proper compliance and readers are encouraged to generally adopt a conservative approach.

Although a detailed consideration of the specific requirements of the AML Laws falls outside of the scope of this chapter, any person subject to the regime will generally need, among other things, to do the following:

- appoint a named individual as an anti-money laundering compliance officer to oversee its adherence to the AML Laws and to liaise with the supervisory authorities;
- appoint named individuals as the money laundering reporting officer and a deputy for the same to act as a reporting line within the business; and
- implement procedures to ensure that counterparties are properly identified, risk-based monitoring is carried out (with specific regard to the nature of the counterparties, the geographic region of operation, and any risks specifically associated with new technologies such as Digital Assets), proper records are kept, and employees are properly trained.

As above, particular practical concerns will often arise in relation to Digital Assets, specifically with regard to the identification of counterparties and the monitoring of source and use of funds. Most, in our experience, will be best advised to consult specialist third-party providers to assist with this process.

Promotion and testing

There are currently no 'sandbox' or other similar programmes in place in the Cayman Islands. However, the Cayman Islands Government has been vocal in promoting the Special Economic Zone ("**SEZ**") to those wishing to develop fintech-related products from the jurisdiction.

The SEZ offers businesses focused on the fintech industry the opportunity to establish physical operations within the Cayman Islands in a more streamlined manner. It provides several benefits, including a simpler, more rapid, and cost-effective work permit process, concessions with respect to local trade licences and ownership requirements, the ability to be operational within four to six weeks, and allocated office space.

When coupled with the other benefits of the jurisdiction and its recently updated intellectual property laws, the SEZ has proven highly popular with the fintech industry. To date, over

50 blockchain-focused companies have been established within it and this is expected to continue to grow. The SEZ also hosts a number of industry-focused events and conferences.

Ownership and licensing requirements

The Cayman Islands does not impose any restrictions or licensing requirements that are specifically targeted at the holding, management or trading of Digital Assets, whether by those doing so for their own account, or those doing so as a manager, trustee or advisor for the account of others.

As such, whether or not any such licensing or regulatory requirement is applicable to a particular activity will fall to be determined in accordance with the existing regulatory regimes, such as the Mutual Funds Law or the Securities Investment Business Law (each as further detailed above).

As also outlined further above, investment funds and managers that operate in the Digital Assets space are likely to need to comply with the requirements set out in the AML Laws.

Mining

The mining of Digital Assets is not regulated or prohibited in the Cayman Islands. We would note, however, that the import duties applicable to computing equipment and the high cost of electricity production in the Cayman Islands are likely to present practical deterrents to the establishment of any material mining operations within the jurisdiction. It is possible that the increased availability of renewable energy options, and the falling price of the same, may mitigate this somewhat in the future.

Border restrictions and declarations

The Cayman Islands does not impose any general border restrictions on the ownership or importation of Digital Assets.

As part of the Cayman Islands' commitment to combating money laundering and terrorist financing, the Customs (Money Declarations and Disclosures) Regulations mandate that individuals transporting money amounting to CI$15,000 (approximately US$18,292) or more into the Cayman Islands must make a declaration in writing to customs officers at the time of entry. However, the Customs Law defines "money" as being confined to cash (i.e. bank notes or coins that are legal tender in any country) and bearer-negotiable instruments (i.e. travellers cheques, cheques, promissory notes, money orders). As such, we would not expect such a requirement to apply to Digital Assets. Further, given the nature of Digital Assets, particularly those based or recorded on a distributed ledger, there is also the conceptual question of what would amount to the importation or transportation of the same.

Reporting requirements

There are no reporting requirements in the Cayman Islands specifically targeted at payments of, or transfers in, Digital Assets.

As above, to the extent that such a payment or transfer is made in the context of the conduct of "relevant financial business" for the purposes of the AML Laws, there may of course be an obligation to make certain filings or reports in the event that there is a suspicion of money laundering or other criminal activity.

Estate planning and testamentary succession

There is no particular regime under Cayman Islands law which deals specifically with the treatment of cryptocurrencies or other Digital Assets upon the death of an individual holding them. This means that, in principle, and assuming Cayman law governs succession to the deceased's estate, Digital Assets will be treated in the same way as any other asset and may be bequeathed to beneficiaries in a will, or, if a person dies intestate, will fall to be dealt with under the intestacy rules in the Cayman Islands Succession Law.

Although, as is the case in many jurisdictions beyond the Cayman Islands, there is likely to be some uncertainty as to where the *situs* of a Digital Asset is located (or indeed whether or not a *situs* can be determined at all), to the extent that the asset can be analysed under traditional conflict-of-laws rules as sited in the Cayman Islands, then a grant of representation would be required from the Cayman Islands court to preclude the risk of intermeddling claims in dealing with the asset in the Cayman Islands.

The main potential difficulty that may arise is practical; namely that anyone inheriting a Digital Asset will, on the face of it, often only be able to access that Digital Asset if the personal representative of the deceased or the beneficiary (as the case may be) has or can obtain the information needed in order to gain access and control over that Digital Asset (e.g. a private key to the wallet in which it is stored). Most exchanges have policies in place to transfer Digital Assets to next of kin but these policies, and the transfer requirements, will vary between the exchanges.

* * *

Endnotes

1. For the purposes of this chapter, "Digital Assets" shall be used to include all forms of blockchain-based units, whether in the form of securities-like tokens, utility tokens, cryptocurrencies or otherwise.
2. Notably, if the entity itself is "closed-ended" in nature, it will generally fall outside the scope of the law.

Alistair Russell
Tel: +1 345 749 2013 / Email: alistair.russell@careyolsen.com

Alistair is a partner in the corporate and finance group of Carey Olsen in the Cayman Islands and advises on all aspects of finance, fintech, corporate, investment funds and commercial law.

He has advised clients on a broad range of transactions including financing, fintech, ICOs, private equity, joint ventures, mergers and acquisitions and capital markets, and is described by clients in *IFLR1000* as "the best Cayman lawyer we've ever worked with".

Alistair was formerly with Skadden, Arps, Slate Meagher & Flom and Cleary, Gottlieb, Steen & Hamilton, each in London.

Alistair obtained a Bachelor of Civil Law with distinction from Christ Church, Oxford University, and an LL.B. with first class honours from King's College London.

Dylan Wiltermuth
Tel: +1 345 749 2010 / Email: dylan.wiltermuth@careyolsen.com

Dylan is a counsel in the corporate and finance group of Carey Olsen in the Cayman Islands and advises on all aspects of on securities, corporate and structured finance and public and private M&A.

He has spent many years advising clients on complex cross-border transactions across a wide range of jurisdictions and has a demonstrable track record of success in mitigating risk and delivering results.

Alistair was formerly with Kirkland & Ellis in London and Freshfields Bruckhaus Deringer in London and New York.

Dylan obtained an LL.B. with first class honours from Bond University.

Carey Olsen

PO Box 10008, Willow House, Cricket Square, Grand Cayman KY1-1001, Cayman Islands
Tel: +1 345 749 2000 / Fax: +1 345 749 2100 / URL: www.careyolsen.com

China

Jacob Blacklock & Shi Lei
Lehman, Lee & Xu

Government attitude and definition

While China has officially endorsed the underlying "distributed ledger" technology of blockchain (in Chinese: 区块链 or "Qūkuài liàn", which translates literally as "block chain"), authorities have adopted a sceptical and restrictive attitude toward Bitcoin (in Chinese: 比特币 or "Bǐ tè bì", which translates roughly as "special currency"), and other cryptocurrencies (in Chinese: 加密货币 or "Jiāmì huòbì", which translates as "cryptographic currency".

China's 13th five-year plan, released in 2016, described blockchain as a critical "strategic frontier technology" and called for increased research and development in technology and practical applications. China President Xi Jinping has called for technical innovations in "A new generation of technology represented by artificial intelligence, quantum information, mobile communications, internet of things and blockchain". The Ministry of Commerce has proposed blockchain solutions in areas ranging from credit reporting and supply chain management, to e-commerce and the financial industry. The tax bureau is exploring a pilot project which would place tax receipts on the blockchain to aid payment verification.

In contrast, cryptocurrencies are met with scepticism and considered to carry potential to create financial and even social instability. China regulation of Bitcoin dates back to the 2013 "Notice on Preventing Bitcoin Risk" (the "Notice"), an official notice issued in coordination by several Chinese regulatory bodies (People's Bank of China Ministry of Industry and Information Technology China Banking Regulatory Commission China Securities Regulatory Commission China Insurance Regulatory Commission).

The Notice seeks to reduce financial sector risk, by confirming "Bitcoin" shall not be treated as "currency", and reaffirming that there is only one official currency of the PRC, the renminbi ("RMB"). The Notice lists characteristics of Bitcoin identified as separating it from a true fiat currency: "Bitcoin is not issued by any monetary authority, it does not have the status of legal tender and the obliged payment status of currency, it is not currency in the true sense. It does not have equal legal status with currency, and it cannot and should not be circulated as currency on the market."

The Notice further states that Financial and Payment Institutions may not "use Bitcoin to set price for product or services, not buy or sell Bitcoins, not act as a market maker for Bitcoins, not underwrite insurance related to Bitcoin or cover Bitcoin in insurance, not directly or indirectly provide other Bitcoin related services, including registering, trading, clearing, settlement; not accept Bitcoin or use Bitcoin as payment tool; not start a Bitcoin and RMB or foreign currency exchange; not start a Bitcoin saving, trust or mortgage service; not issue Bitcoin related financial services; not use Bitcoin as investment in trusts or funds".

At the time of the Notice's publication in 2013, Bitcoin was the only major cryptocurrency. Similar prohibitions were renewed and expanded in 2017 with the release of the Tips on Preventing the Risks of so-called "Virtual Currency" such as Bitcoin (the "Tips"), issued by the Internet Finance Association.

The Tips identify clear "financial and social risks" in the growing use of cryptocurrencies (described in Chinese official documents as virtual currencies, "that cannot be ignored"). The Tips raise concerns about cryptocurrency being used for "money laundering, drug trafficking, smuggling, illegal fund-raising and other illegal and criminal activities" while at the same time recognising that some users of cryptocurrency may simply be speculators or investors, and many may be uneducated regarding risks of utilising cryptocurrencies as investments. The Tips closes by reminding financial industry participants to abide by relevant laws, which is best interpreted as referring back to the Notice.

Neither the Notice nor the Tips bans Bitcoin or other cryptocurrency from China, nor restricts individuals from holding and transferring cryptocurrencies. However, cryptocurrencies are prohibited to be used as a currency, and financial institutions are prohibited from offering cryptocurrency-related services. This leaves cryptocurrency in China in a largely unregulated grey area. Per the Notice, Bitcoin itself is to be treated as a "Virtual Commodity". Reasonable people may assume that this means Bitcoin would be treated by the law similarly to any other commodity; however, this is not clearly specified anywhere in the law. Importantly, this Virtual Commodity status is not explicitly extended to any other cryptocurrency as identified in any other law or regulation. Under the Chinese system of civil law, this calls into question whether other cryptocurrencies shall have the status of "Virtual Commodity".

In the first half of 2017, cryptocurrencies peaked in China with wild speculation as to Initial Coin Offerings ("ICOs"). There were over 65 ICOs in first part of 2017, with Chinese investors estimated to have deposited at least RMB 2.6 billion (almost USD 400 million) during the first half of that year. This created twin risks of uncontrolled capital flight from China, and potential economic destabilisation from inexperienced retail investors losing substantial sums of money in speculative ICOs, many of which were identified to be scams or not far from scams.

In September 2017, Chinese authorities stepped in with the Announcement… on Preventing Initial Coin Offerings (ICO) Risks (the "Announcement"). The Announcement effectively banned all ICO activity within the PRC as "unauthorized and illegal public fundraising" and "unauthorized public sales of securities".

The Announcement also made illegal all cryptocurrency exchanges within the PRC: "any of so-called token financing and trading platforms may not engage in the exchange services between any legal tender and tokens or between 'Virtual Currencies', or engage in the sale of tokens or Virtual Currencies for itself or as a central counterparty, or provide services such as pricing and information intermediary for tokens or Virtual Currencies."

China's Block/Chain

In contrast to cryptocurrency, the Chinese government has been much more favourable to blockchain technology itself; however, it has nevertheless identified a need to closely regulate blockchain services. In February 2019, the Cybersecurity Administration of China implemented the Blockchain Information Service Management Regulations ("BISMR") which established the legal framework for the operation of a blockchain-based business within the PRC.

While typical cryptocurrency blockchain technology emphasises anonymity for transactions, privacy, and avoidance of institutions, the BISMR emphasises China's conception of "Cyber Sovereignty" and the importance of the distributed ledger for preserving information.

Under the BISMR, enterprises providing blockchain-based services must register as such with regulators, and must collect real name and identity of users of the blockchain service. Blockchain service providers have an obligation to monitor use of the blockchain for illegal purposes, stop illegal use, remove illegal content, report illegal activities to authorities, and provide records to authorities on demand.

The BISMR regulations may be best understood, as a legal means to ensure that illegal content is "Blocked" from publication by usage restrictions and by obligations for the service provider to remove prohibited content from the blockchain.

At the same time, real name registration requirements and requirements for blockchain service providers to maintain records of use work to "Chain" users of the blockchain network to their activities and content posted to the network.

Thus, China may be said to adopt a "Block/Chain" approach to blockchain regulation.

This may cause special regulatory hurdles to Western companies providing blockchain-based services, where Western-based users may have certain expectations as to privacy, which may be put at risk as the company attempts to expand services into China's 1.3 billion-person market. This may lead to unique solutions where one might find an internal China law-compliant blockchain network within China, which functions separately and does not interact with an external, globally accessible blockchain network.

Cryptocurrency backed by the People's Bank

There has been speculation of an official, central bank-backed cryptocurrency in China since early 2017. A July 2017 article in *MIT Technology Review* cites People's Bank of China ("PBoC") internal documents which reveal the PBoC had been engaged in prototyping of such national cryptocurrency as much as two years ago and has been testing the prototype since then.

As recently as July 2019, in the wake of the announcement of the Facebook-backed cryptocurrency Libra, the Director of the People's Bank of China Research Bureau confirmed that the Chinese government is launching a research initiative for a new cryptocurrency platform.

There have been no other official announcements about an official PRC cryptocurrency to date; however, on August 1, 2019, the PBoC announced it had secured six blockchain-related patents, including patents touching on cryptocurrency wallets, systems for cryptocurrency exchange, and synchronisation systems, among others.

Cryptocurrency regulation

Cryptocurrencies themselves are not directly regulated in the PRC; however, each of the primary ways users would typically interact with cryptocurrencies are highly regulated, if not outright prohibited. As mentioned above, the Notice prohibits financial institutions and payment institutions from providing Bitcoin-related services. Bitcoin and other cryptocurrency may not be used as money. ICOs and cryptocurrency exchanges are prohibited per the Announcement.

However, as stated above, there is no outright ban on users owning cryptocurrency or making transfers of cryptocurrency, whether sending or receiving.

Bitcoin is named a "Virtual Commodity" as per the Notice and should theoretically be treated as any other commodity able to be exchanged between individuals for an agreed value of other currency or other commodity. PRC law or regulation has not thus far gone into deeper explanation as to what "Virtual Commodity" is under law or how it may be same or different from a standard commodity.

Importantly, a recent China court decision appears to clarify the legal status of Bitcoin in China by finding a legally recognised property right in Bitcoin. The ruling comes from Hangzhou Internet Court, a specialised court established in August 2017, which handles matters related to internet commerce. In one case, the plaintiff claimed that he had purchased 2.675 bitcoins via the online marketplace operated by Alibaba's Taobao e-commerce platform. The purchased bitcoins were stored in a "virtual wallet" online. Later, when the plaintiff sought to sell the bitcoins and withdraw the money, it was discovered that the shop which had sold the bitcoins (and offered the online storage) had closed, leaving the individual unable to access the bitcoins or the purchase funds.

The plaintiff filed the lawsuit against the operator of the online shop and against the Taobao online platform which hosted the shop, claiming RMB 76,300 in compensation and damages. What's interesting is that although the plaintiff was not victorious in the case due to lack of supporting evidence, the court went out of its way to discuss the legal aspects of Bitcoin in the context of PRC property law. The court indicated in its July 2019 decision that Bitcoin met the legal requirements to be considered virtual property because it is "valuable, scarce, and disposable".

When discussing such a judgment, it is important to keep in mind that Chinese court decisions are each an independent interpretation of the law and judgments do not establish legal precedent for future cases to follow. However, it is a good guess that on an issue as sensitive as Bitcoin, the judge in this case would have some idea of high-level unofficial expectations for legal treatment of Bitcoin, which likely informed the conclusions offered in the decision. If ownership of Bitcoin were actually deemed illegal in China, it is likely the court case would have been thrown out at an early stage for not having an actionable claim.

Sales regulation

In general, transfer of Bitcoin, cryptocurrencies or tokens between two individual private citizens is not illegal, and is not specifically regulated. For example, an individual owner of Bitcoin ("BTC") may agree with an individual owner of Ripple ("XRP") to transfer a certain amount of BTC to the owner of Ripple in exchange for either an agreed value of RMB, or an agreed value of XRP.

Nothing in current PRC law or regulation makes either of these potential transactions illegal. If the owner of BTC receives RMB in exchange for the BTC transfer, the law would treat it as exchanging valid PRC fiat currency ("RMB") for a commodity at an agreed price. The BTC owner would be obligated to send the agreed amount of BTC to the target wallet just as a shop owner hands over a bottle of water after receiving the purchase price in RMB.

Likewise, if the two exchanged BTC for XRP, this is not prohibited by PRC law because it is the direct action of two private individuals rather than an online transaction facilitated by a publicly facing online cryptocurrency exchange.

However, all of the above must be understood with the caveat that cryptocurrency is not to be used as or replace fiat currency. For example, it would be illegal within PRC for a

purchaser to pay for an apple by sending Bitcoin to the seller, as RMB is the only officially recognised currency.

In contrast, conducting an ICO whereby an individual or small start-up entity accepts money from investors which goes toward establishing a cryptocurrency, with promises of future returns or granting of coins to the donator, is patently illegal under the Announcement. In this case, it does not matter whether the ICO activity is conducted online and offered to the entire population or conducted in a closed face-to-face environment. The important difference in these scenarios is that the ICO format directly resembles sales of securities. While ICOs are not regulated by PRC Securities Law *per se*, they are illegal because they are deemed a form of unlicensed offering of securities.

The Announcement identifies ICOs as a "scheme" to "issue and sell tokens to investors in exchange for the so-called Virtual Currencies such as Bitcoins and Ethercoins, which in essence is an unauthorized and illegal public fundraising… illegal issue of securities, illegal fundraising, financial fraud… and other illegal criminal activities".

Taxation

Currently, there are no specific tax laws or regulations which refer to cryptocurrencies, which creates a grey area. Normally a tax bureau would not hesitate to impose taxes on any kind of income. However, cryptocurrencies are in a unique situation as banks and financial institutions are prohibited from offering cryptocurrency-related services, and exchanges of cryptocurrencies are also prohibited. The PRC Taxation Bureau has no capability or infrastructure to monitor revenues from cryptocurrency trading. We are not aware of any example where tax authorities in the PRC collected tax against revenue generated via cryptocurrencies. While it is impossible to offer a definite statement of official tax treatment of cryptocurrencies, we believe that because of restrictions on cryptocurrency-related services, and cryptocurrency exchanges in general, as well as limitations to institutional capacity, the Tax Bureau would not be inclined to officially tax revenues from cryptocurrencies.

However, in the event tax authorities become aware of a large amount of money in a bank account which is not attributable to normal business activities or employment, and the tax authorities have no record of such money being taxed, we would expect tax authorities to deem those funds as taxable income and levy a tax in accordance with law, regardless of the nature of the origin of the funds.

Money transmission laws and anti-money laundering requirements

China implements strict capital controls designed to limit the amount of capital outflow from China to other countries via foreign exchange. Individuals are limited to transporting or sending up to USD 50,000 outside of PRC annually, and corporate remittances abroad are closely scrutinised and must meet the approval of China's State Administration of Foreign Exchange ("SAFE").

Cryptocurrencies risk destabilising this system of capital controls by allowing individuals to transfer money abroad without relying on Chinese banks and going through the SAFE process.

As discussed above, the PRC implements a very strict currency control regime which places severe restrictions on convertibility of currency and ease of transfers abroad. These rules apply universally. Any use of cryptocurrency to transfer over USD 50,000 per individual

out of the territory of the PRC annually will likely be deemed a violation of individual limitations of foreign exchange transfers. Note there is no such restriction on receiving over USD 50,000 or more of cryptocurrency within the territory of China via a transfer coming from outside the territory of China.

Companies seeking to remit funds abroad for business purposes are also required to report to SAFE, and go through a formal application and approval process for the foreign remittance. Any corporate entity utilising cryptocurrency to transfer significant sums of money abroad would also likely be deemed in violation of currency exchange and foreign remittance regulations set by SAFE.

According to the Notice, banks "should closely monitor the trends and activities Bitcoin and other similar virtual commodities with the characteristics of anonymity and easy cross-border access, seriously consider its money laundering risk, research and implement targeted preventative measures. The branches should include lawfully established organizations that provide Bitcoin registration or exchange services in its area into its anti-money laundering monitoring, and supervise them to strengthen their anti-money laundering monitoring".

The notice goes on for a second paragraph regarding obligations of "Bitcoin" websites to undertake anti-money laundering issues; however, this is less relevant now as anything which may be considered a "Bitcoin website" in PRC has been taken offline.

Though banks are tasked with monitoring cryptocurrency-related activities for money laundering issues, the same banks have been prohibited from doing cryptocurrency-related business and all Chinese-located exchanges that the PRC banks would be in a position to coordinate with in anti-money laundering issues have been shut down.

Promotion and testing

As mentioned above, the PBoC is currently engaged in research and development of a new Central Bank Digital Currency ("CBDC"), which is coordinated by a new Digital Money Laboratory. The goal of the PBoC's CBDC will be to maintain state control over "monetary sovereignty" and the idea that a virtual currency must be issued by the state central bank in order to be valid as currency.

Since 2018, the PBoC has been recruiting blockchain technology and legal experts to further develop the technical and legal aspects of implementation of such CBDC. The PBoC is also studying the legal and economic impact of a planned CBDC implementation. The Digital Money Laboratory has submitted more than 40 patent applications for blockchain and cryptocurrency-related technologies.

In a recent interview, Zhou Xiaochuan, President of the People's Bank of China, responded to the news that the People's Bank of China recognised that replacement of paper money by new technologies is "inevitable". Mr. Zhou's comments suggested the PBoC was seeking to balance desire for anonymity in cryptocurrencies against interests of maintaining social security, financial stability and social order, and the ability to combat criminal activities.

Mr. Zhou cited energy consumption and storage restraints as key technical barriers to effective implementation of the CBDC for the next several years.

Other than the above-mentioned PBoC research and development programme for a national cryptocurrency, it is unlikely that any special cryptocurrency research and development programmes have been established. However, the State Counsel has named blockchain in official documents as a key technology of the future requiring additional research and indigenous innovation.

National level endorsement

The PRC government is far more interested in promoting research and development in new applications for blockchain and distributed ledger technology, rather than cryptocurrency. At the national policy level, a reference to "blockchain" first appeared in the "13th Five-Year Plan for National Informatization" issued by the State Council in December 2016. According to the plan, China should strengthen the advanced layout of strategic frontier technology, and "strengthen the basic research and development and frontier layout of new technologies" such as blockchain, and several other futuristic technologies.

In August 2017, the State Council issued an official Guiding Opinion which encouraged the "Development of personalized software by using open source code and the pilot application of new technologies such as blockchain and artificial intelligence" in support of cloud computing and big data applications.

Two months later, in October 2017, the General Office of the State Council issued the "Guiding Opinions on Actively Promoting Supply Chain Innovation and Application", proposing that China should strengthen the construction of supply chain credit and supervision service system via study of "new technologies such as blockchain and artificial intelligence".

While there are no officially announced projects implementing blockchain research in these fields, we can say for sure that blockchain has caught attention at the highest levels of government as a powerful, innovative economic force.

Local level implementation

Domestic regions have launched diverse incentive policies for blockchain technology research, including: Beijing; Guizhou; Guangzhou; Fujian; Zhejiang; Hong Kong; and 18 other regions which have issued blockchain policies, such as financial support, office space and more.

One big example of this is a new Free Trade Zone in Hainan. Following the FTZ model which China used successfully to attract foreign manufacturing to the country through special incentives, the Hainan FTZ aims to attract blockchain research. The FTZ, established in October 2018, will see the entire Island of Hainan designated a "Blockchain Test Zone", with the local Hainan government investing in promising blockchain products and building a new blockchain test facility.

The focus of the Hainan FTZ is blockchain research, centred on the "Oxford-Hainan Blockchain Research Institute" jointly built by the Hainan Eco-Software Park and Oxford University's Blockchain Research Centre. The Hainan FTZ is expected to attract interest from leading blockchain research divisions from both the academic and corporate sectors.

Ownership and licensing requirements

Pursuant to the Notice and the Tips, financial institutions, including generally banks, insurance companies, securities companies and investment management companies, are not allowed to engage in a wide variety of Bitcoin- and cryptocurrency-related services; specifically, they are prohibited from:

- setting a price on Bitcoin products and services;
- trading Bitcoin or acting as a central counterparty;
- providing insurance coverage on Bitcoin; and
- providing business services directly/indirectly related to Bitcoin, including: register, trading, clearing, and settlement of Bitcoin; receiving or using Bitcoin as method of

payment; exchanging Bitcoin for RMB or foreign currencies; participating in businesses related to storing, custody, and collateralising of Bitcoin; issuing financial products related to Bitcoin; and taking Bitcoin into asset pools of trusts and funds.

A plain reading of the Notice would suggest that these restrictions would apply to investment advisors and fund managers as target financial institutions. Investment advisors and fund managers are therefore prohibited from "participating in businesses related to storing, custody, collateralizing of Bitcoin; issuing financial products related to Bitcoin; taking Bitcoin into asset pool of trusts and funds" among other key cryptocurrency-related businesses. While the notice only specifically names Bitcoin, the later Tips appears to have the effect of extending the same prohibitions to all cryptocurrencies.

Because cryptocurrency-related services are prohibited by financial institutions and treated very seriously by the authorities, there are no licensing requirements which would permit such activities.

Mining

The National Development and Reform Commission ("NDRC") has issued a new draft this year of the Catalogue of Guidance for Industrial Structure Adjustment (2019 edition, draft for comments) (the "Draft Guidance Catalogue"). The Catalogue of Guidance for Industrial Structure Adjustment is an industrial policy document issued by the NDRC, which lays out national priorities as to economic, industrial and technology priorities and goals. A draft catalogue is a non-final version released for public comment, but can provide valuable insight into actual thinking of policymakers, and often the final product will be very similar to the draft.

In the 2019 Draft Guidance Catalogue, cryptocurrency mining activities are singled out as "obsolete" and even given the label of "backward production technology equipment". This basically means that cryptocurrency mining activities are officially disfavoured as a form of business. We also note that no "phase out" period is given, which indicates that the disfavoured approach to cryptocurrency mining is to be implemented immediately.

While implementation of this document with cryptocurrency restrictions in its current form will not make cryptocurrency mining "criminal", the document will certainly be used to make operations more difficult for cryptocurrency miners. Any businesses which had formerly been approved for cryptocurrency mining operations will be subject to shutdown or forced to change business model, and new businesses attempting to start up cryptocurrency mining operations will not be allowed to proceed. Reports are becoming more frequent of local police raiding and shutting down cryptocurrency mining operations, which had been flagged due to abnormally high power consumption; we expect such trends to continue.

Cryptocurrency mining operations are disfavoured by Chinese authorities both due to the burden on public electrical power infrastructure and the broader potential uses of cryptocurrency as an alternative to the RMB and as a means to bypass RMB currency controls on foreign exchange.

Border restrictions and declaration

There are currency reporting and cross-border transfer agreements as discussed above, which transfers of cryptocurrency across borders will likely be deemed in violation of. However, there are no specific regulations as to the transfer of cryptocurrency across borders, or declaration of cryptocurrency holdings at border crossings or at customs.

Reporting requirements

There are numerous other restrictions on cryptocurrency-related activities as described above; however, currently there are no formal requirements for the reporting of cryptocurrency transactions which exceed a certain minimum. There will be regular tax reporting requirements where a user receives income related to cryptocurrency transfers; however, this is not a requirement specific to cryptocurrency.

Estate planning and testamentary succession

There have not been any amendments to PRC estate planning and testamentary succession laws directly dealing with cryptocurrencies. However, given that the Notice describes cryptocurrency as a "Virtual Commodity" and that the recent Hangzhou Internet Court decision found a valid property right in Bitcoin, it is reasonable to assume that cryptocurrencies may be treated as any other property item for the purpose of estate planning and testamentary succession.

Specifically, Chinese law allows for testamentary succession and distribution of properties via a will. It is reasonable to treat cryptocurrency as property which may be distributed by a will, or would be distributed by a court in accordance with the PRC law of inheritance in absence of a valid will.

Likewise, for personal cryptocurrency wallets, we see no reason why the wallet address could not be written on a piece of paper and kept in a secure envelope along with the will, as may be done with any other confidential document, along with instructions on who shall be given the envelope upon death of the principal.

Jacob Blacklock
Tel: +86 8532 1919 / Email: jblacklock@lehmanlaw.com
Jacob has worked as a legal professional in China for over five years, regularly advising clients in areas of foreign direct investment, M&A, and doing online business within China.

Shi Lei
Tel: +86 1510 1509 810 / Email: steve.shi@lehmanlaw.com
China Licensed Attorney, University College London Master, former Huawei Contract and Commercial Manager.

Lehman, Lee & Xu

10-2 Liangmaqiao Diplomatic Compound, No. 22 Dongfang East Rd., Chaoyang, Beijing, China
Tel: +86 8532 1919 / URL: www.lehmanlaw.com

Cyprus

Karolina Argyridou, Prodromos Epifaniou & Akis Papakyriacou
Verita Legal K. Argyridou & Associates LLC

Government attitude and definition

In Cyprus, the topics of blockchain and cryptocurrency are emerging as new areas of law, with both potential participants, as well as regulators, gradually showing increased interest. As a result, the Cyprus Securities and Exchange Commission ("**CySEC**") has established an innovation hub aiming to establish a dialogue with businesses providing emerging financial technologies to determine and accelerate their business models in line with CySEC's commitment to ensuring regulated entities' investor protection. CySEC, via the innovation hub, offers support to market participants who are introducing innovative financial products or services.

The Cyprus government, by Council of Ministers' decision N.85.629, dated 30 August 2018, has formed an *ad hoc* working group to develop and implement blockchain technology in Cyprus. The aim of the working group is to prepare a detailed action plan for the development of blockchain technology.

It is apparent that Cyprus is taking important steps to keep up with the international developments and trends by introducing new and innovative technologies applicable to financial services.

Cryptocurrency regulation

In Cyprus, there are currently no specific references to cryptocurrency in the legal or regulatory framework in force, and cryptocurrencies are not, *per se*, regulated. However, both the Central Bank of Cyprus ("**CBC**") and CySEC have issued a number of warnings to potential cryptocurrency investors as well as to investment firms ("**CIF**") looking to deal in or promote or provide cryptocurrencies.

Specifically, on 7 February 2014, the CBC issued an announcement entitled "*attention to the risks associated with virtual currencies*". The CBC therein stressed that cryptocurrencies are not considered "*legal tender*", noting also that any activity relating to cryptocurrencies is not authorised by the CBC, pointing out that "*the public needs to be aware of the fact that there are no specific regulatory measures to cover losses from the used of virtual currencies if the platform that exchanges or holds them collapses and thus there is the risk of losing the entire amount deposited*". The CBC also sets out, indicatively, a number of risks associated with cryptocurrencies:

- lack of guarantee or legal obligation to reimburse at face value;
- the price of virtual currencies is highly volatile and may rise sharply or even fall to zero value;

- any merchant may refuse to accept cryptocurrencies for payments; and
- transactions in cryptocurrencies are more likely to be misused for the purpose of illegal activities.

CySEC, on 6 February 2014, issued an announcement to draw the attention of the public, and more specifically potential investors, to the warning of the European Banking Authority ("**EBA**") on the risks in connection or arising out of the purchase, possession or trading of cryptocurrencies. Additionally, CySEC, through the aforementioned announcement, shared the report on the characteristics, functions and risks of virtual currency that was issued by the European Central Bank.

Following the aforementioned announcement, CySEC, on 18 March 2014, issued an additional announcement outlining, *inter alia*, the following risks associated with buying, holding, exchanging or trading in cryptocurrencies:

- cryptocurrencies deposited in an e-wallet may be stolen; and
- transactions in cryptocurrencies may involve money laundering and terrorist financing activities.

Subsequently, CySEC, on 13 October 2017, issued an announcement entitled "*Warning to investors on trading in virtual currencies*". CySEC therein set out, *inter alia*, the following risk associated when buying, holding, exchanging or trading in cryptocurrencies:

- Trading in cryptocurrencies or in contracts for difference ("**CFDs**") relating to cryptocurrencies is not suitable for all investors.
- There are no specific EU regulatory provisions that would protect existing and/or potential investors who trade on these products.
- Trading in cryptocurrencies comes with a high risk of losing all your invested capital.

In addition to the aforementioned risks, CySEC, in the same announcement, warned investors that they must be careful in the following practices:

- "*"Guaranteed" high investment returns, with little or no risk;*
- *Unsolicited offers (without providing full analysis of the risks involved);*
- *Sounds too good to be true, as investments providing higher returns typically involve more (high) risks;*
- *Sales practices characterised by direct or indirect pressure or promises to actual or potential investors to trade in such products).*"

Furthermore, CySEC stressed that: "*Investors should invest in an Initial Coin Offering* ("**ICO**") *project if they have the necessary experience and knowledge, are confident of the quality of the ICO project itself and are prepared to lose their entire funds.*"

On 15 May 2018, CySEC issued Circular C.268 (the "**Circular**"), entitled "*Introduction of new rules governing derivatives on virtual currencies*", which replaced Circular C.244 entitled "*Trading in virtual currencies and/or trading on contracts for differences relating to virtual currencies*", issued by CySEC on 13 October 2017. The Circular clarifies, *inter alia*, the following:

- any activity relating to cryptocurrencies is not currently regulated by CySEC; and
- derivatives on cryptocurrencies, however, are now capable of qualifying as financial instruments under the law that provides for the provision of investment services, the exercise of investment activities, the operation of regulated markets and other related matters L.87(I)/2017 (the "**Law**"). Among the financial instruments listed in Part III

of the First Appendix of the Law, derivatives on cryptocurrencies may fall under the following:

"*i. "[…] any other derivative contracts relating to securities […] which may be settled physically or in cash";*

ii. "financial contracts for differences";

iii. "[…] any other derivative contracts relating to assets […] not otherwise mentioned in this Section, which have the characteristics of other derivative financial instruments"."

"*Therefore, depending on their specific characteristics and use, providing investment services in relation to derivatives on virtual currencies will require specific authorisation by CySEC*."

Additionally, the Circular outlines the obligations of CIFs when providing investment services in derivatives on cryptocurrencies. Specifically, the Circular highlights the following non-exhaustive list of obligations:

- "*act honestly, fairly and professionally, in accordance with the best interests of their clients;*
- *provide fair clear and not misleading information to their clients;*
- *provide appropriate guidance on and warnings of the risks associated with investments in those instruments;*
- *have adequate product governance arrangements;*
- *execute orders on terms most favourable to the client;*
- *maintain adequate capital.*"

Furthermore, the Circular also provides the following:

- CIFs must consider the product governance requirements when manufacturing, designing and/or distributing derivatives on cryptocurrencies; and
- CIFs must provide the investors or potential investors with all information including but not limited to the risks associated with the derivatives on cryptocurrencies and fees and costs.

Moreover, it is provided that CIFs:

- should ensure that the reference prices used are gathered from publicly available sources of good repute;
- shall consider the risks associated with derivatives on cryptocurrencies in the context of their internal Capital Adequacy Assessment ("**ICAAP**"); and
- shall consider the ESMA intervention measures and leverage limits.

Sales regulation

ICOs have become an increasingly popular way to increase funds. It is quite common for cryptocurrencies to be used in an ICO. There is no prohibition on ICOs in Cyprus. It is noted that care needs to be taken in order to ensure that the way in which an ICO is conducted does not cause a breach of the relevant regulatory framework. The Alternative Investment Fund with Limited Number of Persons would potentially be an appropriate vehicle for such ICOs in Cyprus, as it has no diversification requirements and is a particularly flexible investment vehicle.

Money transmission laws and anti-money laundering requirements

CySEC, on 19 February 2019, issued a Consultation Paper with respect to the proposed amendment of the Prevention and Suppression of Money Laundering and Terrorist Financing Law 188(I)/2007 to 2019 (the "**AML Law**") for the prevention and suppression of money laundering and terrorist financing.

The proposed amendments intend to extend the scope of the AML Law by applying the AML Law obligations to the use of the cryptocurrencies.

This Consultation Paper concerns entities engaging in the following activities/services in relation to cryptocurrencies:

- "*exchange between cryptocurrencies and fiat currencies;*
- *exchange between one or more forms of cryptocurrencies;*
- *transfer of cryptocurrencies;*
- *custodial and/or administrative services related to cryptocurrencies or instruments enabling control over cryptocurrencies;*
- *participation in and provision of financial services related to an issuer's offer and/or sale of cryptocurrencies*."

Additionally, this Consultation Paper concerns customers who are purchasing, holding or transferring cryptocurrencies.

In its Consultation Paper, CySEC, in line with ESMA's guidance on ICOs and Cryptocurrencies, has stressed that money laundering is one of the most significant identified risks. CySEC, like ESMA, is of the view that all cryptocurrencies and related activities should be subject to AML Law provisions.

CySEC contends that since launching the CySEC Innovation Hub, CySEC has been contacted by numerous entities engaging in cryptocurrencies, a number of which do not fall within the existing legal and regulatory framework. As a result, CySEC is of the view that it is imperative to proceed with the transposition of the parts of Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 (the "**AMLD5**") concerning the following activities:

- "*exchange services between virtual currencies and fiat currencies;*
- *the custodian wallet providers' activities.*"

CySEC, in its Consultation Paper, proposes the definition deriving from the AMLD5 and seeks consultation on the merits of creating an all-encompassing definition of "*virtual assets*", which would include the definition of "*virtual currencies*" as provided in the AMLD5 and the definition of the "*virtual assets*" as provided by the FATF.

CySEC has also proposed an extension of the scope of the AML Law to go beyond the provisions of the AMLD5 and include the following activities and services:

- "*exchange between crypto assets and crypto assets;*
- *transfer of virtual assets; and*
- *participation in and provision of financial services related to an issuer's offer and/or sale of a crypto asset.*"

Promotion and testing

CySEC has established an Innovation Hub to foster a better, more effective relationship between entities operating, *inter alia*, in the areas of cryptocurrencies and blockchain.

Further to CySEC's initiative to set up the Innovation Hub, the Cyprus government has also taken the first steps towards the implementation of blockchain technology in Cyprus, through the formation of an *ad hoc* working group.

Ownership and licensing requirements

There is no restriction on a party owning cryptocurrencies in Cyprus.

Mining

There is no specific restriction under Cyprus law.

Border restrictions and declaration

There is no specific restriction under Cyprus law.

Reporting requirements

Reporting requirements apply only to derivatives on cryptocurrencies.

Estate planning testamentary succession

The legislative framework in respect of estate planning and succession is not drafted in a way which allows clear conclusions as to the treatment of cryptocurrencies. We would expect that the treatment of cryptocurrencies would be the same as the treatment of any other movable property in Cyprus.

Subject to the provisions of EU Regulation 650/2012 (more commonly known as Brussels IV), Cyprus Cap 195 applies to the estate of any person deceasing as a domiciliary of Cyprus, and to all immovable property located in Cyprus. That is, Cyprus succession laws will apply to movable and immovable property of a person domiciled in Cyprus, and to Cyprus-*citus* immovable property irrespective of the deceased's domicile at the time of death.

Cyprus law provides for a form of forced heirship by which if a deceased leaves a spouse and child or spouse and descendant of a child or no spouse but a child or descendant of a child, then the disposable portion (i.e. that portion that the deceased can freely dispose of by will) must not exceed ¼ of the net value of the estate, the remaining "statutory portion" being due to the aforementioned close relative(s) of the deceased. Where the deceased leaves no spouse, child or descendant of a child, the rules of forced heirship do not apply and 100% of the estate of the deceased who is domiciled in Cyprus may be disposed of freely by will.

As a Member State of the European Union, EU Regulation 650/2012 (more commonly known as Brussels IV) was adopted on 4 July 2012 and applies to all deaths after 17 August 2015 in all EU Member States with the exception of the UK, Denmark and Ireland. Amongst other things, Brussels IV provides that:

- The default position is that the courts of the Member State in which the deceased was habitually resident have jurisdiction in succession matters (Article 21).
- The courts of the Member State of the deceased's nationality may have jurisdiction if the deceased chose to apply the law of the state of his nationality (Article 22).
- A European Certificate of Succession can be used to confirm the status and rights of beneficiaries and personal representatives (Article 62).

Karolina Argyridou
Tel: +357 2200 0408 / Email: karolina@veritalegal.com

Karolina graduated from the University of East Anglia with first class honours (LL.B.) and obtained her Master's in Law (LL.M.) from the London School of Economics and Political Sciences with distinction (Banking and Financial Regulation). Prior to setting up the firm, Karolina had spent several working as internal legal counsel to credit and financial institutions including Renaissance Capital, where she specialised in providing advice on banking law matters, financing structures, trading of claims of distressed assets and distressed debt, committed and uncommitted risk participations, investment and financial services legislation, capital markets, regulatory advice and advice on general corporate matters. Karolina has worked with government authorities on numerous projects for the drafting and transposition of major banking and financial services laws, and has advised on matters related to the NLP legal framework. Karolina also provides training to professionals on banking and financial services matters.
Karolina is a member of the Cyprus Bar Association.

Prodromos Epifaniou
Tel: +357 2200 0408 / Email: prodromos@veritalegal.com

Prodromos graduated from Aristotle University and subsequently obtained his Master's in Law from the University of Bristol (LL.M. in Commercial Law). Prodromos completed his pupillage with a Cyprus law firm and subsequently worked for various law firms and financial institutions in London such as Standard Chartered Bank and Skadden, Arps, Slate, Meagher & Flom LLP. Before joining K. Argyridou and Associates LLC, Prodromos worked for investment firms in Malta and Cyprus. Prodromos' main areas of practice are data protection and investment services. Prodromos advises various institutions and organisations on GDPR and MiFID II matters.
Prodromos is a member of the Cyprus Bar Association. Prodromos is also registered as a mediator in the Cyprus Registry of Mediators.

Akis Papakyriacou
Tel: +357 2200 0408 / Email: akis@veritalegal.com

Akis graduated from the University of Salford with first class honours (LL.B.) and obtained his M.Sc. from the University of Oxford (Corpus Christi). Akis attended the City Law School where he passed the Bar Professional Training Course (Very Competent). Following the completion of his studies, in 2016, Akis returned to Cyprus, completing his vocational training in one of the leading law firms, where he continued working after the completion of his training, specialising in corporate, banking and finance law, until September 2018 when he joined K. Argyridou & Associates LLC. Akis focuses on corporate, banking and finance transactions, with experience in both local and international finance transactions. His knowledge and expertise also extends to merger and acquisition transactions, corporate restructurings, employment law matters and fund-related matters.
Akis is a member of the Cyprus Bar Association.

Verita Legal K. Argyridou & Associates LLC

92 Ifigenias Street, Athena Building, 4th Floor, Nicosia 2003, Cyprus
Tel: +357 2200 0408 / URL: www.veritalegal.com

Estonia

Priit Lätt
PwC Legal Estonia

Government attitude and definition

Estonia continues to enjoy a reputation for being tech savvy, open to innovation and a jumping platform for globally successful tech disruptors like Bolt (formerly Taxify), TransferWise, Pipedrive and many others. *Wired* magazine has stated that Estonia is the "most advanced digital society in the world".

The most important Estonian state e-solution is called "X-Road" – the open-source backbone upon which Estonia's entire digital infrastructure runs, allowing the nation's various e-service databases, both in the public and private sector, to link up and operate in harmony. First put into practice in 2001 (it has been upgraded and altered many times since), X-Road is rooted in a blockchain – it lacks a centralised or master database, all information is held in a distributed data system and can be exchanged instantly upon request, providing access 24/7. Estonia is probably the only country in the world where 99% of public services are available online 24/7.

The Estonian government has been testing blockchain technology since 2008. Since 2012, KSI Blockchain technology, developed by Estonian-based company Guardtime, has been in production use in Estonian governmental data registries such as the national health, judicial and legislative systems, with plans to extend its use to other spheres such as personal medicine, cybersecurity and data embassies. Incidentally, KSI is used by NATO and the US Department of Defense.

Another thing that allows so much of Estonian life to be done "on the blockchain" is its use of verified digital identities. Nearly every one of the country's 1.3 million citizens has an ID card, which functions as much more than simply a driver's licence or passport. This eID uses a public key encryption and allows a person to be verified in an online environment. This is what allows a person digital access to things such as the voting system or the ability to fill a pharmaceutical prescription.

Estonia is also a pioneer in e-Residency, which enables people around the world to receive a virtual residency in Estonia, with access to the digital solutions provided by the government. As of 2019, there are almost 50,000 e-Residents.

In 2014, Estonian commercial bank LHV Pank developed and tested a blockchain-based financial product called CUBER (Cryptographic Universal Blockchain Entered Receivables) and a mobile app called Cuber Wallet. CUBER was meant to be a building block for various innovative financial products.

Estonia has already enacted specific anti-money laundering (**AML**)/counter-financing of terrorism (**CFT**) regulations applicable to services related to cryptocurrencies (custodian

wallet service and exchange service) since November 27, 2017. Thus, Estonia is the first EU Member State to follow the approach of the Fifth EU Anti-Money Laundering Directive (**5AMLD**).

Cryptocurrency regulation

Cryptocurrencies still do not possess a legal status of currency or money, but they can be accepted by natural and legal persons as a means of exchange or payment.

Estonia is the first EU country to provide clear regulation of cryptocurrencies, cryptocurrency exchanges and custodian wallet service providers for AML/CFT purposes by adopting the 5AMLD into the national legislation.

The definition and legal nature of cryptocurrencies (i.e., are they a right, thing or private money) in the civil law is unsettled, and there is no case-law on this subject in Estonia.

Sales regulation

In this section we shall address the sale of cryptocurrency tokens by companies during their professional activities.

In order to assess which laws apply to a certain cryptographic token sale, the type of token must be identified. There is no official regulation aimed at classification of crypto tokens; therefore it is advisable to involve a legal professional to provide a legal opinion on the classification of the respective token prior to initiating the sales process, as the results of the classification may considerably influence the legal obligations of the seller.

The Estonian Financial Supervision and Resolution Authority (**EFSA**) has published unofficial guidelines for ICO issuers and token traders on how to categorise crypto tokens issued in an ICO, and which laws apply to each category.[1] According to these guidelines, crypto tokens are divided into two: tokens that grant their owner a reasonable expectation for profit or governance rights (commonly referred to as security tokens); and tokens that do not promise any profits or monetary claims. The second group is further divided into three: cryptocurrency – payment instruments for products/services (Payment tokens); charity (Charity tokens); and tokens that grant access to a platform/system or a right to use a product/service (Utility tokens).

In order to receive feedback or discuss a specific ICO and the laws applicable to it, it is recommended to provide the EFSA beforehand with at least the following information:

- Name of the project for which funds are to be raised.
- Name and contact details of the project company/ICO organiser.
- Timeline of the project: timeline of fundraising, project implementation milestones.
- Description of the developed/offered product/service (main characteristics).
- Which investors does the ICO target?
- Will there be any restrictions for the investors?
- Which technological solutions will be used in the project/ICO?
- In which (virtual) currency and how is it possible to invest into the project?
- What is the volume of the ICO?
- How and where will the funds be allocated?
- Will a new token be created within the ICO? How?

- When and how is the token transferred to the investor?
- What are the characteristics and functions of the token?
- What rights does the token grant to the investor?
- How will compliance with the provisions of the AML/CFT regulations be ensured?
- How and where is it possible to sell or buy the token later?
- Can the token be used to buy products/services or to make payments to third persons?
- Does the token issuer plan to repurchase the tokens?

During 2018, 31 ICOs were closed in Estonia with a total of 323 million dollars raised.

Security tokens

The EFSA has explained that offering of tokens that fall under the definition of "security" as stipulated in § 2(1) of the Securities Market Act (**SMA**) brings legal obligations to the issuer/seller, infringement of which may result in considerable fines.

Pursuant to the § 2(1) of the SMA, each of the following applicable proprietary right or contract transferred on the basis of at least unilateral expression of will is a security, even without a document being issued therefor:

i) a share or other similar tradeable right;

ii) a bond, convertible security or other tradeable debt obligation issued which is not a money market instrument;

iii) a subscription right or other tradeable right granting the right to acquire securities specified in clauses i) or ii);

iv) an investment fund unit and share;

v) a money market instrument;

vi) a derivative security or a derivative contract;

vii) a tradeable depositary receipt; and

viii) greenhouse gas emissions for the purposes of the Atmospheric Air Protection Act.

In the context of crypto tokens, the most relevant definitions among these are i), ii), iv), v) and vi).

Tokens are *shares*, if they grant their owners rights to a holding in the company, rights to a share of profit, or voting rights in corporate matters. Under the Estonian Commercial Code (§ 148(5), § 226), shares grant shareholders: the right to participate in the management of the company and in the distribution of profit and of remaining assets on dissolution of the company; the right to participate in the general meeting of shareholders; and other similar rights prescribed by law or the articles of association.

Tokens are *investment fund units or shares* if they represent a unitholder's share in the assets of a common fund. According to the Investment Funds Act, a *common fund* is a pool of assets which is established from the money collected through the issue of units or other assets and assets acquired through investment of money, and which is jointly owned by unitholders. An *investment fund* is a legal entity or pool of assets, which involves the capital of a number of investors with a view to investing it in accordance with a defined investment policy for the benefit of the investors in question and in their common interests.

According to § 2(2) of the SMA, a *money market instrument* is an unsecured, transferable and marketable debt obligation, which is traded on the money market, including a treasury debt obligation, commercial paper, certificate of deposit, bill of exchange secured by a credit

institution, or other security complying with the aforementioned characteristics, stipulated in Regulation 2017/565 (EU) of the European Parliament and of the Council[2] (EU 2017/565) article 11. According to the aforementioned regulation, the money market instruments shall have the following characteristics: (a) they have a value that can be determined at any time; (b) they are not derivatives; and (c) they have a maturity at issuance of 397 days or less.

According to § 2(3) of the SMA, a *derivative instrument* is a tradeable security expressing a right or obligation to acquire, exchange or transfer, the underlying assets of which are securities, or the price of which depends directly or indirectly on: (a) the stock exchange or market price of the security; (b) the interest rate; (c) the securities index, other financial index or financial indicator, including the inflation rate, freight rate, emission allowance or other official economic statistics; (d) currency exchange rates; (e) credit risk and other risks, including climatic variables; or (f) the exchange or market price of a commodity, including precious metal.

The EFSA's position seems to be that the tokens do not have to correspond to these definitions literally in order to be regarded as securities, rather it is sufficient if the token has the overall characteristics of a security (substance-over-form approach). If the token corresponds to any of these characteristics, the offering of it may constitute the issuance of securities and, depending on its exact nature, be governed by the rules of public offering as prescribed in § 12 of the SMA. That being the case, it is required to register a respective prospectus at the EFSA.

The issuance will not be regarded as a public offering and no prospectus is required in the case of:

- an offer of securities addressed solely to qualified investors;
- an offer of securities addressed to fewer than 150 persons per Contracting State, other than qualified investors;
- an offer of securities addressed to investors who acquire securities for a total consideration of at least €100,000 per investor, for each separate offer;
- an offer of securities with a nominal value or book value of at least €100,000 per security; or
- an offer of securities with a total consideration of less than €2,500,000 per all the Contracting States in total, calculated in a one-year period, of the offer of the securities.

As of July 2019, there have not yet been any security token public offerings (**STO**) in Estonia. However, according to EFSA, there has been considerable interest to for conducting STOs in Estonia.

Payment tokens

According to the EFSA guidelines, tokens shall be considered as payment tokens if they are also intended for use outside of the respective token issuer's platform as payment instruments for other products and services provided by third persons. Payment token directly corresponds to the concept of "virtual currency" as defined in § 3(9) of the Money Laundering and Terrorist Financing Prevention Act (please see below). Such tokens do not give rise to any claims on their issuer.

Issuing or selling payment tokens to the public may fall under the definition of provision of the custodian wallet service according to the Money Laundering and Terrorist Financing Prevention Act (please see below) and thus the issuer should follow at least the due diligence measures provided in this legal act.

Charity tokens

According to the EFSA guidelines, a fundraising for the development of a business project shall be considered as a donation only under the condition that it does not lead to: (i) a participation in the issuer; or (ii) any obligation to repay the funds, interest, dividend, or any other repayment, or cash flow. In addition, no right of use of a service or product shall arise in connection with the donation.

If the issuer is gathering donations in exchange to tokens, the issuer must expressly indicate that the token is a charity token. In such a case, the issuer will only have certain taxation obligations.

Utility tokens

According to the EFSA guidelines, an ICO, where the tokens offered grant their purchasers access to a product or service, is in essence a prepayment for a product or service. Consequently – taking into account that the contracts entered into within an ICO use means of communication (a computer network) – such ICOs are subject to the provisions of the Law of Obligations Act regarding the distance contracts entered into through means of communication and computer network.

Utility tokens are essentially commodities and the usual contractual obligations apply. Additionally, various consumer protection obligations must be met if the buyers are natural persons, such as the notification obligation and the obligation to allow the consumer to withdraw from the contract with simplified procedure.

Taxation

Estonia has not enacted any specific tax regulation on ICOs or cryptocurrencies. Estonian tax legislation does not include any special tax rules for income, profits or gains arising from transactions involving cryptocurrencies, or for charges made in connection with cryptocurrencies. Still, Estonian tax authorities have issued formal guidance in relation to VAT and income tax treatment of cryptocurrencies and mining.

Value added tax (**VAT**)

For the purposes of VAT, cryptocurrencies are considered the same as currency such as euros, etc. Thus, the usage of cryptocurrencies as remuneration is equal to the usage of legal tender and therefore out of the scope of VAT.

The supply of services which consist of the exchange of traditional currencies for units of cryptocurrencies and *vice versa* are financial transactions exempt from VAT. This approach is in line with ruling C-264/14 of the European Court of Justice.

The services provided by miners are outside the scope of VAT. However, it is still unclear how the VAT treatment of the mining changes if a pool is used.

Estonian tax authorities have not yet clarified VAT treatment of wallet service providers.

The standard VAT rate is 20%.

Corporate income tax

Estonia uses a distinctive corporate tax system in which the taxation of corporate profits is deferred until the profits are distributed. Any retained earnings are thus effectively tax-exempt as long as the shareholder(s) can defer profit distributions. Such exemption covers both active and passive types of income.

Corporate profits are subject to taxation upon distribution of dividend or other types of deemed or hidden profit distribution (e.g., liquidation proceeds, capital redemptions, representation expenses, gifts and donations, non-business-related expenses, transfer pricing adjustments).

Distributed profits are generally subject to 20% corporate income tax (20/80 on the net amount of the profit distribution). For example, an Estonian company that has profits of €100 available for distribution can distribute dividends of €80, on which it must pay corporate income tax of €20. Thus, the proceeds from an ICO are not taxed with corporate income tax at the rate of 20/80 until such proceeds are distributed to the shareholder(s).

From 2018, the corporate income tax rate on regular dividends was reduced from 20% to 14% over an ongoing three-year cycle. According to the new rule on regular profit distributions, the payment of dividends in an amount which is below or equal to the amount of average taxed dividends paid during the three preceding years, will be taxed at a rate of 14% (the tax rate on the net amount being 14/86 instead of the regular 20/80). In cases where the recipient of the 14% dividend is either a resident or non-resident individual, a 7% withholding tax rate will apply unless a tax treaty provides for a lower withholding tax rate (5% or 0%). There are also transitional rules. 2018 is the first year to be taken into consideration for the purposes of determining the average dividend.

Personal income tax

For personal income tax purposes, cryptocurrency is treated as property, the alienation and exchange of which gives rise to capital gains. Income from trading in cryptocurrencies is taxed as business income which, in addition to personal income tax, is also subject to social security contributions.

Income received will be taxed at a 20% flat tax rate.

Employee compensation tax issues

It is rather common that employees recruited early on may receive a certain amount of their yearly salary in the form of cryptocurrencies as a means of compensation and encouragement. Such compensation in non-monetary form should be taxed as fringe benefits under Estonian legislation.

Fringe benefits are any goods, services, remuneration in kind or monetarily appraisable benefits which are given to a person in connection with an employment or service relationship, membership in the management or controlling body of a legal person, or a long-term contractual relationship, regardless of the time at which the fringe benefit is granted.

Fringe benefits are subject to 20/80 income tax and 33% social security contributions (on a gross-up basis). The employer must calculate the tax on the total amount of all fringe benefits granted. The tax base for social security contributions purposes includes both the value of the benefit and the income tax paid on this benefit. Fringe benefits received by resident employees are not included in the taxable income in their annual income tax returns.

*Example: where the market value of the fringe benefit is **100**:*

*Income tax due is 25 (20/80 * 100) and social security contributions due is 41.25 (0.33 * (100+25)) = **total tax of 66.25***

Money transmission laws and anti-money laundering requirements

Before 5AMLD, EU financial authorities emphasised that exchanges where virtual currencies are traded and digital wallets used to hold, store or transfer virtual currencies are

unregulated under EU law. However, Estonian regulated virtual currency exchanges already under the AML law, which was in force as from January 2008 until November 27, 2017 (**please see remarks below**). Estonia implemented the 4AMLD (2015/849) and draft 5AMLD (2018/843) into its national law (Money Laundering and Terrorist Financing Prevention Act, **MLTFPA**) on November 27, 2017.

MLTFPA, among other changes, introduced new definitions and provided a clear new regulation for cryptocurrency exchanges and cryptocurrency wallet service providers.

According to MLTFPA:

- *'Virtual currency' means a value represented in digital form, which is digitally transferable, preservable or tradeable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of PSD2 or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive*. It is interesting that the definition in MLTFPA is narrower than the one in 5AMLD. The latter makes it clear that virtual currencies may also be used for other different purposes and find broader applications such as means of exchange, investment, store-of-value products or uses in online casinos.
- *'Virtual currency wallet service' means a service in the framework of which keys are generated for customers or customers' encrypted keys are kept, which can be used for the purpose of keeping, storing and transferring virtual currencies*. This definition is a rather broad one, but it should not extend to non-custodian wallets, where the user (rather than the wallet provider) holds the private key. Thus, if the private key to the cryptocurrency is (also or exclusively) held by the wallet provider, the wallet service provider should be regarded as an obliged entity.
- Providing only exchange of cryptocurrency to cryptocurrency will remain out of scope of the regulation.

According to MLTFPA, an appropriate authorisation must be granted by the Financial Intelligence Unit (**FIU**) to:

a) provide a service of exchanging a virtual currency against a fiat currency; and

b) provide a virtual currency wallet service.

The application for authorisation can be submitted in the Register of Economic Activities accessible through the portal www.eesti.ee, or the webpage at https://mtr.mkm.ee. As of July 2019, the state fee payable for the authorisation is €345. The Financial Intelligence Unit reviews the authorisation application no later than within 30 working days following the date of submission of the application. Prior to the grant of the authorisation, no services shall be offered.

Please note that the rules of operating in the relevant fields of activity subject to authorisation obligation have not been harmonised across the EU. An activity licence granted in another state of the European Economic Area does not grant the right to operate in Estonia, and *vice versa*.

In addition to authorisation, obliged entities under the MTFPA are required to perform AML/CFT due diligence measures in respect of their clients, including identification, verification obligations and monitoring of each of the business relationships.

The main area that will create a struggle for crypto-businesses in Estonia is the banks, i.e. opening a bank account and operating payments, as the banks are quite sceptical when it

comes to cryptocurrency. In order to at least have a chance to open a bank account, a clear and transparent business model, transparent identity of the company (group structure/shareholders, etc.), and effective AML/KYC procedures need to be in place. Therefore, the non-regulated cryptocompany should contact its co-operations partners who are obliged persons under MLTFPA (e.g. banks) in advance to ensure that the company can comply with their internal regulations and requirements.

During 2018, the FIU received in total 1,182 applications for virtual currency wallet service and virtual currency exchange service authorisations. Of these 1,182 applications, 1,124 applications were granted. In the first four-and-a-half months of 2019, the FIU has already issued 427 authorisations.

Remark – Estonian case law

In early 2014, the proprietor of Bitcoin trading platform BTC.ee, Otto de Voogd, was ordered by the Estonian Financial Intelligence Unit of Estonia's Police and Border Guard to provide information on all of his clients. The operations of the Estonian version of the site were halted in February 2014, and de Voogd began legal proceedings against FIU in Estonian courts.

Finally, his appeal in cassation was assessed in the country's Supreme Court. The Supreme Court ordered Estonia's Ministry of Finance, Ministry of Interior, the Bank of Estonia and the Financial Supervision Authority to give opinions on the legality of Bitcoin and on de Voogd's case, specifically on the following: whether Bitcoin trading is under the jurisdiction of Estonian AML/CFT regulations and whether Estonian law on money laundering and terrorist financing is in conformity with the EU law (3AMLD) and with the recommendations of FATF, and whether Bitcoin exchange providers are "alternative mean of payment service providers" as defined by the Estonian AML/CFT law effective in 2014.

On April 11, 2016, the Supreme Court confirmed that Bitcoin exchanges are subject to Estonian AML/CFT regulation and supervision as "alternative means of payment service providers"; in particular, the requirement to identify clients where the client turnover is over €1,000 per month. This important ruling clarified the vague definition of "providers of alternative means of payment", and affirmed the applicability of traditional AML/CFT regulations to innovative business models such as crypto exchanges if they operate in Estonia.

Remark – planned amendments

On May 2, 2019, the Estonian Government approved the draft act on Amendments to the MLTFPA. The purpose of the amendments is to strengthen the competence of the Financial Intelligence Unit in the authorisation process and in the exercise of supervision, and to lay down additional requirements for the application for an authorisation for providers of virtual currency services. The measures taken to mitigate the risks associated with these service providers would enable greater control of these areas of activity and not to authorise such companies that do not actually operate in Estonia. For example, the FIU, while processing authorisation applications, will examine: the background and suitability of board members of companies; the registered address, location of the board and the permanent establishment of the company must be in Estonia; if the company is from a different country, it will have to open a branch in Estonia in order to apply for an authorisation. In addition, the amendment increases the state fee for issuing an authorisation from €345 to €3,300, and the process of granting an authorisation or refusing to do so increases from 30 working days to three months.

The draft act has passed the first reading in parliament. However, private sector organisations have voiced their concern with regards to the draft act and suggested several amendments. Should the draft act pass, those companies that already have an authorisation are given time to bring their activities into line with the new requirements.

Promotion and testing

Advertising

When advertising an ICO, it is important to carefully consider the use of terms in the advertisement and the general requirements for advertising stipulated in the Chapter 2 of the Advertising Act. The advertising must provide a clear and true presentation of the product or service to the persons targeted. In particular, advertising must not be misleading concerning the characteristics of the offered product or service. For example, advertising something as an investment service could be unlawful without the required authorisation. Thus, a utility token must not be advertised as an investment or an investment object.

Public sector

To date, Estonia has no official, state-backed promotional or testing programmes or policies intended for the promotion of cryptocurrencies and blockchain technologies. This, however, does not mean that the state authorities are totally passive or oblivious about the benefits and the need to create appropriate conditions for these technologies, in order to gain competitive advantage over other states that wish to stand out and direct crypto-related capital to their jurisdiction. In the past, Estonia has always been very competitive when it comes to gathering recognition with its innovation and technology-friendly approach and legal atmosphere, and this was also the case with blockchain-related technologies at first.

After the 2019 Parliament elections, the new government coalition stated in its action programme that they will analyse the necessity of regulating crypto assets.[3] However, currently Estonia has no official policy on promoting and regulating cryptocurrencies or blockchain technologies at the government level.

Private sector

One of the most visible private sector organisations when it comes to promoting and raising awareness of blockchain technologies and cryptocurrencies is the Estonian Cryptocurrency Association.[4] Established in October 2014, the Association is a non-profit organisation, the purpose of which is to promote more widespread use of cryptographic resources and make the Estonian cryptocurrency regulatory environment more attractive to investors and crypto-enthusiasts. The Association organises workshops and training on blockchain technologies, instructs people interested in cryptocurrencies, and acts as the main and most active interest group engaging in discussions with the government, and supervisory and regulatory bodies.

In addition, FinanceEstonia,[5] a public-private cluster initiative with the aim of establishing Estonia as a vibrant and innovative location for financial services, has taken an active role in developing the best practices for crypto finance and most efficient AML/CFT regulations for crypto businesses.

Ownership and licensing requirements

Specifically for the purposes of cryptocurrencies, there are no restrictions on investment managers owning cryptocurrencies for investment purposes, nor are there any licensing requirements imposed on someone who holds cryptocurrency as an investment advisor or fund manager under Estonian legislation. However, if the crypto asset in question were to

be classified as a security token (see above), the same restrictions to ownership of the respective token would apply as for investment managers and advisors providing services in the field of the stock market. These restrictions include the obligation to avoid conflict of interest that, in some cases, could mean restrictions on ownership of certain security tokens.

Mining

Mining is permitted, but Estonia has not enacted any specific legal or tax regulation on mining activities.

EFSA has stated that mining cryptocurrency as a field of activity does not fall under the supervision of the Authority.

When a new block is created by the requisite unique identification process and verification by the network, the miner gets rewarded. In this regard, there is no contractual relationship with the miner and there is no supply for consideration for VAT purposes when the reward is granted. Therefore, there does not seem to be a supply for VAT purposes, and the mining of cryptocurrency is outside the scope of VAT.

If a private person is independently engaged in virtual currency mining or data processing and income tax has not been withheld, the private person has to declare such income as business income and pay taxes based on the income tax return.

A person who permanently mines cryptocurrency has to register as a sole proprietor in the Business register. A registered sole proprietor may declare expenses (e.g. equipment) related to business and deduct them from business income. Income tax, social tax and contributions to the mandatory funded pension must be paid on the net income from business according to the income tax return.

Border restrictions and declaration

To date, there are no border restrictions or obligations to declare cryptocurrency holdings pursuant to Estonian legislation.

Reporting requirements

Estonian legislation does not stipulate reporting obligations to individuals making payments in excess of a certain value.

However, obliged entities under applicable AML/CFT regulation have the obligation to monitor the business relationships with their clients in order to identify activities that could indicate suspicious money laundering-related activities. In some cases, large transactions may be considered indications of such suspicious activities, especially if it is uncharacteristic of the usual transactions by the specific client. When the obliged entity identifies suspicious activities that could relate to money laundering or terrorist financing, it should notify the Financial Intelligence Unit.

Estate planning and testamentary succession

Cryptocurrencies are not treated differently from ordinary assets for the purposes of estate planning and testamentary succession under Estonian legislation.

* * *

Endnotes

1. Available online: https://www.fi.ee/en/investment/aktuaalsed-teemad-investeerimises/virtuaalraha-ico/information-entities-engaging-virtual-currencies-and-icos.
2. Available online: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0565&qid=1515161142376&from=ET.
3. Governmental action plan for 2019-2023, available at: https://www.valitsus.ee/sites/default/files/content-editors/valitsus/RataseIIvalitsus/vabariigi_valitsuse_tegevusprogramm_2019-2023.pdf.
4. Please see: https://www.kryptoraha.ee/.
5. Please see: http://www.financeestonia.eu/.

Priit Lätt, Partner
Tel: +372 511 9268 / Email: priit.latt@pwc.com

Priit Lätt, attorney-at-law, heads the intellectual property/IT, public procurement and tax litigation practices at PwC Legal in Estonia.

Priit is a renowned specialist in IP, IT (including cryptocurrencies and crypto finance), tax and public procurement law, representing and advising Estonian and international companies and public institutions. Priit also has significant experience in representing clients in complex disputes which have created precedents at the Supreme Court, including the constitutional review chamber. Among other things, Priit has represented a client in Estonia's biggest software dispute and in Estonia's first Bitcoin-related regulatory lawsuit. Priit also successfully represented a client in a trademark dispute, in which the Supreme Court declared several provisions of the Code of Civil Procedure and Government Regulations that established limits to legal fees in civil disputes, as invalid and unconstitutional. Priit has advised several ICOs and launches of innovative blockchain projects.

Priit participated as the only attorney in a public and private sector work group, which for the first time in Estonia developed a recommended standard contract for the public procurement of software development.

Major international legal publications (e.g., *Chambers*, *The Legal 500*, *WTR1000*) have repeatedly identified Priit as one of top attorneys in the practice areas of IP, IT and tax law.

Priit is the founder of Estonian Cryptocurrency Association (2014) and has been a long-term member of its management board. In addition, he gives lectures on cryptocurrencies and ICOs at the University of Tartu and numerous crypto conferences.

Priit has been a member of Estonian Bar Association since 2001 and he is also a member of the IP/IT commission of the Estonian Bar.

PwC Legal Estonia

Pärnu mnt 15, 10141 Tallinn, Estonia
Tel: +372 6141 858 / URL: www.pwclegal.ee

France

Christophe Perchet, Juliette Loget & Stéphane Daniel
Davis Polk and Wardwell LLP

Government attitude and definition

Over the past few years, France has been at the forefront of the blockchain revolution in the European Union ("**EU**"), while the French Government has gradually established a favourable legal framework for initial coin offerings ("**ICOs**"), in collaboration with various players in the French crypto ecosystem.

As early as April 2016, France became the first country to recognise blockchain technology in the field of cash vouchers, also called "*minibons*", a particular type of promissory note primarily used in crowd-lending transactions, by allowing issuers to register *minibons* directly into the blockchain.

In October 2017, the French Financial Market Authority (the "**AMF**") launched a unique "digital-asset fundraising support and research programme" named UNICORN (for "Universal Node to ICO's Research & Network"), to support and analyse ICOs, which operates similarly to a "sandbox" programme (see **Promotion and testing**, below).

In December 2017, France adopted a specific ordinance to become the first country to authorise the registration and transfer of unlisted securities through the use of blockchain technology.

In March 2018, Bruno Le Maire, the French Minister of the Economy, declared that he wanted Paris to become the capital of ICOs, through the implementation of a very innovative optional legal framework governing ICOs. Following this announcement, the French Strategy and Prospective General Commission ("*France Stratégie*") published a report, in June 2018, relating to blockchain and cryptocurrencies and proposing several reforms to enable the sound development of this technology in France.

In December 2018, France adopted a decree implementing the specific conditions under which unlisted securities may be registered and transferred using blockchain technology, thereby paving the way for the development of security tokens offerings in France.

In terms of personal taxation, following a decision rendered in April 2018 by France's highest administrative court (*Conseil d'état*) which lightened the tax burden on profits resulting from cryptocurrency transactions, the 2019 Finance Act introduced an even more favourable flat-tax rate of 30% (including social contributions) (see **Taxation**).

In April 2019, in line with the feedback received following a public consultation on ICOs and crypto-assets launched by the AMF, the draft "Pacte" bill (the "**Pacte Act**") finally established an innovative *ad hoc* legal framework governing ICOs and digital assets services providers (see **Sales regulation**).

In short, the French Parliament has adopted a favourable legal framework, and France currently stands out in the European Union as a "blockchain/crypto-friendly" jurisdiction, through a "soft touch" approach favouring innovation and entrepreneurial projects.

This friendly position does not mean that France considers cryptocurrencies (none of which are backed by the French Government or the European Central Bank) as "real money" or otherwise gives them equal standing with domestic or foreign fiat currencies. In March 2018, the French Central Bank (*Banque de France*) published a paper regarding the main issues, risks and perspectives raised by Bitcoin and other cryptocurrencies, in which it focuses on the reasons why "cryptocurrencies" cannot be qualified as such. As a result, the French Central Bank considered the term "cryptocurrency" to be unsuitable and that the term "crypto-asset" would be preferable instead. Following such publication, the French regulatory authorities have started using the words "crypto-asset" or "digital asset", delineating the fundamental difference to "real money" or "fiat currencies".

In particular, the French Central Bank explained that "crypto-assets" do not fulfil the customary roles of fiat currencies because: (i) they are too volatile to be used as "units of account" (*unité de compte*); (ii) they are not as efficient as fiat currencies (they are difficult to use, there are high transaction fees and there is no guarantee against fraud); and (iii) they have no intrinsic value and hence cannot be used as safe reserves.

The French Central Bank also emphasised that, pursuant to the French financial and monetary code, the only currency in France is the Euro and therefore "crypto-assets" may not be considered as either a means of payment or electronic money under French law. This is logical given that "crypto-assets" are not issued against a cash deposit. As a result, under French law, it is impossible to require someone to accept "crypto-assets" as payment, and "crypto-assets" do not carry a repayment guarantee at any time and at face value in the event of unauthorised payment, in each case in contrast to fiat currencies.

In this article, the word "crypto-assets", which is the term used by the French regulators, will be used instead of "cryptocurrencies", other than in the titles.

Cryptocurrency regulation

As discussed below (see **Sales regulation**), with the enactment of the Pacte Act, France has decided to implement specific regulations governing crypto-assets that do not constitute financial instruments. Unless crypto-assets fall within the previously existing legal framework governing securities offerings and trading, and in accordance with an analysis to be made on a case-by-case basis depending on the rights and obligations conferred, crypto-assets now fall under the optional regime for public offerings of tokens established by the Pacte Act and the related regulation applicable to the secondary market.

Sales regulation

In October 2017, in view of regulating fundraising activity based on crypto-assets and blockchain technology, the AMF launched (i) a public consultation on ICOs to gather the views of stakeholders on the different means of supervision, and (ii) a "digital-asset fundraising support and research programme" to support and analyse these transactions, named UNICORN.

At the time of this consultation, the AMF carried out an initial high-level study of these transactions and their legal implications and found that while some of the ICOs identified may fall within existing legal provisions (such as the regulation applicable to intermediaries

in miscellaneous assets, the public offering of financial instruments, or managers of alternative investment funds), most of these issuances would actually fall outside of the scope of any regulation.

According to the AMF, this analysis must be made on a case-by-case basis depending on the rights and obligations attached to each crypto-asset. In particular, if such rights and obligations prove to be close to those of a security, *i.e.* because they carry financial and/or political rights, such as dividend and/or voting rights, respectively, the AMF may qualify such crypto-asset as a security. In this case, the sale of such crypto-asset would have to comply with French securities laws, including notably the obligation to publish a prospectus under certain conditions.

Given such uncertainties for issuers, the AMF proposed three options for the supervision of future ICOs: (i) promote best practices without changing existing law; (ii) extend the scope of existing law to treat ICOs as public offerings of securities; and (iii) propose an *ad hoc* regime adapted to ICOs.

In February 2018, the AMF published a summary of the responses received following the public consultation on ICOs, pursuant to which a large majority of respondents expressed strong support for the establishment of an appropriate legal framework for this new type of fundraising method.

Taking these answers into consideration, the Pacte Act adopted by the Parliament on April 11, 2019 introduced this new legal framework. The Pacte Act was reviewed and approved by the French Constitutional Court (*Conseil constitutionnel*), promulgated by the French President and then published in the Official Journal (*Journal Officiel*). The Pacte Act came into force on May 24, 2019 and the provisions relating to crypto-assets are currently applicable.

This framework comprises an optional visa for ICOs open to companies established or incorporated in France wishing to ensure that their contemplated ICO is fully compliant with French law and, in particular, will not be subject to the regime applicable to financial instruments.

Under this new legal framework, issuers are free to decide whether to implement a regulated ICO, subject to the AMF approval, or to proceed without the French regulator's approval. In order to obtain the AMF visa, issuers have to comply with the obligations below provided by the Pacte Act:

- the issuers shall be legal entities established or incorporated in France;
- the issuers shall provide their subscribers with an information document containing any relevant information about the offering, the issuer, the rights attached to the tokens, the underlying project and its related risks, with such information being accurate, clear and not misleading; and
- the issuers shall set up the means to monitor and secure the assets collected as part of the offering, in compliance with the rules on anti-money laundering combating financing terrorism ("**AML/CFT**") and know your customer ("**KYC**").

The provisions described herein are supplemented and clarified through amendments to the General Regulations of the AMF which have been approved by the French Government's decree dated May 27, 2019. The implementing regulations include the following provisions:

- The AMF will have 20 days from receipt of a completed application to decide whether or not to grant its visa. The visa is granted to one offering only and will be effective for the duration of the relevant offering, which may not exceed six months.

- The information document must include, at a minimum: (1) a description of the token offering, the issuer, the rationale for the token offering and the intended use of the proceeds raised in the offering; (2) a description of the rights attached to the tokens and the conditions and the means to exercise those rights; (3) a description of the terms of the offering (*i.e.* number of tokens to be issued, subscription terms, soft cap and hard cap); (4) the technical details of how the offering will be performed; (5) a description of the main characteristics of the issuer and the persons involved in the structuring and development of the project; (6) the key risks associated with the issuer, the tokens, the offering and its achievement; and (7) an indication of the accounting treatment for the tokens issued and whether the issuer is or intends to be accompanied by a statutory auditor.
- The information document must also include (1) a disclaimer on the scope of the AMF visa and the limited nature of its review, as well as (2) a global warning with respect to the inherent risks associated with any investment in an ICO, which must also be included in any promotional communications.
- Issuers may optionally attach to the information document the source code for the issuance (*i.e.* a computer program containing the instructions to execute the issuance) or conduct an audit of such source code and describe its conclusions.
- Issuers must inform the subscribers of any fact or change likely to have a significant impact on their investment decision that arises after delivery of the visa but before the closing of the offering. However, no right of withdrawal is granted to them in such cases.
- With regard to the means set up to monitor and secure the assets collected as part of the offering, issuers must offer sufficient guarantees in terms of reliability, operability and efficiency. In this respect, the AMF has given three examples of solutions that it considers satisfactory, through the implementation of (i) an escrow agreement with a professional, (ii) a multiple signature system, or (iii) a smart contract.
- Within two business days following completion of the offering, the issuer is required to publish a press release setting forth the results of the offer, the contents of which will be specified in an AMF instruction to be published in due course.

In order to ensure complete transparency and publicity of this optional visa, the AMF will make public a "white list" of approved ICOs. Such an initiative is likely to promote the development of ICOs: this institutional endorsement will encourage new issuers to launch their offerings and potential investors to subscribe to such offerings.

However, the EU may cast a shadow over such an innovative approach. On November 13, 2017, the European Securities and Markets Authority ("**ESMA**") published a warning to companies involved in ICOs as issuers on the potential qualification that crypto-assets could receive, pursuant to which these companies could be involved in offering "transferable securities" to the public. Such qualification would trigger the application of certain EU securities laws and regulations, such as the Prospectus Directive/Regulation, the Markets in Financial Instruments Directive ("**MiFID**"), the Alternative Investment Fund Managers Directive and the fifth Anti-Money Laundering Directive. ESMA has not published any further information regarding the qualification of crypto-assets.

On October 19, 2018, the Securities and Markets Stakeholders Group ("**SMSG**") published a report on ICOs and crypto-assets advising ESMA on the steps that should be taken to mitigate the risks of ICOs and crypto-assets, especially for investors. The SMSG urged

ESMA to (i) provide guidelines on the interpretation of the MiFID definitions of "transferable securities" and "commodities" in order to achieve supervisory convergence, (ii) send a letter to the European Commission asking it to consider adding tokens used as investment products to the MiFID list of financial instruments, and (iii) provide guidelines for national authorities operating or wishing to operate a sandbox or innovation hub.

Taxation

In December 2018, the French National Accounting Standards Authority (*Autorité des normes comptables* or "**ANC**") released specific public guidance clarifying the accounting and tax treatment of ICO proceeds in France. For taxation purposes, a distinction should be made between the rules governing token issuers and those applying to subscribers.

The accounting treatment of ICO proceeds depends on the rights and obligations attached to the tokens offered, and accordingly may be registered under three different accounting categories. In all cases, the tokens are registered on their issuance date for their subscription price. As a result, the tax treatment of ICO proceeds would be as follows:

- the proceeds from tokens registered under "debt and other liabilities" (*emprunts et dettes assimilées*) shall not be subject to corporate tax;
- the proceeds from tokens registered under "deferred revenues" (*produits constatés d'avance*) shall be subject to corporate tax as revenues are gradually recorded, which results in taxation being phased over several years; and
- the proceeds from tokens registered under "revenues" (*produits*) shall be subject to immediate taxation under corporate tax.

For profits made in 2019, the rate of French corporate tax is 28% up to profits of €500,000 and 31% above this amount plus surtaxes of 3.3%. Such French corporate tax will be progressively reduced to 25% plus surtaxes in 2022. Such tax is payable upon closing of the financial year during which the ICO has been completed (*i.e.*, between 1 and 12 months following the ICO in most cases, and up to 18–24 months following the ICO for a newly incorporated ICO issuer).

Under the same interpretation, the sale of cryptocurrencies would qualify as a "sale of goods and/or services" under Directive 2006/112/EC on valued-added tax ("**VAT**"), transposed into each EU country's domestic law, and therefore the sale of crypto-assets to EU purchasers will be subject to VAT, the rate of which is currently 20% in France. Note, however, that the above-mentioned treatment does not apply to cryptocurrencies which qualify or could be qualified as "security tokens", which are subject to the tax regime applicable to the sale of securities, *i.e.* subject to registration fees only (at a 0.1% rate) and excluded from VAT.

With respect to personal taxation, the 2019 Finance Act introduced a *sui generis* flat rate tax of 30% (including social contributions) on capital gains realised by individuals upon the occasional purchase/sale of crypto-assets. This rate is the same as the one that applies to securities' capital gains (dividends, shares, etc.). In addition, under this new regime, the trade of one crypto-asset against another crypto-asset is considered as a simple non-taxable interlayer transaction. Any losses incurred may only be offset against capital gains of a similar nature recorded within the same year.

However, certain gains are excluded from this tax treatment and therefore remain subject to income tax, the rate of which is currently up to 45% (plus social contributions which are currently set at 17.2%). These include:

- gains resulting from the taxpayer's participation in the creation and functioning of the bitcoin system, *i.e.* gains resulting from "mining" activities; and

- gains resulting from the recurring acquisition and sale of bitcoins, thus materialising the existence of a commercial activity, *e.g.* gains resulting from professional trading activities.

Money transmission laws and anti-money laundering requirements

In March 2018, the French Central Bank (*Banque de France*), together with the French Prudential Authority (*Autorité de contrôle prudentiel et de résolution* or "**ACPR**"), proposed the introduction of a new status for providers of services related to crypto-assets, as well as new obligations on such providers with respect to the security of transactions and the protection of their clients. The French Government followed their recommendation and established a new regulatory framework for "digital assets services providers" (*prestataires de services sur actifs numériques* or "**DASPs**") through the Pacte Act.

Digital assets services comprise the following:

1. custody of private cryptographic keys for third parties;
2. trade of digital assets with fiat currencies;
3. trade of digital assets with other digital assets;
4. operation of a digital assets trading platform; and
5. (i) receipt and transmission of orders on behalf of third parties, (ii) portfolio management on behalf of third parties, (iii) investment advice to digital assets purchasers, (iv) underwriting of digital assets, and (v) making guaranteed and non-guaranteed investments in digital assets.

In order to provide the services mentioned in points 1 and 2 above, the service provider must be registered with the AMF as a DASP and be subject to the approval of the ACPR. The exercise of these services is prohibited for any unregistered person. The AMF will assess in particular the reputation and professional qualifications of the directors and beneficial owners of the relevant DASP and will verify that they have adequate AML/CFT procedures in place, as described below.

In addition, any service provider that performs one (or more) of the services listed above may or may not decide to apply for an optional visa from the AMF. To obtain this quality label, DASPs will have to obtain professional liability insurance (or comply with the capital requirements set forth in the General Regulations of the AMF), implement adequate security procedures, an internal control system and conflict check policies and establish a resilient IT system.

Once DASPs are approved by the AMF, they must comply with a set of obligations that depend on the type of services provided. The AMF will publish the list of registered providers and the list of approved DASPs and the services they are approved to provide.

A decree of the French Government and amendments to the General Regulations of the AMF to be published in due course will provide the definitions of each service, the registration conditions, the common conditions for performing one or more services, the common approval conditions and the specific approval conditions for each of the services.

Until the entry into force of the Pacte Act, compliance with France's anti-money laundering ("**AML**") rules, including the related KYC requirements, was only required for platforms converting fiat currencies into crypto-assets or vice versa (thereby acting as an intermediary between the purchaser and the seller).

In May 2018, the EU Member States adopted an amendment to Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the "**AML Directive**"), to subject crypto-asset exchange platforms and custodian wallet providers to the AML and terrorism financing obligations (in particular to KYC obligations), in line with traditional financial intermediaries. This amendment did not impact French law since French crypto-asset/fiat exchange platforms were already subject to AML requirements and KYC obligations. However, the amendment to the AML Directive extended these obligations throughout the EU, thereby ensuring the implementation of adequate safeguards and making it impossible for players to perform regulatory arbitrage on this basis within the EU.

Since the Pacte Act became applicable, compliance with AML and KYC requirements is necessary to obtain an optional visa for ICOs. Moreover, DASPs providing the above-mentioned services in points 1 and 2 and all those applying for the visa from the AMF, on a voluntary basis, have to comply with AML and KYC requirements. These requirements are therefore applicable to both primary and secondary markets.

Under French and EU law, the AML requirements primarily cover the following:

- *customer due diligence obligations*: platforms are required to verify the identity and, in certain cases, the "effective beneficiary", *i.e.* the actual individuals behind a legal entity, whether it is a company, a foundation or a trust, and the origin of the money used throughout the platforms; and
- *reporting and information obligations*: if the due diligence obligations lead to suspicion about an individual or a legal entity, platforms are required to report the situation to an authority specifically in charge of gathering such reports made by cryptocurrency platforms.

Finally, we note that, due to the AML and KYC challenges raised by the holding of crypto-assets, French banks have been reluctant to open bank accounts to token issuers, which has hindered the development of ICOs and crypto/blockchain projects. The Pacte Act addresses this issue by providing that financial institutions must establish objective, non-discriminatory and proportionate rules governing access to bank accounts for token issuers which have obtained the AMF visa. In the event a financial institution denies any such access, it will have to inform the ACPR of the reasons for such denial. A forthcoming decree will specify the remedies and time limits applicable in any such case.

Promotion and testing

In France, as discussed above, the approach adopted by the AMF is very close to a "sandbox" following the launch, in October 2017, of a public consultation relating to ICOs and the above-mentioned UNICORN programme to support and analyse these transactions (see **Sales regulation**).

As part of this consultation, the AMF organised meetings with several players of the blockchain/crypto ecosystem and received 82 contributions from them and other specialists in this field. In February 2018, as part of the UNICORN programme, the AMF announced that it had advised about 15 companies during the first two months of the programme (around 50% of blockchain-related projects), and that the total amount raised or planned to be raised by these project developers was around €350 million.

In November 2018, the AMF published a study on ICOs in France and worldwide and noted that the following trends can be observed: (i) at the global level, this type of financing

remains marginal, representing a total of €19.4 billion since 2014, with France accounting for a modest share (€89 million was raised by 15 issuers); and (ii) in the French market, ICOs are being considered by companies aiming to strengthen their community and to avoid capital dilution.

Overall, the AMF demonstrated an awareness about the importance of these topics and a willingness to get in touch and learn from the ecosystem to shape a specifically adapted legal framework.

In addition, at the European level, in April 2018, most of the European countries, including France, signed a declaration relating to the establishment of a European Blockchain Partnership, intended to act as a vehicle to foster cooperation among Member States in the exchange of technical and regulatory expertise. This declaration, and the partnership that it creates, follows the launch in February 2018 of the EU Blockchain Observatory and Forum, designed to help cultivate new blockchain opportunities in Europe. The stated goal of the partnership is to ensure that Europe continues to play a leading role in the development and roll-out of blockchain technologies.

In relation to promotion, the Pacte Act provides that only ICO issuers which have obtained the AMF visa and the approved DASPs are allowed to engage in solicitation activities (*activités de démarchage*) to support their ICO or service(s).

France is therefore keen on promoting research and investment in cryptocurrency and blockchain-related projects through specific programmes and actions run by governmental authorities.

Ownership and licensing requirements

Under French law, there are very few investment funds which have invested all or even part of their funds in crypto-assets. This is principally explained by the fact that French law, in particular, and EU law in general, were not well-suited to enable investment funds to invest in crypto-assets.

French Undertakings for Collective Investment in Transferable Securities ("**UCITS**", otherwise known as *OPCVM* in France), which are open for distribution to retail clients, are constrained by law to invest in a specific restricted list of assets, into which crypto-assets do not fall. For this reason, French UCITS cannot invest in crypto-assets.

French Alternative Investment Funds ("**AIF**", otherwise known as *FIA* in France), which are open to professional investors only (institutional investors, large firms and investors with sufficient financial experience and competence and also retail clients under certain specific conditions) and therefore are less regulated than UCITS, are less constrained with respect to the assets in which they may invest. However, one of the conditions laid down by the French financial and monetary code is that the title to such asset must be "*evidenced by a mechanism that is recognised under French law*". In the present case, the fact that the title to a crypto-asset is evidenced by registration into a blockchain is not – yet – recognised under French law and therefore an AIF cannot invest in crypto-assets either. Nevertheless, French law has already recognised the possibility of registering certain assets into a blockchain, namely for cash vouchers, *i.e.* "*minibons*", and unlisted securities, and may evolve in the future to also recognise a crypto-asset registered into a blockchain.

Before the entry into force of the Pacte Act, the only option left for a French investment fund to invest directly in crypto-assets was to use a very specific French vehicle known as "other alternative investment funds" ("**Other AIF**", otherwise known as *Autres FIA* in

France). This vehicle may be either regulated *ex ante* by the AMF and open to both professional and non-professional investors, or merely declared *ex post* by the AMF, in which case it is open to professional investors only. In this respect, for an Other AIF to be regulated by the AMF and therefore be open for distribution to both professional and non-professional investors, the Other AIF manager must obtain a portfolio management company licence from the AMF.

However, following the entry into force of the aforementioned Pacte Act, two types of investment funds are now officially allowed to invest part of their funds into crypto-assets: (i) professional specialised investment funds (*fonds professionnels spécialisés* or "**FPSs**"), subject to compliance with the liquidity and valuation rules applicable to them; and (ii) professional private equity investment funds (*fonds professionnel de capital investissement* or "**FPCIs**"), subject to a limit of 20% of their assets.

FPSs are collective investment funds that are not subject to authorisation but must be declared to the AMF and whose main purpose is to invest in various types of assets, including unlisted companies and real estate assets. They may therefore adopt investment rules that differ from those of approved funds. These funds are open to professional investors, to retail clients investing through discretionary portfolios and to any investor investing at least €100,000.

This evolution also enables insurers to offer life insurance policies based on digital assets, through FPSs, and the Pacte Act amended the French Insurance Code to allow FPSs to be included in life insurance account units. Although certain conditions regarding the investor's financial situation or experience, which will be specified by decree, must be complied with, there is no longer a limit on the assets in which PSIFs eligible for life insurance can invest.

FPCIs are investment vehicles designed to invest in unlisted assets. From a regulatory point of view, at least 50% of their assets must consist of (i) unlisted securities on French or foreign regulated markets, or (ii) shares in limited liability companies.

Many FPCIs are for a restricted group of investors (professionals or investors with sufficient financial experience and competence) and are not advertised. These funds sometimes request "lighter approval" from the AMF and do not always request authorisation to conduct a public offering. Some FPCIs are intended to address a wider audience and must seek the approval of the AMF to be allowed to advertise and solicit potential investors. In such case, there are specific rules governing the conditions and limits of the assets' holding.

Mining

"Mining" bitcoin and other crypto-assets is permitted and unregulated under French law. However, the revenues generated by "mining" activities are submitted to a specific taxation regime (see **Taxation**).

Border restrictions and declaration

There is no specific border restriction or obligation to declare crypto-asset holdings under French law.

Reporting requirements

Under French law, there is no reporting requirement for crypto-asset payments made in excess of a certain value.

Estate planning and testamentary succession

Under French law, there is no special treatment for crypto-assets for the purposes of estate planning and testamentary succession, and crypto-assets should be treated like any other assets in such situations.

* * *

Acknowledgment

The authors acknowledge with thanks the contribution to this chapter by Daniel Arroche.

Mr Arroche is an associate in Davis Polk's Corporate Department, practising in the Paris office. Tel: +33 1 56 59 36 82 / Email: daniel.arroche@davispolk.com.

Christophe Perchet
Tel: +33 1 56 59 36 50 / Email: christophe.perchet@davispolk.com
Mr Perchet is a corporate partner in Davis Polk's Paris office. His practice focuses on domestic and cross-border public and private mergers and acquisitions, joint ventures as well as related litigation. Mr Perchet has recently represented major companies in a variety of complex transactions, including Valeo, A.P. Møller – Mærsk and Carrefour.

Juliette Loget
Tel: +33 1 56 59 36 21 / Email: juliette.loget@davispolk.com
Ms Loget is counsel in Davis Polk's Corporate Department, practising in the Paris office. Her practice focuses on domestic and cross-border public and private mergers and acquisitions and includes representing companies and investment banks in domestic and international capital markets transactions. She has recently represented major French and international companies in a variety of complex transactions, including Technip, Valeo, Solvay, Eramet and A.P. Møller – Mærsk.

Stéphane Daniel
Tel: +33 1 56 59 36 46 / Email: stephane.daniel@davispolk.com
Mr Daniel is an associate in Davis Polk's Corporate Department, practising in the Paris office.

Davis Polk and Wardwell LLP

121 avenue des Champs-Elysées – 75008 Paris, France
Tel: +33 1 56 59 36 00 / URL: www.davispolk.com

Germany

Dr Stefan Henkelmann & Lennart J. Dahmen
Allen & Overy LLP

Government attitude and definition

The German government's[1] views on and approach to cryptocurrencies is ambivalent. On the one hand, there is an awareness that the digital age is progressing with an ever increasing dynamism. To reflect these developments, the government has produced a relatively granular digital agenda.[2] On the other hand, there are major concerns that are very much driven by (retail) investor protection considerations, specifically in relation to cryptocurrencies.

In Germany, cryptocurrency is neither treated as money nor given equal dignity with domestic or foreign fiat currency. Rather, cryptocurrency is treated as an investment asset which contributes to the consumer-protection concerns that the German government has expressed: the German government has published a warning relating to the unlawful marketing of cryptocurrencies.[3] In this public warning, the government expressly underlines the fact that cryptocurrencies are not legal tender (*gesetzliche Zahlungsmittel*) but merely substitute currencies (*Ersatzwährungen*). The warning also states that cryptocurrencies as such are not *per se* problematic. Rather, the government points out that some related business practices may raise consumer protection and legal concerns or even be of a fraudulent nature.

The German federal financial supervisory authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* – **BaFin**) has also recently published a public warning relating to the marketing of cryptocurrencies via ICOs.[4] BaFin criticises the use of the term "ICO" as opposed to "IPO" in the securities context, as IPOs can be assumed to be of a highly regulated and transparent nature, whereas this is often not the case for ICOs. In its public warning, BaFin also points to the following particular areas of risks identified:

- Tokens are generally assumed to be subject to high volatility. BaFin identifies a general risk that liquid secondary markets are not available, which means that investors risk being ultimately stuck with an illiquid asset.
- BaFin also adopts the view that a substantial number of companies financed via ICOs exhibit underlying business models that are still in an experimental stage, which also generates an underlying business risk. Smart contract elements may be complex, opaque and hard to scrutinise from an investor's perspective. Moreover, Bafin identifies the particular risk that smart contract codes may be subject to successful attacks and therefore open to manipulation by third parties.
- The regulatory authority also raises the general criticism that white papers are often of poor quality from a transparency perspective, and that ICO transparency is not sufficiently regulated. It even identifies the general risk that statements made in white papers may be objectively insufficient, incomprehensible or even completely misleading.

- BaFin closes its public warning with the following advice addressed to potential investors:[5]

  Before making any investments in tokens, investors should ensure that they fully understand the related risks and potential rewards. To this end, investors should ask the respective issuers as many questions as necessary in order to achieve an adequate level of transparency. Investors should also try to verify relevant statements via independent sources.
- Investors should ensure that the features of the ICO (including the underlying project, if any) are aligned with their individual investment needs and risk appetite.

More recently, BaFin has identified cryptocurrencies as an "area of focus" in its Annual Report 2018.[6] In particular, BaFin focuses on the provision of regulated services without the required licence and thus continues to link ICOs and cryptocurrencies with potentially illegal activity. Additionally, BaFin also recognises the legal uses of cryptocurrencies and tokens and has stated that it does not intend to hinder innovation, but also has expressed concerns regarding the integrity of the financial markets and on investor protection.

BaFin's president *Felix Hufeld* currently does not regard cryptocurrencies as presenting a particular risk from the perspective of financial stability.[7] He has, however, recently expressed concerns that the widestream adoption of cryptocurrencies through social networks, such as the Libra token proposed by Facebook, may trigger macro-economical concerns and may deserve global regulatory attention.[8]

The German Bundesbank, whose mandate includes macro-prudential supervision and monetary policy within the ambit of the ECB-led Eurosystem, also regularly publishes opinions and insights into the crypto sector. The attitudes expressed in such publications towards cryptocurrencies vary.[9]

While the German government's view on cryptocurrency is characterised by a substantial degree of scepticism, the German Government has embraced the underlying *distributed ledger technology* (DLT) and has recently put forward a discussion paper (*Eckpunktepapier*) that, once adopted, would allow for electronic securities that could be issued in dematerialised form.[10] In its discussion paper, the German government has acknowledged ESMA's efforts in this area[11] and has confirmed that it will defer to European regulation on the matter of "Utility Tokens/Cryptocurrencies". However, the German government suggests, at the same time, to create a national framework for the public offering of utility-tokens to bridge any gaps until harmonised measures are available. While the view of the German government is ostensibly aimed at utility tokens, but it could also apply to other forms of tokens.

Cryptocurrency regulation

German law does not provide for a general prohibition relating to the issuing, mining nor possession of, nor trading in cryptocurrencies. The same is true for security, asset and utility tokens. However, regulatory licensing and prospectus requirements may be applicable,[12] which means, however, that there are specific hurdles which may be overcome if the respective legal requirements are met.[13]

From a technical legal perspective, cryptocurrencies were classified by BaFin back in 2011 as financial instruments according to Sec. 1(11) of the German Banking Act (*Kreditwesengesetz*).[14] They fall in the sub-category of so-called "units of account" (*Rechnungseinheiten*), which are a specific national category of financial instruments not based on EU law.

Back in 2013, BaFin issued additional cryptocurrency guidance in light of the growing significance of Bitcoin. The guidance is, however, also applicable for the general classification of cryptocurrencies. The key issue is that the respective tokens qualify as a substitute for legal tender, as they are accepted for payment based on private law agreements, i.e. in contrast to a public law regulation, which is the core feature of fiat currencies.

Most recently, the Berlin Appellate Court has accused BaFin of regulatory overreach in a criminal case and did not apply BaFin's classification of bitcoins as financial instruments (units of account).[15] While the court held that cryptotokens are (currently) not caught by German regulation, BaFin has not changed its view and continues to treat cryptocurrencies as financial instruments. Given current legislative developments (see below), it appears that BaFin's view will be entrenched in law.

BaFin also states in its guidance that cryptocurrencies do not generally qualify as regulated e-money, since there is no central e-money issuer.[16] Even where there is a central issuer, however, an assessment on the basis of the German definition of e-money must be conducted. According to the German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*), e-money is defined as any monetary value that is stored electronically, including magnetically, and takes the form of a claim against the issuer which is issued in return for payment of funds in order to make payment transactions within the meaning of Sec. 675f (4), first sentence, of the German Civil Code (*Bürgerliches Gesetzbuch*) and which is accepted by a natural or legal person other than the issuer.

That being said, tokens which exhibit features that go beyond serving as a mere payment substitute, i.e. security, asset and utility tokens in particular, must be classified on a case-by-case basis. They may qualify as securities or even units or shares in investment funds.[17]

In its ICO guidance of February 2018,[18] BaFin explains that tokens may well classify as securities, so-called capital investments or even units or shares in investment funds.

The classification of cryptocurrencies and tokens in a wider sense, i.e. including security, asset and utility tokens, has far-reaching implications for anyone dealing in them on a commercial basis. In the following paragraphs, the authors will focus on the licensing requirements under financial supervisory law according to the German Banking Act, as well as the resulting AML compliance obligations.

Using cryptocurrencies purely as a substitute for cash or book money in order to participate in the economic cycle in the exchange business is not an activity subject to any licensing requirements under financial supervisory law or other authorisations under German public law. This means that using cryptocurrencies as a means of payment is not a regulated activity, or, in other words, "going shopping" with cryptocurrencies is not a regulated activity for the purchaser, nor is the mere acceptance of cryptocurrencies as a substitute currency by the seller.

Certain commercial dealings in cryptocurrencies and other types of tokens can trigger licensing requirements under financial supervisory law pursuant to the German Banking Act. According to Sec. 32 (1) sent. 1 German Banking Act, anyone wishing to conduct banking business or to provide financial services in Germany on commercial terms, or on a scale which requires commercially organised business operations, requires written authorisation from BaFin. It is important to note in this context that "actively targeting the German market" from abroad is already sufficient to trigger the relevant licensing requirements under German law, i.e. a physical presence in Germany is not necessarily required.

Typical business constellations that are subject to authorisation requirements include commercial trading platforms, often called exchanges, if either: (i) those buying and selling cryptocurrency commercially in their own name for the account of others carry out principal broking services; or (ii) the platform is operating a multilateral trading facility. In addition, and depending on the exact circumstances, providers acting as "currency exchanges" offering to exchange legal tender for cryptocurrency or cryptocurrency for legal tender carry out trading for own account, proprietary trading, contract broking or investment broking, which is also generally subject to authorisation in each case. Advising in relation to cryptocurrencies may constitute regulated investment advice. Holding security tokens in custody (in "hot" or "cold" wallets) may qualify as safe custody business. Finally, underwriting an ICO may be "regulated underwriting or placement business" within the ambit of the German Banking Act. Given this magnitude of potentially licensable activities, it is clear that any intention to handle cryptocurrencies on a commercial basis, where such activities are targeted at the German market, must be assessed on a case-by-case basis. The following are definitions of potentially regulated activities that require prior written authorisation from BaFin:

- Principal broking services are defined as the purchase and sale of financial instruments in the credit institution's own name on the account of others.
- Safe custody business is defined as the safe custody and administration of securities for the account of others.
- Underwriting business (hard underwriting) is defined as the purchase of financial instruments at the credit institution's own risk for placement in the market or the assumption of equivalent guarantees.
- Investment broking is defined as the brokering of business involving the purchase and sale of financial instruments.
- Investment advice is defined as providing customers or their representatives with personal recommendations in respect of transactions relating to certain financial instruments where the recommendation is based on an evaluation of the investor's personal circumstances, or is presented as being suitable for the investor and is not provided exclusively via information distribution channels or for the general public.
- Operation of a multilateral trading facility (MTF) is defined as operating a multilateral facility which brings together a large number of persons' interests in the purchase and sale of financial instruments within the facility according to set rules in a way that results in a purchase agreement for these financial instruments.
- Placement business (soft underwriting) is defined as the placement of financial instruments without a firm commitment basis.
- Contract broking is defined as the purchase and sale of financial instruments on behalf of and for the account of others.
- Portfolio management is defined as the management of individual portfolios of financial instruments for others on a discretionary basis.
- Proprietary trading is defined (in simplified terms) as the purchase and sale of financial instruments for own account as a service for others.

A recent legislative proposal will introduce a definition of "crypto-assets" and the "crypo-asset custody" as an additional category of regulated activity (see further below). This category will serve to capture cryptocurrencies that are not caught by German regulation as units of account.

Sales regulation

As regards the sales regulation for cryptocurrencies, commercial distribution may trigger the aforementioned licensing requirements for distributors under financial supervisory law (e.g. typically at least investment broking) due to the fact that these are financial instruments under the German Banking Act.

Beyond the licensing requirements under financial supervisory law, the legal position becomes very complex. The following are points that need to be considered in any detailed assessment:[19]

(i) While cryptocurrencies are financial instruments (units of account) within the ambit of the German Banking Act, they do not qualify as financial instruments under the German Securities Trading Act (*Wertpapierhandelsgesetz*), i.e. the conduct requirements under German law. The situation is different if tokens go beyond being a mere substitute currency; in such case they may qualify (in particular) as securities according to the definitions set out in the German Securities Trading Act, triggering complex conduct regulation of their distribution.

(ii) The test for whether a cryptocurrency qualifies as security considers whether (simplified) securities-like rights are attached to the tokens and whether there is a minimum required fungibility, which can be generally assumed if they are (crypto-)exchange-traded.

(iii) The classification as "security" may also trigger prospectus requirements and where a token sale ICO, is issued to raise funds for a specific purpose, an assessment as to whether the tokens constitute units or shares in investments funds within the ambit of the German Capital Investment Code (*Kapitalanlagegesetzbuch*) must be made. Where an investment fund is in fact established and managed, this constitutes a prohibited activity if no licence under the German Capital Investment Code is obtained, which in turn can have far-reaching criminal and civil liability implications.

The above points trigger wide-reaching consequences, including conduct regulation and documentation requirements, the details of which go well beyond the scope of this publication.

Taxation

Handling (in the widest sense) cryptocurrencies may have complex tax implications under German law. In the following paragraphs, one of the most pressing issues is given an overview on, i.e. the classification for VAT-purposes.[20]

On 27 February 2018, the German Ministry of Finance (*Bundesfinanzministerium*) issued its guidance concerning the VAT treatment of certain dealings in cryptocurrencies in light of the decision by the ECJ, dated 22 October 2015 (C-264/14 – *Hedqvist*).[21] The core statements of this guidance are set out below:

(i) Exchanging cryptocurrency into fiat and *vice versa* is exempted from the VAT regime.

(ii) The mere use of cryptocurrencies as a means of payment is not a taxable transaction for VAT purposes (i.e. the "cash leg" of a sales transaction).

(iii) Mining is not a taxable activity for VAT purposes.

(iv) Offering digital wallet services in return for consideration is a taxable activity for VAT purposes under German tax law where such service is offered in Germany.

(v) Providing a crypto exchange platform may be a taxable activity for VAT purposes, depending on the precise circumstances.

Additionally, transactions in cryptocurrencies may be subject to German income tax, provided the seller is a German tax resident.

Money transmission laws and anti-money laundering requirements

German payment services regulation is provided for in the Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*) which transposes the Second Payment Services Directive (PSD II)[22] as well as the E-Money Directive.[23]

Since cryptocurrencies do not constitute legal tender, "payment accounts", i.e. electronic wallets (hot or cold) where related keys are "stored", do not constitute payment accounts[24] according to Sec. 1 (17) Payment Services Supervision Act. It follows that licensable activities attaching to the opening and operation of payment accounts, such as direct debit business and credit transfer business (involving payment transactions in fiat currency), are not applicable. Due to the fact that fiat currency is not "remitted" where, for instance, a person exchanges fiat for crypto, transfers the crypto to a third party and this third party (re-)exchanges into fiat, there are very convincing arguments that such activities do not trigger licensable money remittance business according to the Payment Services Supervision Act either, even if they are performed on a commercial basis.

That being said, close attention must be paid to the structuring of any "fiat cash legs" involved when structuring a business model that involves transactions in cryptocurrencies, beyond the licensing requirements under financial supervisory law. One criterion that would lead the model to fall outside the ambit of the Payment Services Supervision Act is that no unlicensed administrator receives, stores or manages fiat currency for the account of any customer or any third party. The details need to be analysed on a case-by-case basis.

The mere use of cryptocurrencies and other tokens as a means of payment for goods and services and the sale and exchange of self-procured cryptocurrency does not subject the relevant persons or undertakings to any obligations under the German Anti-Money Laundering Act (*Geldwäschegesetz*).

Where commercial dealing in cryptocurrencies triggers licensing requirements under financial supervisory law according to the German Banking Act, by way of express statutory reference in the German Anti-Money Laundering Act, however, this also means that the person or undertaking becomes an "obliged person" (*Verpflichteter*) for the purposes of German AML law.

The German Anti-Money Laundering Act requires obliged persons (*inter alia*) to have effective risk management systems in place as well as to fulfil general due diligence requirements, including customer and beneficial owner identification and verification duties. The obligations also include monitoring obligations, as well as the implementation of organisational processes for suspicious transaction-reporting to competent authorities.[25]

At the level of European law, the European Parliament and European Council reached an agreement in December 2017 that will extend AML obligations to firms operating centralised cryptocurrency exchanges and custodial wallet providers for cryptocurrencies by adding them to the definition of "obliged entities" contained in the existing directive framework. This means that for such EEA countries where, unlike in Germany, cryptocurrencies do not constitute financial instruments and thus (in an nutshell) commercial dealings in them do not trigger licensing requirements under financial supervisory law, which in turn trigger AML obligations, there will be a minimum harmonisation of AML law in the crypto sector. A first draft of the implementation act has been made available in May 2019 that will

introduce an additional regulated service of "crypto-asset custody" (*Kryptoverwahrgeschäft*). This category is aimed at certain crypto-assets that were not classified as "units of account" and will introduce licensing obligations for certain wallet providers. These will be supplemented by AML requirements.

Promotion and testing

In Germany, there is no sandbox or any other type of light-touch regulatory regime available for commercial dealing in or handling of cryptocurrencies or any other types of tokens.

This is due to the fact that in Germany there is no legal basis for any light-touch approach, which could potentially include systematic deviation from the principle of equal treatment of the applicants.

Ownership and licensing requirements

Where cryptocurrencies are held "for the account of others" on a commercial basis, the respective business model must be assessed on a case-by-case basis. Such activities may, in particular, trigger the regulated activities of: (i) portfolio management; (ii) principal broking services; (iii) contract broking; and/or (iv) investment broking according to the German Banking Act or even constitute managing an investment fund, which is a licensable activity under the German Capital Investment Code. Additionally, investment funds may be restricted in their ability to invest into cryptocurrencies.

Mining

BaFin issued public guidance on the regulatory classification of mining back in 2013.[26] According to this regulatory guidance, the creation of new cryptocurrency by solving complex mathematical computational tasks (i.e. mining) does not constitute a regulated activity under the German Banking Act.

Border restrictions and declaration

There is no general prohibition on "importing" cryptocurrencies into Germany or "exporting" them out of Germany.

Reporting requirements

The following paragraphs contain a discussion of some of the core provisions of the German Foreign Trade and Payments Ordinance (*Außenwirtschaftsverordnung*). Cross-border transactions involving cryptocurrencies should be assessed on a case-by-case basis.

According to Sec. 67 (1) Foreign Trade and Payments Ordinance, German residents must notify the Bundesbank, by predefined deadlines, of payments (i) which they receive from foreigners or from residents for the account of a foreigner (incoming payments), or (ii) which they make to foreigners or to residents for the account of a foreigner (outgoing payments).

According to Sec. 67 (2) Foreign Trade and Payments Ordinance, the relevant notifications to the Bundesbank are not required for: (i) payments which do not exceed the amount of €12,500 or the equivalent value in another currency; (ii) payments for the import, export or transfer of goods; or (iii) payments for the granting, receipt or repayment of loans, including the justification and repayment of credit balances, with an originally agreed term or termination deadline of not more than 12 months. Accordingly, the question of whether

using cryptocurrencies as an alternative means of payment does not arise within the exemptions set out in Sec. 67 (2) Foreign Trade and Payments Ordinance. In all other cases of cross-border transactions, the legal interpretation of Sec. 67 (3) Foreign Trade and Payments Ordinance is decisive. According to Sec. 67 (3) Foreign Trade and Payments Ordinance, payments within the meaning of the relevant subdivision of the Foreign Trade and Payments Ordinance shall include netting and offsetting and payments handled by direct debit.

Although Sec. 67 (3) Foreign Trade and Payments Ordinance contains a supplementary legal definition for "payments", it does not further specify the core term of "payments" itself. In other words, Sec. 67 (3) Foreign Trade and Payments Ordinance merely expands the definition of "payment" to include other "movements of assets".[27] Hence the concept of payment must be interpreted broadly. According to the prevailing legal view, therefore, the term "payments" within the ambit of Sec. 67 (3) Foreign Trade and Payments Ordinance means "any transfer of means of payment (cash and book money) between two persons".[28]

Despite such very broad definition of "payments", it is very likely that the definition only applies to payments made in fiat currency.[29] As cryptocurrencies are not legal tender, it is very likely that transactions cannot be classified as payments but rather occur within barter transactions which merely contain the economic components of payments in the legal sense.

Accordingly, it is also very likely that "payments" in cryptocurrencies do not constitute payments within the ambit of Sec. 70 Foreign Trade and Payments Ordinance. According to Sec. 70 (1) Foreign Trade and Payments Ordinance, domestic financial institutions must report (*inter alia*) the following to the Bundesbank within predefined deadlines:

(i) payments for the sale or acquisition of securities and financial derivatives which the financial institution sells to foreigners or buys from foreigners on its own or on a third party's account, and payments which the financial institution makes to foreigners or receives from them in connection with the redemption of domestic securities;

(ii) interest and dividend payments on domestic securities which they make to or receive from foreigners; and

(iii) incoming and outgoing payments for interest payments and similar revenues and expenses, excluding interest on securities received from or made to foreigners on their own account.

Such reporting obligations are not applicable to payments which do not exceed the amount of €12,500 or the equivalent value in another currency.

However, the term "payments" according to the relevant provisions of the Foreign Trade and Payments Ordinance further includes the contribution of objects and rights to companies, branches and permanent establishments.[30] It is very likely that the respective provision applies the concept of payments in fiat currency in an analogous manner to the contribution of objects and rights into companies, branches and permanent establishments located in Germany. It follows that this case-specific sub-definition cannot be taken as a means to argue that transacting in cryptocurrencies is to be generally treated as being equivalent to payments in fiat currency.

However, the question arises as to whether cryptocurrencies, when paid into a German-based undertaking (i.e. by means of a contribution in kind) within the ambit of this definition as a means of raising (equity) capital for such undertaking qualify as "objects" or "rights". While almost all[31] cryptocurrencies are surely not "objects" (*Sachen*), as they do not constitute tangible property (*körperlicher Gegenstand*), cryptocurrencies may from time to time carry

rights attached to them or, from a teleological perspective, the factual possibility to effect economic payments via their use, may be construed as being equivalent to a right within the definition of the term "right" according to Sec. 67 (3) sent. 2 Foreign Trade and Payments Ordinance. Accordingly, where contributions in kind to German-based companies are made in the form of cryptocurrencies, the transactions in questions should be assessed on a case-by-case basis and it may be advisable to seek a common understanding with the competent authorities.

Estate planning and testamentary succession

As regards the question of how cryptocurrencies are treated for the purposes of estate planning and testamentary succession, the rules according to the German Civil Code (*Bürgerliches Gesetzbuch*) are relevant. German law codifies the so-called principle of universal succession, which means that the heirs assume the legal positions of the deceased in their entirety.

This principle of universal succession also encompasses the general rule that property relations usually pass to the heirs, and intangible rights expire upon death. Cryptocurrency has the character of a substitute for cash or legal tender. As such, it forms part of the property of the deceased and should pass to the heirs after death according to Sec. 1922 of the German Civil Code (BGB). In a sense, the private key (and the wallet), or such other means that allow for the transfer of a given cryptocurrency, should qualify as forming part of the inheritance within the ambit of Sec. 1922 of the German Civil Code.

It thus follows from this analysis that cryptocurrencies should be subject to all the regular rules of inheritance according to the German Civil Code, including that they can be subject to testamentary succession.

* * *

Acknowledgment

The authors would like to thank Dennis Kunschke for his contribution as an author of the chapter in the previous edition on which the current chapter is based.

* * *

Endnotes

1. The term "government" in this case also includes regulatory authorities such as the German *Bundesbank* and the German Federal Financial Supervisory Authority (BaFin).
2. For the general digital agenda and related "hightech-strategie" *cf.* the German government's webpage: https://www.bundesregierung.de/Webs/Breg/DE/Themen/Innovationspolitik/_node.html. Most recently, BaFin has published its own agenda on digitalisation, also addressing cryptocurrencies, *cf.* https://www.bafin.de/DE/DieBaFin/ZieleStrategie/Digitalisierungsstrategie/digitalisierungsstrategie_node.html.
3. Public warning dated 2 February 2018, available at: https://www.bundesregierung.de/Content/DE/Artikel/2018/02/2018-02-02-kryptowaehrung.html.
4. Public warning dated 9 November 2017, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html as well as

further background material dated 15 November 2011 available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1711_ICO.html.

5. This advice is primarily directed at consumers (*Verbraucher*) but written in a general "common sense" manner.
6. For further information, please refer to the BaFin annual report 2018 (available in German) at: https://www.bafin.de/SharedDocs/Downloads/DE/Jahresbericht/dl_jb_2018.html.
7. *Cf.* interview; quotes available at: http://www.faz.net/aktuell/finanzen/digital-bezahlen/bitcoin-und-co-bafin-stellt-regulierung-in-aussicht-15462114.html.
8. *Cf.* interview; quotes available at: https://www.boersen-zeitung.de/index.php?li=1&artid=2019120001.
9. *Cf.* further reference: "Vorteile durch neue digitale Produkte im Zahlungsverkehr" – Interview in German *Focus*, dated 5 February 2018, available at: https://www.bundesbank.de/Redaktion/DE/Interviews/2018_02_05_dombret_focus.html?searchArchive=0&submit=Suchen&searchIssued=0&oneOfTheseWords=cryptocurreny%2C+Bitcoin%2C+Kryptow%C3%A4hrung; "Finger weg von Bitcoin!", Guest commentary in the *Frankfurter Allgemeinen Sonntagszeitung* dated 04 February 2018, available at: https://www.bundesbank.de/Redaktion/DE/Standardartikel/Presse/Gastbeitraege/2018_02_04_thiele_fas.html?searchArchive=0&submit=Suchen&searchIssued=0&oneOfTheseWords=cryptocurrency%2C+Kryptow%C3%A4hrung%2C+Bitcoin; "Auswirkungen virtueller Währungen auf die Finanzmärkte", speech at Union Investment dated 15 January 2018, available at: https://www.bundesbank.de/Redaktion/DE/Reden/2018/2018_01_15_wuermeling.html?searchArchive=0&submit=Suchen&searchIssued=0&oneOfTheseWords=cryptocurrency%2C+Kryptow%C3%A4hrung%2C+Bitcoin.
10. *Cf.* the discussion paper of the relevant Federal Ministries, available at: https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Internationales_Finanzmarkt/2019-03-08-eckpunkte-elektronische-wertpapiere.html.
11. *Cf.* ESMA's Advice on initial coin offerings and crypto-assets, available at https://www.esma.europa.eu/file/49978/download?token=56LqdNMN.
12. *Cf.* under "Sales regulation" below for details.
13. E.g. adequate licences are obtained.
14. *Cf.* the public BaFin guidance dated 19 December 2013, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html.
15. Ruling of the Appellate Court of Berlin of 5 September 2018 (case no: (4) 161 Ss 28/18 (35/18)).
16. Where there is a central issuer, however, detailed analysis must be conducted in order to assess potential classification as e-money.
17. Please refer to further details below.
18. *Cf.* the public guidance issued by BaFin dated 20 February 2018, available at: https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs.html.
19. For further information on the complex legal implications and classifications, *cf.* BaFin's ICO Guidance, available at: https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs_en.html.

20. For further information on taxation of the digital economy, *cf*. *Troetscher* in: Kunschke/Schaffelhuber, FinTech, Grundlagen, Regulierung, Finanzierung, Case Studies, (2018), p. 209 *et seq*.
21. *Cf*. German Ministry of Finance, available at: https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/2018-02-27-umsatzsteuer__liche-behandlung-von-bitcoin-und-anderen-sog-virtuellen-waehrungen.pdf?__blob =publicationFile&v=1.
22. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
23. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.
24. These are defined as an account held in the name of one or several payment service users and serving the execution of payment transactions.
25. *Cf*. *Kunschke*, contribution of input for Germany to Holman/Stettner (*et al*.), Chapter "Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches" in: *The International Comparative Legal Guide to: Anti-Money Laundering 2018*, Global Legal Group.
26. *Cf*. the public BaFin guidance dated 19 December 2013, available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html.
27. *Gramlich* in Hohmann/John § 59 AWV, Rn. 5.
28. *Grämlich* in Hohmann/John § 59 AWV, Rn. 3; *Samm* in: Bieneck, § 21 Rn. 61, and *Contag* in: Schult, § 59 AWV, Rn. 1.
29. On the classification of cryptocurrencies as regards payments *cf*. further *Eckert* in: DB 2013 2108 (2110); Boehm/Pesch MMR 2014, 75 (78); *Spindler/Bille* WM 2014, 1357 (1361).
30. The German original reads: *Als Zahlung gilt ferner das Einbringen von Sachen und Rechten in Unternehmen, Zweigniederlassungen und Betriebsstätten*.
31. There may, however, be certain related physical "emergences" such as cold keys.

Dr Stefan Henkelmann
Tel: +49 69 2648 5997 / Email: stefan.henkelmann@allenovery.com

Stefan is a Partner at Allen & Overy LLP, Frankfurt with broad expertise advising on German and international capital markets transactions. Stefan specialises in advising on securitisations and other structured finance transactions (covering true sale, secured loan and synthetic structures across a broad range of asset classes) and on restructurings in the capital markets sector (including bond restructurings and restructurings of securitisations and related assets), also covering the fintech sector.

Another focus of his practice is the advice on bond transactions including Pfandbriefe, covered bonds, structured notes, hybrid and corporate bonds. Stefan also has broad experience in advising on all related regulatory and insolvency law matters.

He is a lecturer for capital markets law at the Institute for Law and Finance of the Goethe University Frankfurt.

Lennart J. Dahmen
Tel: +49 69 2648 5901 / Email: lennart.dahmen@allenovery.com

Lennart is a member of the International Capital Markets team in the Frankfurt Office of Allen & Overy. He advises banks, asset managers and investment firms on all aspects of financial supervisory law, with a particular focus on investment law/asset management and capital markets regulation. In addition, Lennart has broad experience in the areas of M&A transactions of regulated entities and sanctions/enforcement in the financial sector. Furthermore, Lennart has advised on several regulatory matters related to Brexit, including licensing projects for banks and financial services providers as well as on branch establishments and the provision of cross-border services.

Allen & Overy LLP

Haus am OpernTurm, Bockenheimer Landstraße 2, 60306 Frankfurt am Main, Germany
Tel +49 69 2648 5000 / Fax +49 69 2648 5800 / URL: www.allenovery.de

Gibraltar

Joey Garcia & Jonathan Garcia
ISOLAS LLP

Government attitude and definition

The Government of Gibraltar has approached the growing cryptocurrency and wider blockchain and distributed ledger technology ("DLT")-related sector with a uniquely receptive and progressive attitude. Financial regulators and policymakers in Gibraltar have understood the need for regulation in this sector, responding rapidly to such demand as far back as 2014, with the creation of the Cryptocurrency Working Group. This private sector initiative led to the development of the Distributed Ledger Technology framework ("DLT Framework"), which became effective on 1 January 2018, making Gibraltar the first jurisdiction in the world to deliver a framework of its kind that regulates businesses that use DLT. The DLT Framework includes nine principles that apply to DLT businesses operating in Gibraltar.

The response to this approach has been global and truly significant. Those who know nothing about Gibraltar may be surprised, but those who know the history of the small jurisdiction, with a joined-up partnership between law-makers, regulators and industry, that is able to adapt and evolve to attract the right opportunities at the right level, with the speed and flexibility needed to accomplish such goals, will not be surprised at all.

Since the coming into force of the DLT Framework, the Government of Gibraltar has been delivering on a detailed and strategically formulated activity schedule, created to proactively drive home Gibraltar's very strong DLT message, by researching and identifying key markets and audiences and focusing its marketing in these areas. The Gibraltar Government has launched a new advisory group that focuses on the creation of new technology-related education courses, such as blockchain. The New Technologies in Education (NTiE) group is a joint initiative between the Government and the University of Gibraltar in collaboration with some of the leading new technology companies based in Gibraltar. The advisory group's aim is to address the growing demand for related skills as the sector continues to expand in Gibraltar. The University of Gibraltar is currently running a professional course in this space titled "Professional Certificate of Competence in Blockchain & Smart contracts".

Whilst Gibraltar has shown leadership in this space, development is clearly an ongoing process and Gibraltar is aware of the importance as a jurisdiction, for it to invest in supporting the development of knowledge and skills in tandem with generating economic results as Gibraltar continues to strive for excellence. The Gibraltar Government has created the Gibraltar Association for New Technologies ("GANT"), an association to be formed with the private sector. GANT serves several purposes, primarily enhancing the development in Gibraltar of the use of blockchain and DLT and other future developments (collectively

referred to as "New Technology"), with a view to enhancing the reputation, integrity and public trust in this sector.

GANT has also been tasked to raise the profile of "New Technology" in Gibraltar across a spectrum not necessarily limited to financial services. This includes encouraging respective organisations to emphasise the high value of their reputation and interest in contributing to enhanced client and investor protection and remaining committed to safeguarding customer and jurisdictional interests. GANT also provides a forum for discussion on "New Technology" issues within the membership and to assist other sectors of the wider Gibraltar Finance Centre whilst also assisting and advising the Gibraltar Government on all aspects of this sector.

Legal status of cryptocurrencies

Cryptocurrencies are not considered legal tender in Gibraltar and accordingly, are not issued or guaranteed by the Gibraltar Government. However, cryptocurrencies may still qualify as electronic money ("E-Money") under certain circumstances. On a European level, the regulation of E-Money is based on the EU E-Money Directive. There, E-Money is defined as an electronically, including magnetically, stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions, and accepted by a natural or legal person other than the electronic money-issuer. This definition is in line with the definition contained in the Financial Services (Electronic Money) Regulations 2011 which transpose the E-Money Directive into Gibraltar law. E-Money requires an issuer. Therefore, a cryptocurrency which comes into existence by way of mining (e.g. Bitcoin) without an issuer does not qualify as E-Money. Conversely, a cryptocurrency that is issued by an issuer at par value against fiat and furnished with the promise of the issuer to be redeemed in exchange for fiat, and therefore being accepted as means of payment by third parties, would qualify as E-Money.

Cryptocurrency regulation

Owing largely to the difficulty of regulating cryptocurrencies themselves, the DLT Framework has attempted not to enforce regulation of cryptocurrencies but instead to impose a regulatory regime for firms that carry on by way of business, in or from Gibraltar, the use of DLT for storing or transmitting value belonging to others. Accordingly, regulation will depend on what services a firm is providing customers in respect to their cryptocurrencies and whether this falls under the scope of regulation.

Supplementing the DLT Framework, on 13 March 2018, the Gibraltar Government published a consultation paper detailing proposals "for the regulation of token sales, secondary token market platforms and investment services relating to tokens" ("Token Regulation Proposals") and has since circulated to industry experts a draft Bill implementing the Token Regulation Proposals. The scope of the proposals contained in the Token Regulation Proposals is set out in further detail below.

In keeping with the DLT Framework, the Token Regulation Proposals do not aim to directly regulate tokens (whether cryptocurrencies or otherwise) subject to a token sale, rather how the actual token sale itself is conducted and the persons appointed to supervise the sale and ensure that it complies with the legislation.

Because cryptocurrencies vary widely in design and purpose, it should be kept in mind that these may represent transferable securities, and their promotion and sale would already be

covered by existing securities legislation in Gibraltar such as the Prospectuses Act 2005. Its classification as a security triggers various consequences; in particular, regulatory consequences. The requirement to issue a prospectus when offering securities publicly is only one example of such a requirement. A distinction must be drawn between the concept of a security on the one hand and a financial instrument on the other, with the latter being the broader term.

"Securities" are one of several sub-categories of financial instruments. Regulatory requirements may therefore also arise for non-securities that are classified as financial instruments. This includes the requirements arising under MiFID II, transposed into Gibraltar law through the Financial Services (Markets in Financial Instruments) Act 2018, which, in addition to applying to businesses providing certain investment services or engagement in certain activities with clients in relation to financial instruments, also defines "financial instruments" in a wide form, including forms of commodity derivative contracts and arrangements that may apply to any asset or right of a fungible nature (under certain conditions).

If a cryptocurrency meets the MiFID II definition of a financial instrument, then a number of crypto-asset-related activities carried out by an exchange are likely to qualify as investment services/activities for which a licence is required outside of the DLT Framework. This includes multilateral trading facilities (MTF), organised trading facilities (OTF) and other exchange-related activities.

Sales regulation

Most often, tokens do not qualify as securities under Gibraltar or EU legislation. In the event that they do constitute securities, there is currently an EU-wide framework dealing with this, as has been described above. Accordingly, Gibraltar is not looking to introduce a framework that will modify in any way, securities law or the EU Prospectus Directive requirements. That is to say, the public offering of tokens that constitute securities does not require further regulation from a Gibraltar perspective and will continue to fall under current frameworks governing issuance of securities. The Token Regulation Proposals will introduce legislation covering the promotion, sale and distribution of tokens that will serve some cryptocurrency or functional use, such as prepayment for access to a product or service. Cryptocurrencies that function solely as decentralised virtual currency (e.g. Bitcoin) or as central bank-issued digital currency will be excluded from the Token Regulation Proposals.

The Token Regulation Proposals provide a high-level outline of what lies in store. Amongst other things, it is proposed that new legislation will regulate the promotion and sale of tokens conducted in or from Gibraltar though the appointment of authorised sponsors of public token offerings, who themselves would be regulated.

The Token Regulation Proposals are proposing a requirement for adequate, accurate and balanced disclosure of information to enable anyone considering purchasing tokens to make an informed decision. The legislation may prescribe what, as a minimum, constitutes adequate disclosure, and in what form disclosures are made (*e.g.*, in a key facts document not exceeding two pages). From time to time, guidance on disclosure rules may be published by the Gibraltar Financial Services Commission ("GFSC"), the financial services regulator in Gibraltar.

The token industry often refers to the concept of "self-regulation", and best practice frameworks for token offerings have already been established. The key difference with the Token Regulation Proposals is that while being attractive in the sense that it may be said to

decentralise certain standards and requirements, the concept of self-regulation is also, in many senses "voluntary", and does not necessarily raise the standards through any legally enforceable framework such as the one being proposed in Gibraltar. As a result, the GFSC can ensure and enforce their regulatory objectives through the implementation of the Token Regulation Proposals.

As outlined above, the GFSC intends to regulate authorised sponsors of public token offerings. It therefore appears that the onus of ensuring compliance with appropriate standards will be on the service providers. The GFSC does not intend to regulate token issuers, nor will it regulate the underlying technology or the tokens themselves.

The Token Regulation Proposals will establish a regime for the authorisation and supervision of authorised sponsors possessing appropriate relevant knowledge and experience, who will be responsible for compliance with various obligations. It is intended that an authorised sponsor will need to be appointed in respect of every public token offering promoted, sold or distributed in or from Gibraltar.

Authorised sponsors will be subject to an authorisation and supervision process by the GFSC and must possess suitable knowledge and experience of the industry to be admitted into the sponsorship regime. A critical component for authorised sponsors to be authorised, is to have a local presence in Gibraltar, with "mind and management" based in the jurisdiction. The onus will also be on the authorised sponsors to produce their own codes of conduct, setting out what they consider to be best practices relating to token offerings. These codes will form part of a prospective authorised sponsors' application for authorisation. The introduction of an authorised sponsors regime is comparable to what currently exists today in the UK in relation to regulated public market listings, where Sponsors and Nominated Advisors effectively act as listing agents that guide prospective issuers through the flotation process. It appears this same model is being adapted under the authorised sponsors regime to hand-hold prospective token-issuing entities through a compliant token sale process.

The GFSC will establish and maintain a public register of authorised sponsors and their respective past and present codes of practice.

It should also be noted that entities issuing tokens may separately have to comply with classic consumer protection law, depending on the design of the digital token. All relevant EU legislation covering e-commerce and consumer protection has been transposed into Gibraltar law via various Acts of Parliament or Regulations. The EU e-commerce and consumer protection rules (E-Commerce Directive, Consumer Rights Directive, Directive on Distance Marketing of Consumer Financial Services) all specify the information that should be disclosed.

Taxation

It should be noted that the treatment of cryptocurrencies is not specifically considered in current tax legislation in Gibraltar, nor in accounting standards that are generally accepted in Gibraltar; therefore, where relevant, general principles implicit in current legislation and accounting standards that are believed to be appropriate, are applied.

In Gibraltar there is no capital gains tax, value added tax, death duties, inheritance, wealth, capital transfer, gifts, or withholding tax levied at present. For companies, corporation tax is generally 10%, payable on profits that derive from income accrued in or derived from Gibraltar; that is to say, by reference to the location of the activities which give rise to the profits. Under tax legislation, the location of the activities which give rise to the profits of a business whose underlying activity results in income, and requires a licence and regulation

under any law of Gibraltar, shall automatically be considered to be Gibraltar. Favourable tax packages are also available for High Net Worth Individuals and High Executives Possessing Specialist Skills who want to establish residence in Gibraltar and can benefit from tax payable on income being restricted to a capped amount, which encourages talent toward Gibraltar.

Money transmission laws and anti-money laundering requirements

A DLT firm is caught as a relevant financial business under the Proceeds of Crime Act ("POCA") in Gibraltar. Accordingly, a DLT firm would become subject to KYC/AML obligations. In addition, under the DLT Framework, a DLT firm "must have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing". The requirement is derived from: EU Anti-Money Laundering Directives; the Proceeds of Crime Act 2015; and the FFSC0 Anti-Money Laundering Guidance Notes. There are also additional and specific guidance notes relating to the 'Financial Crime' factor which have been prepared specifically for DLT firms to set out regulatory expectations.

Firms are required to establish procedures to: apply customer due diligence procedures; appoint a Money Laundering Reporting Officer ("MLRO") to whom money laundering reports must be made; establish systems and procedures to forestall and prevent money laundering; provide relevant individuals with training on money laundering and awareness of their procedures in relation to money laundering; screen relevant employees; and undertake an independent audit for the purposes of testing customer due diligence measures, ongoing monitoring, reporting, recordkeeping, internal controls, risk assessment and management, compliance management and employee screening. The frequency and extent of the audit shall be proportionate to the size and nature of the business.

It is possible for a DLT firm's compliance programme to use customer verification tools (such as Jumio) as well as blockchain technology (such as Chainalysis). Because the DLT Framework is based on the application of principles rather than rigid rules, a firm will be able to use innovative solutions provided it can satisfy the GFSC that it can meet its regulatory obligations.

The application of this AML regime to DLT firms has been seen by many as a precursor to the requirements under AMLD5 which will for the first time capture exchanges and pure custody wallet providers. These businesses will already be fully regulated and subject to such requirements if they are operating in Gibraltar.

In addition, it should be noted that POCA now includes within the definition of "relevant financial business", "undertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of distributed ledger technology or a similar means of recording a digital representation of an asset". Essentially, the addition of the new definition of relevant financial business specifically brings sales of a digital asset clearly within existing anti-money laundering laws, which in turn have been very well received by other service providers in the industry.

Promotion and testing

Gibraltar has always maintained itself at the forefront of novel technological development. In fact, if you look in the small print for most online gambling businesses around the world, it is found that most are based in Gibraltar.

Gibraltar is hoping to replicate that philosophy in the blockchain space and follow the success of online gaming, and is doing so by stepping out of the regulatory "sandbox", in the same way as it did back in the gaming days. Rather than creating a "safe space" for businesses to test innovative financial products, services, business models and delivery mechanisms in a live environment without immediately incurring all the normal regulatory consequences of engaging in the activity in question, Gibraltar has instead chosen to provide legal certainty and allow businesses to operate within a purpose-built legislative framework. In doing so, it considers that a flexible, adaptive approach is required in the case of novel business activities, products and business models and that whilst regulatory outcomes remain central, these are better achieved through the application of principles rather than rigid rules. This is because, for businesses based on rapidly-evolving technology, such hard and fast rules can quickly become outdated and unfit for purpose. Accordingly, it has created a principles-based framework based on risk and proportionality, and an outcome-focused, yet robust approach.

The Gibraltar Government recognises that this is a nascent industry and whilst Gibraltar has shown leadership in this space, development is clearly an ongoing process and Gibraltar is aware of the importance as a jurisdiction, for it to invest in supporting the development of knowledge and skills, in tandem with generating economic results as Gibraltar continues to strive for excellence.

Ownership and licensing requirements

If a firm is engaging in an activity for business purposes, which involves the storage or transmission of cryptocurrencies belonging to third parties, it will need to be licensed under the DLT Framework.

Providing investment and ancillary services relating to cryptocurrencies is not currently regulated in Gibraltar. The Gibraltar Government has proposed under the Token Regulation Proposals, to regulate the provision of investment and ancillary services in or from Gibraltar and, to the extent not otherwise caught by existing legislation, their derivatives. This is intended to cover advice on investment in tokens, virtual currencies, and central bank-issued digital currencies, including:

- generic advice (setting out fairly and in a neutral manner the facts relating to token investments and services);
- product-related advice (setting out in a selective and judgmental manner the advantages and disadvantages of a particular token investment and service); and
- personal recommendations (based on the particular needs and circumstances of the individual investor).

This will be proportionately modelled on provisions that currently exist under MiFID II with the aim of ensuring that such services are provided fairly, transparently, and professionally.

A person may hold and trade his own cryptocurrency without the need for authorisation.

Holdings in cryptocurrency by investment advisors or fund managers

If there is an intention to establish an arrangement that enables a number of investors to pool their assets and have these professionally managed by an independent manager, rather than buying investments directly as individuals, then collective investment scheme ("CIS") law is another relevant legal consideration.

The Financial Services (Collective Investment Schemes) Act 2011 defines a "collective investment scheme" as "any arrangement with respect to property, the purpose or effect of which is to enable persons taking part in the arrangement, whether by becoming owners of the property or any part of it or otherwise, to participate in or receive profits or income arising from the acquisition, holding, management or disposal of the property or sums paid out of such profits or income".

The arrangement referred to above must be such that the participants in the arrangement do not have day-to-day control over the management of the assets. Further, the investments and the profits/income arising from them must be pooled, and/or the property managed as a whole.

There are two popular structures for setting up a CIS in Gibraltar: the Experienced Investor Fund ("EIF"); and the Private Scheme ("PS"). These structures are agnostic to the underlying assets they govern for investors.

Typically, a CIS which is to focus on crypto-assets would best be established as an EIF. Only when such a CIS is set up for a small group of persons previously known to each other, and where there will be no promotion of the CIS, would it be suitable to set up a CIS of this nature as a PS. Indeed, the local Gibraltar Funds and Investment Association (GFIA) has recently published a draft code of conduct to this effect which also serves as a reference point of elements that should be kept in mind when establishing funds dealing with crypto-assets. Among other things, the code will cover custody of crypto-assets, valuation, corporate governance and security.

The EIF is designed for professional, high-net-worth or experienced investors. Each investor would need to invest at least €100,000 in the EIF – or its equivalent in an alternative fiat – or prove a net worth of at least €1m, excluding one's personal residence.

The EIF regime is reliant on EIF Directors and other licensed service providers.

A CIS of this nature will fall within the definition of an alternative investment fund ("AIF") under the Financial Services (Alternative Investment Fund Managers) Regulations 2013, which transposes the EU Alternative Investment Fund Managers Directive. Accordingly, there will be multiple considerations that become relevant, both in terms of the sale, promotion and management of that AIF, as well as the depositary arrangements for AIF units.

Mining

The mining of Bitcoin and other cryptocurrencies is not covered by any specific legal or regulatory framework. Accordingly, it is permitted. As set out above, a cryptocurrency such as Bitcoin, which comes into existence by way of mining without an issuer, does not qualify as E-Money and, as a cryptocurrency that functions solely as a decentralised virtual currency, is also excluded from the Token Regulation Proposals. However, this will ultimately depend on how the mining activity is conducted. For example, given the definition of an AIF, if the mining activities are conducted in a particular way which involves a collective group of people and shared infrastructure, an argument could certainly be made that the arrangement would qualify as a collective undertaking in the sense of the legal meaning.

Border restrictions and declaration

Presently, there are no border restrictions in place on declaring cryptocurrency holdings. Instead these restrictions are usually in place for issues such as transport of goods. Though there are no restrictions in this sense, several of the above authorisation processes required

by the regulations will require "mind and management" to be in Gibraltar, comprising an office with registered employees.

Reporting requirements

No specific reporting requirements are triggered for cryptocurrency payments made in excess of a certain value. However, any threshold amounts may determine the record-keeping requirements that may apply to a business under POCA. Businesses under POCA must report suspicious activity of money laundering.

Estate planning and testamentary succession

The law of succession in Gibraltar is largely based upon the UK Wills Act 1837, which is amended by Gibraltar's Wills Act. Administration of estates is governed by Gibraltar's Administration of Estates Act 1933, consolidated in 1948 (as amended).

The law of Gibraltar as it relates to a deceased person who dies domiciled, closely resembles the laws of England & Wales. Moveable and immoveable property are treated differently. In the case of moveable property, the law of the country where the deceased died domiciled is applied.

There are no death duties to pay in Gibraltar.

Estate planning for cryptocurrency presents its own unique difficulties. Ordinarily, probate is a public process completed upon the presentation of various legal documents. Both of these concepts are in conflict with cryptocurrency.

Estate practitioners are going to have to be aware of the specific issues of cryptocurrency when drafting testaments, the aim being to ensure that the cryptocurrency property is accurately reflected, can be properly transferred upon the death of the holder, and also to ensure that the value of the property can be maintained.

As yet, there is no specific guidance issued in Gibraltar in relation to cryptocurrency and estate planning or succession.

Joey Garcia
Tel: +350 2000 1892 / Email: Joey.Garcia@isolas.gi

Joey is considered one of the pioneers for the regulation in of the virtual currency and distributed ledger technology space. He co-chaired the Government's working group on Blockchain for three years which was specifically established to develop the infrastructure to accommodate a specific DLT regulatory framework in Gibraltar and was recognised by *Chambers & Partners* as one of the top 12 lawyers in the world in this space for 2018. He is also ranked as a Bank 1 Fintech lawyer in Gibraltar for 2018/19 and a member of the prestigious global Wharton Reg@Tech think tank in Philadelphia which brings together fintech academics and Regulators from around the world to discuss issues and current developments in the sector. He is also a founding member of the European think tank (thinkBlocktank) established in Luxembourg, and a member and contributor to the Stablecoin Foundation and working group as well as being a member of the Digital Chamber of Commerce in Washington where he co-authored a segment of their recent report 'Understanding Digital Tokens, market overview and guidelines for policymakers and practitioners'. Joey also contributed to the United Nations ODC manual for law enforcement agencies and participates in the UNODC Southeast Asia working group with his focus on trading platforms and international regulatory developments. Joey is an appointed university lecturer on the subject of DLT regulation for legal students as well as being the vice chair of the Gibraltar Association of New Technologies where he is based.

Jonathan Garcia
Tel: +350 2000 1892 / Email: Jonathan.Garcia@isolas.gi

Jonathan Garcia is a partner at ISOLAS LLP and has a wealth of experience in the financial services and regulatory practice areas. He has been involved in shaping Gibraltar's company legislation which led to a full-scale review and overhaul of the legislation and advised the Government of Gibraltar on introducing a new business entity previously not in existence. He has advised various blockchain start-ups on raising finance through initial coin offerings and, more recently, on obtaining regulatory authorisations for carrying out their business activities and part of the Fintech think tank established by the firm, thinkFintech.gi. Jonathan participated in the Blockchain Bundesverband (Association for the Promotion of Blockchain Technology in Germany) working group on Token Regulation and has been elected to the Board of the Gibraltar Funds and Investments Association (GFIA) as it considers updates to legislative positions and innovative products in the crypto space. He is a member of the Chamber of Digital Commerce and one of the founding members of thinkBlocktank, a Luxembourg-based non-profit organisation, bringing together some of the most respected blockchain and distributed ledger technology experts from more than 15 countries, aiming to provide policy recommendations at an EU and worldwide level which will allow a proper regulated and prosperous ecosystem in regards to Digital Assets.

ISOLAS LLP

Portland House, Glacis Road, GX11 1AA, Gibraltar
Tel: +350 2000 1892 / URL: www.gibraltarlawyers.com

Guernsey

David Crosland & Felicity Wai
Carey Olsen (Guernsey) LLP

Government attitude and definition

The Bailiwick of Guernsey ("**Guernsey**"), as one of the world's leading financial centres, has always been an early adopter of financial innovation and has a reputation for expertise and stability. The first-ever commercial deployment of blockchain technology for the private equity market in early 2017, which was pioneered in Guernsey by Northern Trust and IBM, demonstrates that Guernsey is very much open to new innovation and development.

The Guernsey Financial Services Commission (the "**Commission**") is the body responsible for the regulation of the finance sector. One of the founding objectives of the Commission is to protect the public, and to protect and enhance the reputation of Guernsey as a financial services centre, and one of the ways that the Commission seeks to fulfil this objective is to adhere to the highest international standards of compliance and transparency and to adopt a policy of encouraging promoters of only the highest calibre. Accordingly, the Commission has issued advice calling for caution in the field of digital, virtual or cryptocurrencies ("**Virtual Currencies**") and initial coin offerings ("**ICOs**"). The Commission has indicated that whilst it has a broad policy of encouraging innovation, and is keen to liaise with firms or individuals to discuss potential applications, it believes that there are potential risks in the use of Virtual Currencies, especially for retail customers. The Commission has indicated that it would be cautious about approving applications for ICOs which could then be traded on a secondary market, or the establishment of a digital currency exchange within Guernsey, due to the significant risk of fraud and/or money laundering, and has generally issued advice to investors that when investing in Virtual Currencies they should act with extreme caution – and be prepared to lose the entire value of their investment.

At present, there are no cryptocurrencies backed by Guernsey's government, the States of Guernsey, and Guernsey does not have a central bank. There have been no pronouncements from the States of Guernsey or the Commission which would indicate that Virtual Currencies are given any form of equal status as domestic currency, although it should be noted that there have similarly been no pronouncements that would indicate that Virtual Currencies will *not* be treated as a currency or foreign currency.

In general, funds seeking to invest in Virtual Currencies should be aware that whilst the Commission is generally cautious about the regulatory approach which should be taken in relation to Virtual Currencies and ICOs, Guernsey as a jurisdiction is keen to encourage financial innovation, and provided that an applicant can satisfy the Commission that key controls are in place for the protection of investors, there should be no reason why a responsible fund should not be regulated in Guernsey by the Commission.

Cryptocurrency regulation

Guernsey does not at present have any specific regulatory laws or guidance relating to any form of Virtual Currencies or ICOs, but the nature of Guernsey's existing regulatory laws is such that Virtual Currencies and ICOs could be capable of regulation in a number of ways. The Commission has indicated that it will assess any application for regulation by the same criteria that it uses for any other asset types or structure, and look to ensure that key controls around custody, liquidity, valuation of assets and investor information are in place.

A fund based on Virtual Currencies or the making of an ICO, if required to be regulated, is likely to fall under one of two regulatory regimes; that of the Protection of Investors (Bailiwick of Guernsey) Law, 1987 (as amended) (the "**POI Law**") or the Registration of Non-Regulated Financial Services Businesses (Bailiwick of Guernsey) Law, 2008 (the "**NRFSB Law**").

Regulatory position under the POI Law

Every "collective investment scheme" (a "**fund**") domiciled in Guernsey is subject to the provisions of Guernsey's principal funds legislation – the Protection of Investors (Bailiwick of Guernsey) Law, 1987, as amended (the "**POI Law**") – and regulated by the Commission.

Broadly speaking:

- Every fund domiciled in Guernsey (a "**Guernsey fund**") must be administered by a Guernsey company which holds an appropriate licence under the POI Law (a "**POI Licence**").[1] The administrator is responsible for ensuring that the fund is managed and administered in accordance with the fund documentation.
- Every open-ended Guernsey fund must also appoint a Guernsey company which holds a POI Licence to act as custodian (or trustee, where the Guernsey fund is structured as a unit trust). The trustee/custodian is (with limited exceptions) responsible for safeguarding the assets of the fund and, in some of the rules, to oversee the management and administration of the fund by the administrator.

The POI Law makes it a criminal offence, subject to certain exceptions, for any person to carry on or hold himself out as carrying on any controlled investment business in or from within the Bailiwick of Guernsey without a POI Licence. Additionally, it is an offence for a Bailiwick body to carry on or hold itself out as carrying on any controlled investment business in or from within a territory outside the Bailiwick of Guernsey unless that body is licensed to carry on that business in the Bailiwick and the business would be lawfully carried on if it were carried on in the Bailiwick.

Guernsey funds regulation only applies to "collective investment schemes" – arrangements relating to property of any description which involve:

- the pooling of contributions by investors;
- third party management of the assets; and
- a spread of risk.

Thus arrangements with a single investor or a single asset would not usually be classified as a fund.

The POI Law divides Guernsey funds into two categories:

- "**registered funds**", which are *registered with* the Commission; and
- "**authorised funds**", which are *authorised by* the Commission.

The difference between authorised funds and registered funds is essentially that authorised funds receive their authorisation following a substantive review of their suitability by the

Commission, whereas registered funds receive their registration following a representation of suitability from a Guernsey body holding a POI Licence (the administrator, who scrutinises the fund and its promoter in lieu of the Commission and takes on the ongoing responsibility for monitoring the fund).

The POI Law grants the Commission the power to develop different classes of authorised and registered funds and determine the rules applicable to such classes.

Funds seeking authorisation or registration must therefore satisfy the requirements of the POI Law and (where applicable) the applicable rules specified by the Commission.

The rules governing the different classes of Guernsey funds state whether funds in each class may be open-ended or closed-ended (or whether they may choose from either).

A Guernsey fund is open-ended if the investors are entitled to have their units redeemed or repurchased by the fund at a price related to the value of the property to which they relate (i.e. the net asset value).

There is no prescribed period within which the redemption must occur or the moneys be paid.

Fund types in Guernsey include, but are not limited to:

- Registered Collective Investment Schemes (a registered open- or closed-ended fund governed by the Registered Collective Investment Scheme Rules 2018 and the Prospectus Rules 2018).
- Private Investment Funds (a registered open- or closed-ended fund governed by the Private Investment Fund Rules 2016).
- Class A Funds (an authorised open-ended fund governed by the Authorised Collective Investment Schemes (Class A) Rules 2008). Class A Funds are primarily designed for offering to retail investors.
- Class B Funds (an authorised open-ended fund governed by the Authorised Collective Investment Schemes (Class B) Rules 2013). Class B Funds are the most popular form of fund and are suitable for retail and institutional investors alike.
- Class Q Funds (an authorised open-ended fund governed by the Authorised Collective Investment Schemes (Qualifying Professional Investor Funds) (Class Q) Rules 1998). Class Q Funds benefit from a lighter regulatory regime and are therefore limited to Qualifying (sophisticated) Investors.
- Authorised closed-ended funds (an authorised closed-ended fund governed by the Authorised Closed-Ended Investment Schemes Rules 2008).

Regulatory position under the NRFSB Law

The NRFSB Law provides that if an entity carries out certain "financial services businesses" *in or from within the Bailiwick by way of business* then it must, subject to certain exceptions (see below), register with the Commission. A financial services business which is not registered is guilty of an offence.

The NRFSB Law provides that a business holds itself out as carrying on business in or from within the Bailiwick if:

1. by way of business, it occupies premises in the Bailiwick or makes it known by an advertisement or by an insertion in a directory or by means of letterheads that it may be contacted at a particular address in the Bailiwick;

2. it invites a person in the Bailiwick, by issuing an advertisement or otherwise, to enter into or to offer to enter into a contract or otherwise to undertake business; or
3. it is otherwise seen to be carrying on business in or from within the Bailiwick.

Financial services business

The NRFSB Law only applies to businesses specified in Schedule 1 of the NRFSB Law, the relevant parts of which are summarised as follows:

a) Facilitating or transmitting money or value through an informal money or value-transfer system or network.
b) Issuing, redeeming, managing or administering means of payment, including, without limitation, credit, charge and debit cards, cheques, travellers' cheques, money orders and bankers' drafts and electronic money.

For the purposes of the NRFSB Law, the activities listed will only constitute "financial services businesses" when carried on: (i) by way of business; and (ii) for or on behalf of a customer". "By way of business" is interpreted to mean charging some form of fee for the service provided.

A business will not constitute a "financial services business" for the purposes of the NRFSB Law if it is a "regulated business", meaning business carried on in accordance with a licence granted under: the Banking Supervision (Bailiwick of Guernsey) Law, 1994, as amended; the POI Law; the Insurance Business (Bailiwick of Guernsey) Law, 2002, as amended; or the Insurance Managers and Insurance Intermediaries (Bailiwick of Guernsey) Law, 2002, as amended.

Exceptions

Businesses undertaking "financial services business" on an incidental or occasional basis may not be required to register with the Commission. To be excluded, the business must meet *all of the criteria* below:

1. the total turnover of that business, plus that of any other financial services business carried on by the same person, does not exceed £50,000 per annum;
2. no occasional transactions are carried out in the course of such business, that is to say, any transaction involving more than £10,000, where no business relationship has been proposed or established, including such transactions carried out in a single operation or two or more operations that appear to be linked;
3. the turnover of such business does not exceed 5% of the total turnover of the person carrying on such business;
4. the business is ancillary, and directly related, to the main activity of the person carrying on the business;
5. in the course of such business, money or value is not transmitted or such transmission is not facilitated by any means;
6. the main activity of the person carrying on the business is not that of a financial services business;
7. the business is provided only to customers of the main activity of the person carrying on the business and is not offered to the public; and
8. the business is not carried on by a person who also carries on a business falling within Paragraphs 20 to 23A of Part I of Schedule 1 to the NRFSB Law.

In addition, activities that are merely "incidental and other activities", as listed in Part III of Schedule I of the NRFSB Law, do not constitute "financial services businesses". In short, these relate to activities carried out in the course of carrying on the professions of a lawyer, accountant or actuary.

Requirement to register

This is still an evolving regulatory area in Guernsey, and there is some uncertainty as to whether cryptocurrency falls within the terms set out in b) above (and Schedule 1 of the NRFSB Law), but as these are not exhaustive, the cautious approach would be to assume that this section is wide enough to capture cryptocurrency. Further, a) also refers to transfer of money or value, which is wide enough to capture cryptocurrency.

Application to virtual currencies

A person is treated as carrying on controlled investment business if he engages by way of business in any of the "**restricted activities**" specified in Schedule 2 of the POI Law in connection with any "**controlled investment**" identified and described in Schedule 1 of the POI Law. The scope of this chapter does not permit a detailed look at either of these concepts, but generally "restricted activities" include the promotion of funds, dealings with investments (including buying, selling, subscribing for, borrowing, lending or underwriting an investment) or making arrangements for another person to do the same, or operating an investment exchange, each in connection with a controlled investment, which can include either open- or closed-ended collective investment schemes, or general securities and derivatives.

Whether a POI Licence is necessary in relation to an ICO or a fund engaged in any way with a Virtual Currency will largely turn on whether such a Virtual Currency can legitimately be defined as a security. This is likely to be tested on a case-by-case basis in practice, but consideration may be given to whether a Virtual Currency is asset-based or whether it is a more "pure" cryptocurrency.

Given the uncertainty surrounding the nature of Virtual Currencies in Guernsey, it would be prudent to assume that where an endeavour in Guernsey is not subject to regulation under the POI Law, it will be registrable under the NRFSB Law.

Sales regulation

At present, there are no securities laws or commodities laws in Guernsey regulating the sale of Bitcoin or tokens. The POI Law makes it a general offence to operate an investment exchange in relation to a controlled investment without an appropriate POI Licence, but it is generally unclear if any specific Virtual Currency would constitute a "security" for the purpose of the POI Law, and whilst the Commission have not yet adopted an official position on the matter, it would likely find guidance issued by the prominent financial regulators (the U.S. Securities Exchange Commission, the UK Financial Conduct Authority, etc.) persuasive. Given the general uncertainty in this area, it would be prudent for any individual or firm contemplating engaging in the business of running an investment exchange in relation to any Virtual Currency to consult with the Commission at the early stages.

Taxation

There are no specific laws in Guernsey regulating the taxation of Virtual Currencies, and it is therefore likely that they will be taxed in accordance with general Guernsey taxation principles and provisions.

Guernsey does not have a concept of value added, goods and services or consumption tax, capital gains tax, net wealth/net worth tax or inheritance tax (although there are registration

fees and *ad valorem* duty for a Guernsey Grant of Representation where required). Similarly, apart from transfers of Guernsey real property or transfers of interest in certain unlisted entities (other than collective investment schemes) that have a direct or indirect interest in Guernsey real property, which may (subject to exemption) attract a document duty, no stamp or transfer taxes are applicable. Withholding taxes are payable at a rate of 20% solely in relation to the payment of dividends by a Guernsey company to a Guernsey resident individual (unless the company has exempt status), but are not payable in relation to the payment of dividends to non-residents, or on interest, royalties or service fees. Guernsey does not have specific anti-avoidance rules but does have a broad general anti-avoidance provision which targets transactions where the effect of the transaction or series of transactions is the avoidance, reduction or deferral of a tax liability.

Guernsey has introduced economic substance legislation for accounting periods commencing on or after 1 January 2019. The details of this legislation are beyond the scope of this chapter but economic substance requirements should be considered in the context of structures containing Guernsey tax-resident companies.

It would therefore be prudent to assume that any income arising from a Virtual Currency (whether in the form of a Virtual Currency or otherwise), or any income arising in the form of a Virtual Currency, will be taxable in line with Guernsey income tax provisions and valued at the appropriate spot rate on the date that the income arises, although the Guernsey Income Tax Office has not made a formal statement on the matter and may determine that another valuation method should be used.

Corporate Income Tax

A company is treated as tax-resident in Guernsey if:

1) it is incorporated in Guernsey;
2) it is incorporated outside of Guernsey but is "centrally managed and controlled" in Guernsey (control for these purposes refers to strategic control, and is generally exerted by directors, making the location of board meetings and other decision-making key); or
3) it is incorporated outside of Guernsey but is directly or indirectly controlled by one or more Guernsey resident individuals (control in this case referring to shareholder control instead of director control, and generally applies where one or more natural persons are able to secure by the means of holding shares that the affairs of the company are conducted in accordance with their wishes).

Companies resident in Guernsey are subject to income tax on their worldwide income (although certain reliefs are available to prevent double taxation). Most companies that are tax-resident in Guernsey are taxed at a standard rate of 0%, but income arising from certain activities is taxed at 10% or 20%. This includes (but is not limited to) income arising from fund administration, investment management (except in relation to funds) and fiduciary business (each of which are taxed at the 10% rate), and income arising from large retail businesses (taxable profits in any year exceeding £500,000), the ownership of land and buildings in Guernsey, regulated trading activities such as telecommunications or the importation and/or supply of gas and hydrocarbon oil in Guernsey (which are taxed at the 20% rate).

Unit trusts are treated as companies for Guernsey income tax purposes and limited partnerships and limited liability partnerships are considered tax-transparent, and so are not taxable entities in Guernsey.

There is an exemption regime available for collective investment schemes, entities beneficially owned by collective investment schemes, and entities established for the purpose of certain specified activities relating to a specific collective investment scheme. Applications for this exemption must be made annually and attract a payment of an annual fee currently fixed at £1,200. Where an exemption is granted, the entity is treated as not being resident in Guernsey for tax purposes and is not liable for Guernsey tax on non-Guernsey source income (including Guernsey bank deposit interest).

Personal income tax

Individuals in Guernsey pay income tax at a flat rate of 20%. The personal income tax year is based on the calendar year, and income tax returns must be filed by 30 November of the year following the relevant tax year (which filing can be made electronically or on paper).

There are different classes of residence which may affect an individual's tax treatment. Individuals may be:

- "principally resident" – they are in Guernsey for 182 days or more in a tax year, or are in Guernsey for 91 days or more in a tax year and have spent 730 days or more in Guernsey over the four prior tax years;
- "solely resident" – they are in Guernsey for 91 days or more in a tax year, or are in Guernsey for 35 days or more in a tax year and have spent 365 days or more in Guernsey over the four prior tax years, and in either case have not spent 91 days or more in any other jurisdiction in the tax year; or
- "resident only" – they would be treated as solely resident in a tax year, but they have spent 91 days or more in another jurisdiction for that tax year.

Individuals who fall within the scope of any of the above will pay Guernsey tax on their worldwide income, although foreign tax relief is available. Individuals who are "resident only" can elect to pay a standard charge of £30,000, which has the effect of exempting them from Guernsey income tax on their worldwide income (they will still have to pay tax on any Guernsey-source income).

A personal allowance is available for individuals of £11,000 (although earners of more than £100,000 have their allowance reduced by £1 for every £5 exceeding this limit. Certain reliefs are available for pension contributions and mortgage interest which are beyond the scope of this chapter. A Guernsey resident individual can elect for a cap on their income tax liability in relation to their worldwide income (but not in relation to income arising on Guernsey real property).

FATCA and CRS

Guernsey is party to an intergovernmental agreement with the United States regarding the Foreign Account Tax Compliance Act of 2009 ("**FATCA**") and implemented FATCA due diligence and reporting obligations in June 2014. Under FATCA legislation in Guernsey, Guernsey "financial institutions" are obliged to carry out due diligence on account holders and report on accounts held by persons who are, or are entities that are controlled by, one or more natural persons who are, residents or citizens of the United States, unless a relevant exemption applies.

Guernsey is also a party to an intergovernmental agreement with the United Kingdom in relation the United Kingdom's own version of FATCA, which it also implemented in June 2014. However, the United Kingdom's version of FATCA has now been superseded by the adoption by Guernsey (alongside numerous jurisdictions) of the much broader global Common Reporting Standard ("**CRS**").

Guernsey is a party to the OECD's Multilateral Competent Authority Agreement regarding the CRS and implemented the CRS into its domestic legislation with effect from 1 January 2016. Under CRS legislation in Guernsey, Guernsey "financial institutions" are obliged to carry out due diligence on account holders and report on accounts held by persons who are, or are entities that are controlled by, one or more natural persons who are residents of jurisdictions that have adopted the CRS, unless a relevant exemption applies.

It is unclear at this stage what, if any, reporting should take place in relation to Virtual Currencies under FATCA or CRS, and much will turn on whether individual Virtual Currencies are "securities" for FATCA and CRS purposes. Until this point has been settled, it would be prudent to adopt a conservative approach.

Money transmission laws and anti-money laundering requirements

All Guernsey individuals and firms are subject to the Drug Trafficking (Bailiwick of Guernsey) Law, 2000 (as amended), the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002 (as amended) and the Disclosure (Bailiwick of Guernsey) Law, 2007. These laws contain various offences which arise should a financial service business, a non-financial service business or a nominated officer in a financial service business fail to make a disclosure to Guernsey's Financial Intelligence Unit, the Financial Intelligence Service where they have knowledge or suspicion (or reasonable grounds for knowledge or suspicion) of money laundering or terrorist financing. It is also an offence to disclose information or any other matter which is likely to prejudice an investigation by law enforcement.

In addition, regulated entities in Guernsey are bound by various rules and regulations – in particular, Guernsey's anti-money laundering and counter-terrorist financing legislation, including the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations, 2008 and the Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing (current edition June 2019) published by the Commission (the "**Handbook**").

The full scope of Guernsey's anti-money laundering regime, counter-terrorist financing legislation and of all of the applicable laws, rules and regulations applicable to an entity regulated under the POI Law or the NRFSB Law is beyond the scope of this chapter but the key points to consider are as follows:

- a regulated entity should appoint a money laundering reporting officer ("**MLRO**") and Money Laundering Compliance Officer ("**MLCO**") resident in Guernsey;
- the board or equivalent of the entity will have effective responsibility for compliance with Guernsey's anti-money laundering regime and counter-terrorist financing legislation and must take responsibility for the policy on reviewing compliance, consider the appropriateness and effectiveness of compliance and the review of compliance at appropriate intervals, and take appropriate measures to keep abreast of and guard against the use of technological developments and new methodologies in money laundering and terrorist financing schemes. The board may delegate some or all of its duties but must retain responsibility for the review of overall compliance with Guernsey's anti-money laundering and counter-terrorist financing legislation requirements;
- the entity will require appropriate customer take-on policies; procedures and controls will need to be adopted to sufficiently identify and verify identity (to a depth

appropriate to the assessed risk of the business relationship and occasional transaction) of all of its existing and new customers, with enhanced measures in relation to certain customers;

- all transactions and activity will need to be monitored on an ongoing basis to include all business relationships (on a risk-based approach), with high-risk relationships being subjected to an appropriate frequency of scrutiny, which must be greater than may be appropriate for low-risk relationships;
- appropriate and effective policies, procedures and controls must be established in order to facilitate compliance with the reporting requirements of the regulations; and
- appropriate employee screening and training policies will need to be in place.

The Handbook permits the use of technology for customer due diligence, and indeed as referenced above, Guernsey was one of the earliest adopters of blockchain technology in the private equity market for administration purposes. Other administrators have since adopted technologically backed systems for undertaking customer due diligence, and in particular, private equity fund administrator Ipes has set up the ID Register, an online platform for connected due diligence, FATCA and investor reporting.

Promotion and testing

The Commission has introduced the free "Innovation SoundBox" to serve as a hub for enquiries regarding innovative financial products and services, and encourages firms or individuals to use this facility to discuss potential applications in the field of Virtual Currencies at an early stage. No fees are charged for engaging with the Innovation SoundBox.

Ownership and licensing requirements

There are no specific restrictions in Guernsey on investment managers holding cryptocurrencies for investment purposes, and as the regulatory position is unclear, individuals should approach the Commission on a case-by-case basis to determine whether they are required to obtain a POI Licence in order to hold cryptocurrency as an investment advisor or fund manager. The above section, headed "Cryptocurrency regulation", provides more detail on when an individual or entity is required to be licensed under the POI Law, and the section headed "Money transmission laws and anti-money laundering requirements" provides further detail about applicable anti-money laundering and counter-terrorist financing requirements.

Mining

There are no specific restrictions on the mining of Virtual Currencies in Guernsey.

Border restrictions and declaration

There are no specific border restrictions or declarations which must be made on the ownership of Virtual Currencies in Guernsey. However, the Cash Controls (Bailiwick of Guernsey) Law, 2007 (as amended) (the "**Cash Controls Law**") does set out requirements for any person who is entering or leaving Guernsey who is carrying cash in any currency to the equivalent value of €10,000 or more to make a declaration to a Guernsey Border Agency Officer. The definition of "cash" under the Cash Controls Law is broad, including banknotes, bullion, ingots and coins (whether or not in circulation as a medium of exchange) and it is

not clear whether Virtual Currencies would be caught under such a provision. Despite this, it is likely that the Cash Controls Law will not apply to the movement of Virtual Currencies, as to be caught under the Cash Controls Law the cash must be carried in baggage or on one's person and, given the purely digital nature of many Virtual Currencies, it is unclear whether it would be conceptually possible for it to be "carried".

Reporting requirements

There are no specific Guernsey reporting requirements for cryptocurrency payments made in excess of a certain value. However, any transactions should be monitored to ensure that they are compliant with anti-money laundering and countering the financing of terrorism procedures.

Estate planning and testamentary succession

At present, Virtual Currencies in Guernsey are not treated differently than any other asset on the death of the holder. In principle, therefore, if an estate is subject to Guernsey succession laws, Virtual Currencies would be treated in the same way as any other asset and distributed in accordance with the will or intestacy of the holder under Guernsey law. There may, however, be practical difficulties with both locating and distributing any Virtual Currencies which may be stored in virtual wallets or protected by other forms of security, and the means for transferring Virtual Currencies to a successor in title may largely depend on the relevant issuer or exchange.

* * *

Endnote

1. Under the POI Law, such an administrator is referred to as a "designated manager", but in the rules governing the various classes of funds in Guernsey, such an administrator is sometimes described as a "designated administrator". For the sake of convenience, we will refer to them as an "**administrator**" throughout this chapter.

David Crosland, Partner
Tel: +44 1481 741556 / Email: david.crosland@careyolsen.com

David undertakes a wide range of corporate transactions with a particular experience in the launch of investment funds. He is regularly instructed by fund managers, UK and international law firms and other financial services firms on the launch, administration, restructuring and listing of both closed and open-ended investment funds. David was listed in the *International Who's Who of Private Funds Lawyers 2018*. In addition to fund formation, David frequently advises on corporate real estate and general corporate matters, including those with a heavy regulatory content.

David trained at Clifford Chance in London, qualifying as an English solicitor in the Private Funds Group in 2004. While there, he specialised in the establishment of institutional closed-ended investment funds, particularly private equity, real estate and infrastructure funds. In 2006, he spent nine months on secondment at ABN AMRO advising on the structuring and launch of institutional fund-linked investment products, before joining Carey Olsen in May 2007. David became a partner in 2013.

Felicity Wai, Associate
Tel: +44 20 7614 5631 / Email: felicity.wai@careyolsen.com

Felicity is an associate in Carey Olsen's Guernsey Corporate team. She assists on a range of corporate, commercial, banking and finance matters. Felicity joined Carey Olsen in 2016, having trained and qualified as a solicitor in the UK. Having initially read Modern History at Merton College, Oxford, she obtained her GDL (Commendation) at City Law School, London, before completing her LPC at the University of Law in Guildford (Distinction), where she was awarded prizes in Commercial Litigation and Commercial Dispute Resolution.

Felicity is a member of the Law Society of England and Wales.

Carey Olsen (Guernsey) LLP

PO Box 98, Carey House, Les Banques, St Peter Port GY1 4BZ, Guernsey
Tel: +44 1481 727272 / Fax: +44 1481 711052 / URL: www.careyolsen.com

Hong Kong

Yu Pui Hang (Henry Yu)
L&Y Law Office / Henry Yu & Associates

Government attitude and definition

Cryptocurrencies (often called "**coins**" or "**tokens**", and collectively referred to in colloquial manner as "**crypto**") and blockchain technology (certain blockchain technologies may also be referred to as "**Distributed Ledger Technology**" or "**DLT**" for short) have, in their short life span of the past decade, created a new economy which opened a market of new opportunities.

The first cryptocurrency to enter the market was Bitcoin, and it has introduced an effective way to transfer value over the internet by relying on peer-to-peer and distributed verification. Ever since Bitcoin there have been other blockchain-based projects that have introduced new innovations to blockchain technology (these cryptocurrencies are often referred to as "**Altcoins**"), one of the most noteworthy being Ethereum, which allows for the deployment and execution of software on the blockchain called smart contracts. As a result of this growth, many private and public enterprises have formed in Hong Kong to take advantage of the opportunities offered by this new technology, and to leverage Hong Kong's unique position in business, technology and law.

Hong Kong is a unique jurisdiction, as it leverages the "one country, two systems" principle, which gives it a high degree of autonomy. The Basic Law of Hong Kong enshrines various free market principles safeguarding its position as an international financial centre. Thus, given its free market foundations, the legislative council in Hong Kong has yet to pass any new laws and regulations that specifically deal with cryptocurrencies or cryptocurrencies business. However, the rapidly expanding cryptocurrencies or cryptocurrencies businesses market caught the Hong Kong government's attention, resulting in enforcement actions being taken under the existing legislation and new regulatory regimes being introduced with the goal of better protecting investors' interests.

As there is no new primary legislation to directly regulate cryptocurrencies in Hong Kong, there is a certain degree of uncertainty on the legal definition within the statutory law. Nevertheless, there are secondary sources of law, including the designation set by the Secretary for the Financial Services and Treasury Bureau ("**FSTB**"), Professor K C Chan, who designated Bitcoin (specifically) as a "virtual commodity". In a press release, the Hong Kong Monetary Authority ("**HKMA**") stated in 2015 that Bitcoin and other similar currencies were not legal tender but "virtual commodities", and as Bitcoin has no backing – either in physical form or by the issuers – it cannot be qualified as a means of payment or electronic money. The HKMA, which acts as Hong Kong's *de facto* central bank, has also stated that it has no plans to issue any central bank-backed cryptocurrency. On the other hand, the Hong Kong Securities and Futures Commission ("**SFC**") had issued a number of

statements in 2018 and 2019 in an attempt to monitor the activities involving cryptocurrency, including a statement dated 1 November 2018 titled "Statement on Regulatory Framework for Virtual Asset Portfolios Managers, Fund Distributors and Trading Platform Operators" (the "**2018 SFC Statement**") and a statement dated 28 March 2019 titled "Statement on Security Token Offerings" (the "**2019 SFC Statement**"), both of which gradually show the Hong Kong government's stance towards cryptocurrency and cryptocurrency businesses. Interestingly, in the 2018 SFC Statement, the concept of a new asset class called "virtual assets" was introduced, which refers to "a digital representation of value (the "**Virtual Assets**"), and examples include 'cryptocurrencies', 'crypto-assets', 'digital tokens' and 'digital tokens (such as digital currencies, utility tokens or security or asset-backed tokens) and any other virtual commodities, crypto assets and other assets of essentially the same nature'. This seems, to a certain extent, to expand on the HKMA's categorisation of "virtual commodities".

The most observable attitude made by the government and the various regulatory authorities is to warn the public against the uncertainties in the cryptocurrency marketplace. The earliest observable public warning was made by the Hong Kong Police Force in 2014 which highlighted that bitcoins are not money and are not regulated by the HKMA; the volatility of the prices of Bitcoin; the cybersecurity risks associated with dealing with Bitcoin; and any potential fraud especially with "Bitcoin Mining Contracts". Any suspected proceeds of crime should be reported to the Joint Financial Intelligence Unit ("**JFIU**"), a joint unit composed of the Hong Kong Police Force and the Hong Kong Customs and Excise Department ("**CED**"). The press release issued by the HKMA, as referred to above, contained a similar warning about the volatile nature of bitcoins.

With the advent of Ethereum and other smart contract blockchain platforms, new applications of cryptocurrency such as initial coin offerings, or token sale (collectively "**ICO(s)**") become more widely popular in Hong Kong and globally. As many ICO issuers have established their base of operations in Hong Kong and have opened their campaigns to Hong Kong residents, the SFC, the local securities regulator, has issued a statement on ICO on 5 September 2017 warning the public about: (i) the risk of participating in ICO campaigns; (ii) that ICO tokens that possess features of "securities" as defined under the Securities and Futures Ordinance (Cap. 571) (the "**SFO**") would require to be authorised by the SFC, unless an exemption applies; and (iii) that dealing and advising on "securities"-based ICOs would be a "regulated activity" under the SFO and therefore such activity should only be carried out by licensed corporations.

In subsequent public communications, the SFC has stated that it is monitoring the cryptocurrency space and will enforce any relevant provision under the SFO if necessary. Aside from the statements given by the SFC, in early 2018 the Investor Education Centre and the FSTB launched an education campaign on ICOs and cryptocurrencies. The campaign's key message is not to buy something you do not understand. We can therefore see that, the Hong Kong government's view towards cryptocurrencies, that do not possess features of securities, can be described as relatively passive. The regulatory authorities have not called for new legislation to regulate cryptocurrencies, as current laws are still applicable. For now, it is observable that the government and the regulatory authorities aim to educate the public about the risks involved in the cryptocurrency economy and still assessing the suitability of the currently available legislation in regulating cryptocurrencies and protecting the public.

Notwithstanding the above, in 2018, the cryptocurrency economy saw the introduction of security tokens offering ("**STO**"), an alternative to ICOs whereby the tokens being sold to

participants are of securities nature (commonly referred to as "**Security Tokens**"). STO has also introduced the cryptocurrency economy to other new business opportunities including cryptocurrency exchanges that wish to provide trading services to these Security Tokens and technical issuance platforms. Such market trend initiated a range of new regulatory approaches and initiatives to promote fintech development from the SFC and several agencies, given that the Security Tokens would seemingly fall under the jurisdiction of the SFC as bestowed to them through the SFO, including the additional licensing conditions on licensed corporation and the expansion of the regulatory "sandboxes" (as discussed below) as initiated in the 2018 SFC Statement. Hong Kong now appears to take a more proactive approach in exploring the regulation over virtual assets, in particular Security Tokens.

Cryptocurrency regulation

As mentioned above, the HKMA and the SFC have recognised bitcoins and other currencies like it as a "virtual commodity" (it is not clear if and how this extends to other Altcoins), which is a sub-category of "virtual assets" and Hong Kong has not created new legislation or regulations to define those terms. The SFC has not made further clarification on which tokens or coins would fall under the new asset class of "virtual asset" but has admitted that many virtual assets do not necessarily constitute "securities" or "futures contracts" for the purpose of the SFO (which the SFC has now specifically confirmed Bitcoins and Ether as examples), which may be referred to as "**Non-SF Virtual Assets**".

Certain businesses which are common in the cryptocurrency economy are ordinarily regulated in Hong Kong, and thus a cryptocurrency company that wishes to participate in such market must abide by such specific legislation.

Hong Kong does not regulate private possession or transfer of cryptocurrencies between private individuals, on the assumption that the cryptocurrency in question was obtained and is transferred in good faith (cryptocurrencies are subject to anti-money laundering laws which are discussed below).

One of the most noteworthy regulated industries that is quite pervasive in the cryptocurrency economy is the ICO space. ICOs are campaigns where issuers sell blockchain-based tokens to potential participants in exchange for other cryptocurrencies such as Ether or Bitcoin. The purpose of conducting an ICO is to crowdsource funds for a specific project that the issuer aims to develop, and the tokens have certain "utility" within such project; therefore the tokens sold in ICOs are commonly referred to as "**Utility Tokens**". One example is the OAX project (https://www.oax.org/en), which was considered the first ICO in Hong Kong. The conventional ICO follows the ERC-20 Ethereum standard and the sale is conducted through a web portal. Aside from the technical elements, the issuers also circulate several documents to the public during the ICO period such as the white paper (or even technical white paper) and the token sale agreement, if any.

Another type of campaign that is similar to ICOs is STOs, which has risen to attention in recent years. The issuance process of a STO is similar to an ICO save that the tokens being exchanged in return would be Security Tokens, i.e. it possesses the characteristics of equity, debt, structured products or collective investment scheme (the common types of securities under SFO), therefore would be subject to the provisions of the SFO. The offering of the Security Tokens would therefore need to be conducted in compliance with the SFO and in a similar manner as the offering of traditional securities products, including but not limited to the requirement of dealing through intermediaries that are licensed with the SFC and the

requirement of publishing an offering memorandum (or "prospectus" depending on the type of offering being made or whether certain exemptions under the SFO have been relied on). As an industrial practice, the documents commonly found in an ICO, i.e. the White Paper, would also be published.

In general, Hong Kong does not prohibit the possession or trading of Non-SF Virtual Assets, as Bitcoins and currencies similar to it are considered to be virtual commodities and not electronic money, provided the cryptocurrencies are possessed and traded in good faith. There are other regulatory considerations depending on the use of cryptocurrencies, such as the running of ICO campaigns or trading Bitcoin futures contracts.

Sales and distribution of cryptocurrencies

As remarked in the paragraph above, the government has a duty to safeguard the free flow of capital as enshrined under Article 112 of the Hong Kong Basic Law. Trade controls and consumer protection are predominantly controlled by the CED, and the basic trading of cryptocurrencies is subject to oversight by CED. The applicable legislation and regulations on the trading of cryptocurrencies will depend on the actual features of each particular cryptocurrency; for example, some tokens commonly known as "ICO tokens" may actually be Security Tokens instead by nature, i.e. it takes the form of or possesses features that are common in other financial products such as shares, debts, loan notes, interests in a fund or securitisation of another asset or asset class, if not correctly structured. These tokens will therefore be regulated by the applicable legislation such as the SFO.

Trading of Bitcoin in Hong Kong is commonly done on cryptocurrency exchanges, on over-the-counter ("**OTC**") desks and peer-to-peer ("**P2P**") platforms with both consumers and institutional participants; depending on the nature of the transaction, different legislation will apply. In most business-to-consumer transactions conducted on exchanges and OTC desks, general consumer protection laws such as the Sales of Goods Ordinance (Cap. 26) and the Trade Descriptions Ordinance (Cap. 362) apply, with the former specifying the procedures and rights of parties in the transaction, and the latter setting out rules on the prevention of unfair trade practices. Business-to-business transactions are not covered *per se* by the above statutes which are mostly aimed at protecting individual consumers.

Certain commodity exchanges are prohibited from establishing in Hong Kong, under the Commodity Exchanges (Prohibition) Ordinance (Cap. 82) with the list of prohibited commodities being specified in the Schedule of the above Ordinance ("**Schedule**"), e.g. barley, cocoa, coffee, copper, cotton, gold, lead, maize, oats, platinum, rice, rubber, silver, oil seeds and vegetable oils, sugar, timber, tin, wheat, zinc, jute, frozen meat, poultry and fish and soybeans. To date, cryptocurrency (or "virtual commodity") has not been added to the Schedule, and therefore there are no statutory prohibitions on operating exchange in Hong Kong for trading of cryptocurrencies, which are classified as virtual commodities.

Cryptocurrency exchanges and OTC desks do also observe other legal requirements such as anti-money laundering and counter-terrorist financing and customer due diligence checks (further discussed below). There are certain cryptocurrencies that will be restricted in trading on the abovementioned platforms; the first type of restricted cryptocurrencies is Security Tokens.

In the 2019 SFC Statement, the SFC stated that Security Tokens are normally digital representations of ownership of assets (e.g. gold or real estate) or economic rights (e.g. a share of profits or revenue) utilising blockchain technology. The SFC considers that Security Tokens are likely to be "securities" as defined under the SFO and as such are

subject to the securities laws of Hong Kong. Under Schedule 1 of the SFO, there are different categories of "securities", mainly:

Shares – shares are defined under the Companies Ordinance (Cap. 622) and in the common law relate to an equitable ownership interest of a company; such interest gives the shareholders certain rights, as stipulated in the company's articles of association. A cryptocurrency token can form a blockchain-based share certificate, if each token unit represents, *inter alia*, legal or beneficial ownership in the company, a right to vote in shareholders' meetings, and a right to receive dividend or some kind of distribution. Public offerings of such cryptocurrencies would be restricted on the basis that in Hong Kong, under the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32)("**CWUMPO**"), a person shall not issue any form of application for shares in (or debentures) of a company to the public unless the form is issued with a prospectus which complies with the requirements under the same ordinance, unless one of the exemptions is applicable.

- ***Debentures*** – encompasses various debt-based instruments issued by a company. This category is quite broad as it is not necessary for a debenture to be expressly described as one; all that is required is that the instrument evidences a debt obligation by the company, whether or not the debt is charged against the company. Cryptocurrencies that share such features could be considered as debentures and, as mentioned above under the CWUMPO, should be distributed subject to similar restrictions.
- ***Structured Products*** – mainly include products and investment agreements such as equity-linked deposits or equity-linked investments (sometimes a hybrid of securities and regulated investment agreements). "Structured product" is defined under the SFO to instruments which return or amount due or the method of settlement is determined by the references to other price, value, level, securities, commodity, index, property, interest, rate, currency exchange rate or futures contracts. On a *prima facie* basis, this would appear to cover most derivatives products surrounding cryptocurrencies that are surfacing in the market over the last couple of years, but subject to further clarification from the SFC.
- ***Regulated Investment Products*** – as broadly defined in Schedule 1 of the SFO to include any contract that requires an investor to enter into with a profit calculated by changes in the value of any property. This would appear to be a catch-all product to cover most investment contracts whereby the investors are paying for the expectation of profit, in particular applicable to some cryptocurrencies projects where the elements of profits are heavily focused on, in contrast to focusing on the utility functions of the cryptocurrencies.
- ***Collective Investment Schemes*** ("**CIS**") – the provisions concerning CIS products aim to regulate investment products that are collective in nature; examples of such products include unit trusts and mutual funds. Unlike the definition of "shares" above, a CIS may form if the definition under Schedule 1 of the SFO, which includes four components, is satisfied:
  - there must be an "arrangement of property";
  - the participating persons do not have day-to-day control over the management of the property, whether or not they have the right to be consulted or to give directions in respect of such management;

- the property is managed in whole or on behalf of the person operating the arrangements; and/or contributions and profits or income are pooled; and
- the purpose or effect, or the pretended purpose or effect, is to enable the participating persons to receive: (a) profits, income or other returns represented to arise; or (b) payments from the acquisition or disposal of the property.

Any person or intermediary ("**Intermediary**") who carries out business involving Security Tokens in Hong Kong (or targeting Hong Kong investors) is required to be licensed or registered for regulated activities. Any person who markets and distributes Security Tokens (whether in Hong Kong or targeting Hong Kong investors) is required to be licensed or registered for type 1 regulated activity (dealing in securities) under the SFO. Intermediaries being involved in STOs are reminded to comply with all existing legal and regulatory requirements in Hong Kong, in particular:

- ***Professional investors only***. Under the current market, Security Tokens are normally offered to professional investors only. The 2019 SFC Statement confirms that Type 1 Intermediaries should only target clients who are professional investors as defined under the SFO.
- ***Suitability obligations***. When the Intermediary makes recommendation or solicitation of a Security Token, it shall ensure the suitability of its recommendation or solicitation for that client is reasonable in all the circumstances having regard to information about the client of which the Intermediary is or should be aware through the exercise of due diligence.
- ***Complex products***. The SFC considers that Security Tokens would be regarded as "complex product", which is defined as "an investment product whose, terms, features and risks are not reasonably likely to be understood by a retail investor because of its complex structure". Nevertheless, it is generally the Intermediary's (in particular those that operates through an online platform) duty to assess whether a product is a "complex product" or not. If the Intermediary comes to the conclusion that any Security Token it intends to distribute is a "complex product", it should adopt additional investor protection measures to better protect clients' interests by ensuring that clients are well informed about the key nature, risks and features of such Security Token and such Security Token is suitable for them.
- ***Product due diligence***. Intermediaries distributing Security Tokens should conduct proper due diligence for the purpose of developing an in-depth understanding of the STOs and also ascertaining the risk return profile of such STOs.
- ***Information for clients***. In order to help clients make an informed investment decisions, Intermediaries should make clear and adequate disclosure of the material information relating to the STOs in an easily comprehensible manner in order to help clients making an informed investment decision, including but not limited to: providing clients with access to up-to-date STO offering documents and other information; providing clients with material information as soon as reasonably practicable to enable clients to appraise the position of their investments, etc. Intermediaries should also provide prominent and clear warning statements to clients prior to and reasonably proximate to the point of sale or advice.

Should there be any failure to comply with the legal and regulatory requirements during the distribution of STOs, the fitness and properness of the Intermediary may be affected and SFC disciplinary action may follow.

Furthermore, in compliance with the "Circular to Intermediaries on compliance with Notification Requirements" issued by the SFC on 1 June 2018, the SFC has confirmed that any service involving trading of crypto-assets would be considered as a significant change in the nature of business of the Intermediary and would be subject to the notification requirements under the Securities and Futures (Licensing and Registration) (Information) Rules (the "**Information Rules**"), and the 2019 SFC Statement urges the Intermediary to notify the SFC should they wish to be engaged in cryptocurrency-related businesses.

Given the broad nature of the CIS definition (as discussed above), it could be argued that many ICO campaigns could fall within the parameters of the CIS definition, thus being a Security Token. If this is the case, the issuer may not make the ICO open to the public without prior authorisation from the SFC and be in compliance with the SFO as mentioned above. In March 2018, the SFC halted the ICO operated by a company called Black Cell Technology Limited ("**Black Cell**"), which allowed token-holders to redeem their tokens into equity shares in Black Cell. The SFC has considered this arrangement to be a CIS under the circumstances. In the above case, Black Cell has undertaken not to proceed with the ICO. It is important to note that in light of the SFC's numerous statements to date, the regulators are closely observing the ICO and broader cryptocurrency economy to ensure that the relevant securities legislation is complied with, thus cryptocurrency exchange must conduct sufficient legal due diligence to ensure the cryptocurrencies they allow on their marketplace are not considered "securities" otherwise they will also be subject to the provisions under SFO.

Aside from securities, other types of financial instrument markets have also developed in the cryptocurrency economy. Bitcoin-based derivatives products have enjoyed considerable popularity, trading on exchanges such as Bitmex. Bitcoin futures gained even more popularity in late 2017 when CBOE and CME started offering Bitcoin futures contracts. The SFC stated in its announcement on 11 December 2017 that any intermediary in Hong Kong that offers brokerage services for the above Bitcoin futures will be required to obtain the appropriate licences from the SFC (namely "Type 2" when dealing with such futures contracts, and "Type 5" when advising on such futures contracts).

In the broad sense, trading of cryptocurrencies is not restricted in Hong Kong so long as they are classified as "virtual commodities" (and not Security Tokens) and do not infringe on any applicable securities and futures legislation. Cryptocurrency exchanges are not subject to legislation that prohibits the operation of commodity exchanges (but are subject to the laws on commodity exchange as mentioned above).

Virtual asset funds (commonly known as crypto funds)

Along with the 2018 SFC Statement, the SFC issued an appendix titled "Regulatory Standards for Licensed Corporations Managing Virtual Asset Portfolios" (the "**Regulatory Standards**") and a "Circular to intermediaries: Distribution of virtual asset funds" (the "**Circular**"), which focused on the SFC's stance and the regulatory standards to be imposed on: (i) Intermediaries that are licensed to manage portfolios or intend to manage portfolios that invest in virtual assets (the "**Type 9 Intermediaries**"); and (ii) Intermediaries that are licensed to distribute funds or intend to distribute virtual asset funds in Hong Kong (the "**Type 1 Intermediaries**").

Interestingly, the SFC has confirmed that, where a firm only manages a "portfolio" (which covers collective investment schemes and discretionary accounts in the form of an investment mandate or a pre-defined model portfolio) which invests solely in Non-SF Virtual

Assets, it is not required to be licensed or registered for Type 9 regulated activities (asset management) (the "**Type 9 Licence**"), but where a firm manages a fund of funds (even with the underlying fund investing solely in the Non-SF Virtual Assets), the firm is required to be registered for Type 9 Licence (asset management).

Pursuant to the 2018 SFC Statement and the Regulatory Standards, the SFC has developed a set of principles-based standard terms and conditions which would be imposed as licensing conditions (the "**VA Licensing Conditions**") on the Type 9 licensed intermediaries (the "**Type 9 VA Licensed Intermediary** ") which manage or plan to manage portfolios with: (i) a stated investment objective to invest in Virtual Assets; or (ii) an intention to invest 10% or more of the gross asset value (the "**GAV**") of the portfolio (the "**De Minimus Threshold**") in Virtual Assets (collectively, the **"Virtual Asset Portfolio(s)**"). The key VA Licensing Conditions to be imposed include but are not limited to (i) only professional investors are allowed, with proper risk disclosure, (ii) no less than HK$3 million liquid capital, (iii) appropriate portfolio valuation principles must be adopted, (iv) an independent, experienced and capable auditor must be appointed, and (v) an appropriate custodial arrangement must be in place. In particular in relation to condition (ii), a Type 9 VA Intermediary which holds Non-SF Virtual Assets (which, strictly speaking, does not constitute "client assets" under the SFO) for portfolios under its management shall be required to maintain a required liquid capital of not less than HK$3 million (or its variable required liquid capital, whichever is higher).

In addition, the SFC has also confirmed in the Regulatory Standards and the Circular that if a firm distributes a fund under its management that solely invests in Non-SF Virtual Assets in Hong Kong (i.e. the management of such fund's portfolio does not require a Type 9 Licence), it is still required to be licensed or registered for Type 1 regulated activities (dealing in securities) ("**Type 1 VA Licensed Intermediary**") and depending on whether it is authorised by the SFC, the Type 1 VA Licensed Intermediary is required to comply with certain requirements.

Such regulatory approach from the SFC has indicated its acceptance of virtual asset funds being distributed and managed in Hong Kong provided the requirements imposed are fulfilled. As a result, the Hong Kong market has seen a surge of Type 9 Intermediaries making application to the SFC to notify the SFC of its intention to change the nature of its business, in the view of providing services to virtual asset funds. Consequently, Hong Kong may be a good alternative jurisdiction for many fund managers to consider should they wish to launch virtual asset funds, in light of the increasing difficulties in other offshore jurisdictions when dealing with virtual assets.

Taxation

In general, there is no capital gains tax payable from the sale of financial instruments in Hong Kong. That being said, any Hong Kong-sourced income from frequent cryptocurrency trading in the ordinary course of business may be treated as income in case of individual clients, and profits in case of a corporation, and subject to income tax and profits tax respectively, regardless of whether the trading is made in exclusive cryptocurrency or fiat-to-cryptocurrency exchanges. Pursuant to a press release dated 3 April 2019, the government confirmed that the Inland Revenue Department does not maintain statistics specifically on tax payable by persons carrying on virtual asset-related activities and each case should be assessed on the basis of its own individual facts and circumstances. The Inland Revenue Department would also, if necessary, seek relevant information from other tax authorities

through the exchange of information mechanism under tax treaties to assess the situation. Regardless, to date, the Inland Revenue Department has not issued specific guidelines on how it would treat cryptocurrencies for the purposes of tax assessment.

Money transmission laws and anti-money laundering requirements

Many jurisdictions have implemented stringent anti-money laundering and counter-terrorist financing ("**AML/CTF**") laws and regulations, with the majority implementing recommendations set out by the Financial Action Task Force ("**FATF**"), an international inter-governmental organisation that aims to standardise AML/CTF systems around the world.

In Hong Kong, the principal AML/CTF legislation is the Anti Money Laundering and Counter Terrorist Financing Ordinance (Cap. 615) ("**AMLO**") which applies to financial institutions (including HKMA-authorised institutions, i.e. banks, SFC-licensed corporations, licensed insurance companies, stored value facility issuers and money service operators) and "designated non-financial business and professions" ("**DNFBP**") (professions such as being lawyers, public accountants, estate agents, and trust and company services agents), and also creates a licensing regime for money service operators, and trust and company services providers. Businesses that principally deal with cryptocurrencies such as exchanges and OTC desks are not directly subject to the provisions of AMLO, as such businesses do not fall within the definition of a financial institution or DNFBP unless the cryptocurrency business partially operates in a regulated business, for example, providing money services such as money changing and remittance services. Further to the rules set out in AMLO, each regulatory authority has formulated its own guidelines on dealing with AML/CTF issues.

As mentioned in the section on "Government attitude and definition" above, the regulatory authorities in Hong Kong have maintained a cautious approach to cryptocurrencies. In 2014, both the HKMA and the SFC issued circulars to their respective supervised institutions warning of the anonymous nature of cryptocurrency transactions and their inherent money-laundering and terrorist-financing risks. These statements came around the same time as the most noteworthy cryptocurrency money-laundering case stemming from the apprehension and conviction of Ross Ulbricht, the operator of the deep-web marketplace, "Silk Road". Both regulators have clearly indicated the requirement for increased vigilance when dealing with cryptocurrency business, including inquiring into the internal controls on AML/CTF policies and procedures of the cryptocurrency businesses. In light of these requirements, many cryptocurrency businesses voluntarily apply the customer due diligence measures set out in the Schedule 2 of AMLO as part of their AML/CFT policies.

While AMLO sets out specific guidelines applicable to financial institutions and DNFBPs, other businesses and individuals have a statutory duty to report any suspicious transactions under various criminal statutes, namely the Drug Tracking (Recovery of Proceeds) Ordinance (Cap. 405) ("**DTRPO**"), Organised and Serious Crimes Ordinance (Cap. 455) ("**OSCO**"), and the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) ("**UNATMO**"). Any suspected transactions involving money laundering, terrorist financing or receipts of crime must be reported to the JFIU by submitting a suspicious transaction report ("**STR**"); failure to file a STR is a criminal offence which is liable to a fine of HK$50,000 and a three-month imprisonment. As highlighted above, many cryptocurrency businesses implement AML/CTF measures to comply with the relevant suspicious

transaction reporting provisions under the DTRPO, OSCO and UNATMO, and also the likely requests from their banks in Hong Kong.

Promotion and testing

Various regulatory bodies in Hong Kong embrace the government's plan to promote fintech and financial innovation in the city. Currently the HKMA, SFC and the Insurance Authority are operating "sandbox" programmes that allow innovative financial products to be tested in a limited regulatory environment.

The first regulatory sandbox was introduced by the HKMA on 6 September 2016 (the "**HKMA Sandbox**"). The HKMA Sandbox provides HKMA-authorised institutions ("**AIs**"), e.g. banks, to allow for live testing of financial technologies before their formal launch. AIs must set applicable boundaries to conduct the trials on the client base and must offer appropriate customer-protection measures to resolve customer losses. On 28 November 2017, the HKMA introduced the Fintech Supervisory Sandbox 2.0 Chatroom that allows AIs to receive supervisory feedback through emails, video conferences and face-to-face meetings from the HKMA's Fintech Facilitation Office and Banking Department during the early stages when the new technological application is being contemplated by the AIs. As of July 2018, the HKMA reported that it had supervised four distributed technology projects; this means that banks in Hong Kong are actively looking at rolling out blockchain technologies as part of their services. One of the visible disadvantages of the HKMA sandbox is that it is only available to AIs or technology companies that are associated with an AI. Technology start-up companies who do not meet the above criteria are not permitted to access the HKMA sandbox.

The SFC sandbox was announced on 29 September 2017 (the "**SFC Sandbox**"). The objective of the SFC Sandbox is to allow firms to utilise innovative technologies and demonstrate a genuine commitment to carry out SFC-authorised activities through the use of financial technology that may increase the quality of products and services for investorsin Hong Kong. The SFC Sandbox will be opened to qualified firms who are "fit and proper" and hold applicable SFC licences and comply with the licensing requirements such as Financial Resources Rules. The SFC will impose licensing conditions on firms in the SFC Sandbox, which can be removed upon the firms' exit from the SFC Sandbox when the firm satisfies the requirements to operate outside of the SFC Sandbox. The guidelines from the SFC do not specify what technologies are permitted in the SFC Sandbox as they only require a genuine commitment to use financial technology in carrying out regulated activity, i.e. a cryptocurrency-based service that falls within the preview of regulated activity. Similar to the HKMA Sandbox, access to the SFC Sandbox is also limited to firms that hold SFC licences or people who qualify for SFC licences, which may also limit the access to the SFC sandbox for start-up companies.

Along with the 2018 SFC Statement, the SFC issued an appendix titled "Conceptual Framework for the Potential Regulation of Virtual Asset Trading Platform Operators" (the "**Conceptual Framework**"), setting out the potential regulations over "virtual asset trading platform operators" (commonly known as the "cryptocurrency exchanges") (the "**Platform Operators**"). The Conceptual Framework expanded the existing SFC Sandbox to cover the operation of cryptocurrency exchange (referred to as the Virtual Asset Trading Platform in the 2018 SFC Statement). If the SFC considers a Platform Operator is demonstrating commitment adhering to the high standards of the SFC, the Platform Operator may be placed in the SFC Sandbox where it will work closely with the SFC for the exploration of any

prospect in the SFC granting licences to it, subject to licensing conditions. If, at the end of the initial stage of the SFC Sandbox, the SFC concludes that it is appropriate to grant a licence to and to regulate the Platform Operators, the SFC has indicated that it will consider granting a licence to a qualified Platform Operator and impose certain licensing conditions as set out in the Conceptual Framework.

Some of the key proposed licensing conditions include (i) restricting services to "professional investors" only who have passed the suitability test, (ii) AML/CFT requirements on customers, (iii) limitations on trading of ICO tokens within the initial 12 months, (iv) prevention of market manipulative and abusive activities, (v) ongoing reporting obligations, (vi) insurance requirements, and (vii) segregation and custody of customers' money and virtual assets. In relation to "professional investors", they should have shown sufficient knowledge in virtual assets (including the relevant associated risks) before being offered the trading services of virtual assets. The required level of knowledge in virtual assets is still subject to clarification. Platform Operators may also be subject to licensing principles where they must establish and disclose their virtual assets admission criteria, set up a committee responsible for decision-making to admitting virtual assets and also adopt a fee structure to avoid any potential, perceived or actual conflict of interest when receiving payment for admitting virtual assets. Another condition worthy of further mention relates to the insurance requirements. The Platform Operators may be required to take out an insurance policy for risks associated with the custody of virtual assets, such as theft or hacking. The SFC indicates that the insurance policy would be expected to provide full coverage for virtual assets held by a Platform Operator in hot storage and a substantial coverage (for instance, 95%) for those held in cold storage. There are currently very limited insurance options on the market and, even if available, given the relatively short history and the significant value fluctuation of virtual assets, it is possible that the insurance products would require a higher premium and thus increase the operation costs of the Platform Operators.

As a result of the 2018 SFC Statement, Hong Kong has witnessed a surge of Platform Operators expanding their business to cover the Hong Kong market with the hope of participating in the SFC Sandbox and eventually be granted a licence to trade Security Tokens. As of the date of this publication, it is yet to be seen how the SFC will finalise its licensing regime for cryptocurrency exchanges, as the SFC Sandbox is currently being conducted in closed-door discussions with the SFC and there are already comments from the industry on how the proposed licensing direction would impose an uncommercial burden on the business.

Ownership and licensing requirements

Ownership of cryptocurrencies is currently not subject to any restrictions or regulations in Hong Kong, provided that they are obtained in good faith. Possession of cryptocurrencies may be illegal when their sources originate, amongst others, from computer crime, which under Hong Kong laws are proscribed in section 161 of the Crimes Ordinance (Cap. 200), and section 27A of the Telecommunications Ordinance (Cap. 171) and other applicable Hong Kong legislations including the DTRPO and the OSCO which establish offences for handling the proceeds of crime.

There are no requirements to date to obtain any licence to own or trade cryptocurrencies which are classified as "virtual commodities". On the other hand, this statement is subject to exceptions when dealing with securities and futures involving cryptocurrencies, such as

Bitcoin futures: a broker who wishes to offer such contract to their clients will require the appropriate SFC licences.

Mining

Mining is the process of creating new blocks on the blockchain; this process includes verifying transactions and collecting "block rewards" of cryptocurrencies. This type of activity is common to blockchain platforms that use the "proof-of-work" consensus algorithm, where the transaction is proved by the computing power used to process it. There are other consensus models such as "proof of stake", where the block producers stake their cryptocurrencies to gain the rights to process the transaction.

Assuming that "mining" is considered as mining of "proof of work"-based cryptocurrencies (such as Bitcoin) to date, there are no specific regulations governing mining of cryptocurrencies in Hong Kong. Moreover, to date no Hong Kong governmental body has issued any guidance that discourages, restricts or prohibits Bitcoin mining activities. Whether cryptocurrency mining is legally permitted in Hong Kong is subject to other regulations in Hong Kong under certain circumstances, will be discussed below.

Mining operations (especially for cryptocurrencies such as Bitcoin) can be highly industrialised operations, usually involving the use of hundreds of ASIC (application-specific integrated circuit) computers to mine cryptocurrencies. Such operations closely resemble large-scale data centre operations. Any regulations that apply to other similar applications such as data centres may also be applicable to cryptocurrency mining sites. In Hong Kong, data centre facilitation is overseen by the Office of the Government Chief Information Officer.

Businesses that intend to operate large-scale data centres should be aware of the relevant land-use rights stipulated under the laws of Hong Kong. Under the statutory Outline Zoning Plans ("**OZP**") prepared by the Town Planning Board under the Town Planning Ordinance ("**TPO**"), such data centres belong to "Information Technology and Telecommunications Industries" for cryptocurrency mining purposes and would therefore require application for amendment to the OZP under Section 12A of TPO. Apart from zoning permission, it should be noted that development of a site is subject to, *inter alia*: the terms and conditions of the land lease governing the site; the usage set out in the occupation permit; and the deed of mutual covenants, if any.

The operation of a data centre involves mechanical and electrical installations which may be subject to statutory requirements in Hong Kong. The key statute in question is the Buildings Energy Efficiency Ordinance (Cap. 610) and, in order to comply with the ordinance, the owner or operator of a data centre in a prescribed building should engage a Registered Energy Assessor to certify that its building services installations have complied with the requirements under the above ordinance. The above rules would only be applicable to large-scale cryptocurrency mining operations and would not likely apply to domestic or small-scale mining operations.

Border restrictions and declaration

Prior to recent legislative changes, there were no statutory declaration requirements on the import and export of large quantities of money in Hong Kong as advised by FATF Recommendation 32. As of 16 July 2018, with the commencement of the Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance (Cap. 629)

("**CMPCBNIO**"), a person who physically imports or exports large amounts of currency or bearer-negotiable instruments ("**CBNIs**") through the designated checkpoints stated in the CMPCBNIO must now disclose and declare such movement to CED. The disclosure threshold is set at HK$120,000 (Schedule 4 of the CMPCBNIO).

The new CMPCBNIO is only applicable to CBNIs, which are defined as cash or negotiable instruments such as bearer cheques, promissory notes, bearer bonds, traveller's cheques, money orders or postal orders. As Bitcoin has so far been classified by the HKMA as a "virtual commodity", it should not fall within the definition of CBNI, but it is unclear how this would apply to other Altcoins. There would also be considerable difficulties in enforcing this provision, as CMPCBNIO requires the physical movement of CBNIs; thus to enforce the declaration requirements, the CED would have to prove that Bitcoins were physically moved across the border.

Reporting requirements

In Hong Kong, there is no requirement to report cryptocurrency transactions of any amount. Profits generated through cryptocurrency trading may be subject to declaration in a tax return under the applicable tax legislation, as discussed above. As cryptocurrencies are not defined as CBNIs, there is no obligation to declare them to CED when importing them to Hong Kong.

Estate planning and testamentary succession

In essence, any cryptocurrencies or cryptocurrency accounts would be treated as personal property and would fall into the estate of the deceased, which can be administered by the Executor named in the will of the deceased or an Administrator appointed by the Probate Court. The Executor or the Administrator could apply for a "Grant of Probate" or a "Letter of Administration" before he is allowed to handle the cryptocurrencies or exchange accounts.

Ordinary access to cryptocurrencies requires the user to have access to the private key to make transactions on the blockchain, and if the private key is lost then the cryptocurrencies are irrecoverable. Thus when conducting estate planning, arrangements should be made to preserve the private key beyond the death of its owner, such as recording the recovery seed and storing in a safe environment (i.e. a bank safe deposit box). Cryptocurrency exchange accounts may be accessed by the Executor or the Administrator in accordance with the procedures of each exchange; like with many internet-based services, this may require the Executor or the Administrator to submit the certificate of death, the Grant of Probate and/or the Letter of Administration to the exchange.

Yu Pui Hang (Henry Yu)
Tel: +852 2115 9525 / Email: hyu@lylawoffice.com

Mr. Yu is the founding partner of L&Y Law Office and Henry Yu & Associates. He obtained his bachelor of law degree in England and is qualified as a solicitor in both England & Wales and Hong Kong.

Over recent years, Mr. Yu has developed a strong interest in the blockchain industry and his enthusiasm and insightful views have been affirmed widely by various professional bodies. Mr. Yu is a member of the Innotech Committee (a.k.a. the Technology Committee) of the Law Society of Hong Kong, and he has also been appointed as: Hon. Legal Advisor to the Hong Kong Federation of Innovation and Invention; Hon. Legal Advisor to the Institute of Financial Technologists of Asia; and Hon. Legal Advisor to the GHM-Greater Bay Area TECHFIN Association. From time to time, Mr Yu represents the Bitcoin community at meetings with the Legislative Council Members, the HKMA and the FTSB.

L&Y Law Office / Henry Yu & Associates

Suite 806 / Suite 806A, 8/F, Tower Two, Lippo Center, 89 Queensway, Admiralty, Hong Kong
Tel: +852 2115 9525 / URL: www.lylawoffice.com

India

Anu Tiwari & Rachana Rautray
AZB & Partners

Introduction

In India, over the past few years, the use of technology, including blockchain, to fuel financial transactions has boomed significantly. Such development has not gone unnoticed by most regulators such as the Reserve Bank of India ("**RBI**") (Indian Central Bank) which has reacted, for the most part, favourably. Whilst the present government has supported innovation to promote a digital or cashless economy, cryptocurrency still remains an outlier.

The RBI took notice of the use of cryptocurrency in open markets around 2013 and has since responded by cautioning users, holders and traders of the use of "virtual currency" while remaining silent on the legality of its use, including in 2017. Similarly, other regulators, such as the Enforcement Directorate and Income Tax Department, have been swift in their actions to shut down businesses associated with cryptocurrency by conducting raids under the guise that the use of cryptocurrency was in violation of foreign exchange and anti-money laundering regulations.

In light of the above, most entities dealing in cryptocurrency took a backseat in their operations from 2017 onwards, especially after the RBI prohibited cryptocurrency for regulated entities, when global and as well local markets seemed to be moving towards an economy being driven by technology. In fact, while the Indian government remained silent on the definition of "cryptocurrency", it continued to support "pre-paid" instruments or tokens issued by private players in exchange of products or services being offered on their platform. In fact, regulators have since supported the use of "blockchain", demonstrated by RBI's Blockchain whitepapers in 2017 and 2019 deliberating upon the use of blockchain while merely commenting on one such use of cryptocurrency as a medium of exchange to secure transactions.

Pursuant to the previous finance minister's budget speech in 2018, the government had constituted an inter-disciplinary committee which included representatives from the RBI, to examine: (i) the status of cryptocurrency in India and globally; (ii) the existing global regulatory and legal structures governing cryptocurrency; and (iii) measures to address issues relating to consumer protection and money laundering.

Despite the contents of the above report remaining confidential, per publicly reported news sources, the government is moving towards a wholesale ban on the use of cryptocurrency.

Historic stance taken by the government

After the RBI circular dated April 6, 2018 ("**Circular**"), the dealing of cryptocurrency in India today has been substantially blocked. Through the Circular, the regulator banned all

RBI regulated entities (i.e., banks, financing institutions, non-banking financing institutions) from dealing in cryptocurrency. These entities were provided a three-month period within which all accounts dealing with cryptocurrency had to be shut down. Consequently, while the RBI *per se* did not ban cryptocurrency, it chocked any financial dealing contemplated by a buyer, seller or trader in cryptocurrency.

Other regulators, such as the Securities Exchange Control Board of India ("**SEBI**") have continued to remain silent on its stance on cryptocurrency.

Judicial approach to cryptocurrency

Several stakeholders have approached the judiciary by filing petitions before the Indian Supreme Court ("**SC**") in order to compel the government to provide clarity.

The two primary petitions seeking to address the legality of cryptocurrency were filed by (i) Vijay Pal Dalmia and Siddharth Dalmia through civil writ petition 1071 of 2017 on June 2, 2017 ("**Dalmia Petition**"), and (ii) Dwaipayan Bhowmick through civil writ petition 1076 of 2017 on November 03, 2017 ("**Bhowmick Petition**").

The Dalmia Petition was filed against the Union of India (through the cabinet secretary), Ministry of Home Affairs, Ministry of Finance and the RBI ("**Respondents 1**"), seeking an order to direct Respondents 1 to "restrain/ban the sale/purchase of or investment in, illegal cryptocurrencies and initiate investigation and prosecution against all parties which indulged in the sale/purchase of cryptocurrency".

The grounds for the stated petition, as available on public sources, was based on: (i) the anonymous nature of cryptocurrency transactions which makes them well-suited for funding terrorism, corruption, money laundering, tax evasion, etc.; (ii) production and introduction of new cryptocurrency has been generated by private parties, without the intervention of the government, and hence violating the Constitution; (iii) the use of cryptocurrency has been in contravention of several laws such as FEMA and the Prevention of Money Laundering Act, 2002; (iv) ransomware attacks have occurred through the use of Bitcoin; (v) illegal cryptocurrency provides an outlet for personal wealth that is beyond restriction and confiscation; (vi) cryptocurrency exchanges have encouraged "benami" transactions and made it difficult for government authorities to identify such transactions; and (vii) trading of illegal cryptocurrency bypasses prescribed KYC Norms.

Pursuant to the above petition, the Bhowmick Petition was filed against the Union of India through the Ministry of Finance, Ministry of Law and Justice, Ministry of Electronic and Information Technology, SEBI, RBI, Income Tax Dept. (through its secretary) and the Enforcement Directorate (through its joint director) ("**Respondents 2**") seeking an "issuance of direction to regulate the flow of bitcoins as well as requiring the constitution of a committee of experts to consider prohibition/regulation of bitcoins and other cryptocurrencies".

The grounds for the petition, as available from public sources, *inter alia* include: (i) Bitcoin trading/transactions, being unregulated, lack accountability; (ii) investigators can only track Bitcoin holders who convert their bitcoins to regular currency; (iii) counterfeiting of cryptocurrency is not an issue so long as the miners keep the blockchain secure; (iv) bitcoins may be used for trade and other financial activities without accountability, having an effect on the market value of other commodities; (v) conversion of Bitcoin into foreign exchange does not fall under the purview of the RBI, making such transactions highly unsafe and

vulnerable to cyber attacks; (vi) presently, no regulator has the power to track, monitor and regulate cryptocurrency transfers; (vii) cryptocurrency has the potential to support criminal, anti-social activities, like money laundering, terrorist funding and tax evasion; and (viii) use of cryptocurrency could result in financial implications if left unchecked.

Subsequent to the aforementioned petitions, industry participants such as Kali Digital had filed writ petitions challenging the constitutionality of the Circular and reiterated the need for clarity on regulation. Other stakeholders, such as the Internet and Mobile Association of India had also filed intervention applications in the Bhowmick Petition in order to draw attention to the impact any regulation on cryptocurrency may have to their businesses. It had also challenged the RBI Circular as being unconstitutional and highlighted to the Supreme Court on the hindrance to their businesses in light of the Circular.

While the above matters remain *sub judice*, the Supreme Court in February, 2019 provided the Indian Government, a period of four weeks, to frame a policy on cryptocurrency, which is still awaited.

There have been recent reports that the Government is looking to introduce a new legislation on cryptocurrency and looking at introducing a jail term for "holding, selling or dealing in cryptocurrency", making it a "non-bailable" offence. This, if affected, will further impact the future of the cryptocurrency business in India.

Set out below are possible reasons for such a ban and the way forward for the cryptocurrency business in India.

Possible reasons for the ban

RBI's primary reason is to protect its investors, since cryptocurrency lacks any intrinsic value and affords anonymity to its holder. Per news reports, the RBI is determined to "ring-fence gullible investors and lenders from scams, several of which have happened internationally". Given the nature of trades, an imposition of know-your-customer regulations does not *per se* assist in reducing the threat of fraudulent transactions since it may be difficult to identify the original holder of cryptocurrency.

In fact, an anonymous holder possesses other problems, such as inadequate recourse available in case of illegal activity, since an accused must be an "identifiable party" for the judiciary to call upon and hold accountable for such illegal activity. Therefore, while any currency including fiat currency could facilitate illegal transactions and tax evasion, cryptocurrency could go a step further and protect a party engaging in such activities, rendering common holders vulnerable.

A commonly cited reason for distrust by governments/regulators that is associated with investor protection is the lack of control exerted by central authorities over cryptocurrency. While rendering the banking system redundant may not immediately seem problematic, regulators worry that an investor would have no recourse in the event a payment is hacked or there is a failure of transfer of funds due to a technical glitch. Further, the lack of a banking system would also be alarming for most investors given that the system supports immediate provision of funds as well as income through interest over funds already earned by the investor.

Cryptocurrency distinct from prepaid instruments ("PPIs")

In fact, the anonymous nature and lack of intrinsic value of cryptocurrency are the primary distinguishing factors from "prepaid instruments", the latter being completely legal and

regulated today. Prepaid instruments and payment systems are regulated by the Payments and Settlement Act, 2007 ("**PSSA**") and RBI Master Directions on Issuance and Operation of Prepaid Payment Instruments dated October 11, 2017 ("**Master Directions**"). The intent of the PSSA is to regulate prepaid instruments, i.e., payment systems that affect electronic transfers. The Master Directions define prepaid instruments as "payment instruments that facilitate purchase of goods and services, including financial services, remittance facilities, etc., against the value stored on such instruments". In fact, the regulations further specify that these instruments may be loaded/reloaded with cash, by debit to a bank account, by credit and debit cards, and other PPIs (as permitted from time to time). The electronic loading/reloading of PPIs shall be through payment instruments issued only by regulated entities in India and shall be in INR only. Based on the above, the instrument is merely acting as a mode to transfer regulated currency, similar to a bank transfer.

Therefore, unlike cryptocurrency, whose value (if any) may be contingent upon its demand/supply, pre-paid instruments do have an intrinsic value associated with them as well as their holder being clearly identifiable.

Alternative route: cryptocurrency as a deposit or security?

Given that cryptocurrency is often associated with speculation, one could explore whether the acceptance of certain cryptocurrencies such as tokens could constitute a deposit or a security. The (Indian) Securities Exchange Board, unlike the RBI, continues to remain silent on the subject, possibly since, in India, a security has been defined to include "shares, scrips, stocks, bonds, debentures, debenture stock, or other marketable securities of a like nature in an incorporated company or body corporate". While, cryptocurrency may be arguably marketable, it is not in the nature of shares, scrips, stocks, debentures, etc. issued in relation to a body corporate. However, should the regulator see scope in regulating cryptocurrency and initial coin offerings akin to securities and initial public offerings, similar to other overseas jurisdictions, the definition of a "security" may see revision.

Similarly, debt/deposits in India are associated with the repayment of money. It is arguable that the issuance of cryptocurrency could create a debt on the part of the issuer to the extent that the consideration for the issuance is treated as a debt until cryptocurrency is transferred to the purchaser.

While the aforementioned regulations seem possible, the anonymity of the parties involved in the transaction may continue to pose a hurdle to the regulation of cryptocurrency even as a deposit or security.

Conclusion

While industry participants await the government's decision on cryptocurrency and details regarding the contours of a possible ban, most stakeholders argue that, like every "banned activity", the activity does not come to a halt but instead moves to jurisdictions permitting such activity, as the Indian experience also suggests post-2017 after the RBI Circular. On the same basis, stakeholders are still trying to sensitise the Government about the potential of disruptive technologies such as cryptocurrencies, capitalise on the burgeoning revenue potential and work with the industry.

It has previously been reported that the RBI itself looked to launch a digital currency using blockchain technology and, despite its discomfort with cryptocurrency, has promoted the use of blockchain. In light of this, even if the Government were to introduce a wholesale

ban on cryptocurrency in India, it is likely to be a regressive step, in turn also affecting the growth and development of the nascent blockchain industry in India, which has shown immense potential. The devil being in the details, it will be useful to wait until the contours of the proposed Indian cryptocurrency law are finalised.

Anu Tiwari
Tel: +91 22 6639 6880 / Email: anu.tiwari@azbpartners.com

Anu Tiwari holds a Bachelor of Law degree from the National University of Juridical Sciences and is a partner at AZB & Partners with extensive experience in M&A, JVs, financial regulatory, asset management, IT/ITES, including emerging technology, i.e. blockchain, payment systems, cryptocurrency and general corporate advisory. Anu regularly advises banks, non-banks (NBFCs), asset managers/securities market intermediaries, global information technology (IT) and payments/FinTech players on regulatory and M&A (both domestic and cross-border) aspects. His practice includes advising on cyber-security, financial crimes and regulatory investigations. He has actively participated in various policy initiatives, including as a Member of the Confederation of Indian Industries (CII) – FinTech Working Group, and as a Member of the Legal Advisory Sub-Committee, Reserve Bank India (RBI) Committee on Household Finance.

His accolades include the following:

- Recognised by *IFLR 1000* in Mergers and Acquisitions (2018 and 2019).
- Ranked by *Mergermarket* in the top 5 (by volume) and top 10 (by value) lawyers in India, in the corporate and financial services league tables, respectively (2018).

Rachana Rautray
Tel: +91 22 6639 6880 / Email: rachana.rautray@azbpartners.com

Rachana Rautray, holds a Bachelor of Law degree from National University of Juridical Sciences, Kolkata, and is an associate with AZB & Partners with extensive experience in various practice areas including mergers & acquisitions, and general corporate and commercial law. Rachana regularly advises banks, non-banks (NBFCs), securities market intermediaries, global information technology (IT) and payments/FinTech players on regulatory and M&A (both domestic and cross-border) aspects. Her practice includes advising on data protection/cyber-security, financial crimes and regulatory investigations involving the RBI, SEBI and Government of India.

AZB & Partners

AZB House, Peninsula Corporate Park, Ganapatrao Kadam Marg, Lower Parel, Lower Parel West, Mumbai, Maharashtra 400013, India
Tel: +91 22 6639 6880 / Fax: +91 22 6639 6880 / URL: www.azbpartners.com

Ireland

Maura McLaughlin, Pearse Ryan & Caroline Devlin
Arthur Cox

Government attitude and definition

While the Irish Government has, to date, remained largely silent on its attitude towards cryptocurrencies, the Irish Department of Finance issued a Discussion Paper on Virtual Currencies and Blockchain Technology in March 2018. The Paper discusses various aspects of both, such as risks and benefits of currencies, but also gives examples and details of countries which are either proponents or opponents of cryptocurrencies and/or blockchain technology.

While the Discussion Paper does not outline or represent the attitude of the Irish Government on this topic, it states that no one policy measure or State agency has the ability to comprehensively address all the risks and opportunities in the area. Instead, it states that to evaluate each of these issues, the Irish Government will require the expertise of multiple State agencies such as the Department of Finance, the Revenue Commissioner, the Data Protection Commission and the Department of Business, Enterprise and Innovation to allow for the development of holistic policy measures that encourage innovation while addressing risks to consumers, investors and businesses.

In order to facilitate this process, the Department of Finance established an inter-departmental working group on blockchain and cryptocurrencies in March 2018 to, amongst other things, monitor international developments in the area, engage with other areas of Government, assess possible involvement, and consider if policy recommendations will be necessary.

In Ireland, cryptocurrencies are not regarded as either "money" or "currency". The Central Bank of Ireland (CBI) has issued a warning on its website that cryptocurrencies are not legal tender and are neither guaranteed nor regulated by the CBI. The dangers associated with such currencies, as mentioned by the CBI in its warning, include their extreme volatility, the absence of regulatory protection, and the risk of being given misleading or incomplete information.

The CBI also issued an "Alert on Initial Coin Offerings" in December 2017. The purpose of the alert is to warn against, amongst other things, the high risk of losing all invested capital due to the lack of regulation and the associated risk of becoming the victim of fraud or other illicit activities. Extreme price volatility was also mentioned as one of the risks.

There are currently no cryptocurrencies which are backed by either the Irish Government or the CBI. While other jurisdictions around the world are investigating the use of digital currencies, no such plans have been announced to date by either the Irish Government or the CBI.

Cryptocurrency regulation

There is no specific cryptocurrency regulation in Ireland, but there is also no specific prohibition in Ireland on any activities related to cryptocurrency.

The CBI is the competent authority in Ireland for the regulation of financial services including electronic money, payment services and securities law. The CBI has yet to indicate the extent to which existing financial regulation will apply. The CBI has issued warnings in relation to ICOs and cryptocurrencies and has also contributed to the European Securities and Markets Authority (ESMA)'s warnings to both consumers and to firms engaged in ICOs (see also "Government attitude and definition").

In respect of cryptocurrency regulation, we expect that the CBI will focus on securities law and the recognised EU concepts of "transferable security" and "financial instruments" as defined in the 2014 European Union Markets in Financial Instruments Directive (MiFID II) and the characteristics which they view as bringing cryptocurrencies or tokens within those definitions. Depending on their structure, cryptocurrencies could be classified as transferable securities, which would bring them within scope of a range of securities laws. For example, the issuer of a cryptocurrency may be required to publish a prospectus (or avail of an exemption) prior to their being offered to the public, or certain activities in respect of the cryptocurrency may require authorisation as an investment firm under MiFID II.

A pure, decentralised cryptocurrency is unlikely to be a transferable security, while a token with characteristics similar to a traditional share or bond may be. It is also possible that true "utility" tokens intended for exclusive use on a platform or service will not be transferable securities. The definition of transferable security is non-exhaustive and it is for each issuer and their advisers to determine whether their cryptocurrency or token is a transferable security.

In January 2019, ESMA published advice to the European institutions on ICOs and crypto-assets recognising the gaps and issues with existing EU rules and calling for a harmonised EU-wide approach in this area.

As in many jurisdictions, the regulatory environment in relation to cryptocurrencies and their interaction with securities law is not yet settled and ESMA acknowledges that, depending on how an ICO is structured, it may fall outside the regulated space entirely.

Sales regulation

Depending on the structure of an ICO or token, it may fall within the regulated space and require the publication of a prospectus (or availing of an exemption from that requirement, see above) prior to it being offered to the public.

Taxation

There are no specific rules for dealings in cryptocurrencies, and normal basic principles apply. The Irish Revenue confirmed this in a publication issued in May 2018. The taxation of dealings in cryptocurrencies will generally follow the underlying activities. Thus the receipt of cryptocurrency by a trader in lieu of cash for goods or services rendered will generally be taxed as income. Dealing in cryptocurrencies of themselves will depend on the nature and level of activity of the dealer. Occasional investment in and disposals of cryptocurrencies would likely be treated as a capital receipt, currently taxed at 33%. Where there is significant and regular dealing, this could be considered to be trading, which for a company would be taxed at 12.5%, or the marginal higher rates for individuals. The actual

tax position will depend on an analysis of the specifics of each transaction, and would need a case-by-case consideration, as is normal in trading activity. Cryptocurrencies are not a functional currency, and therefore accounts should not be prepared in cryptocurrencies for tax purposes. If it is assumed that the profit may be taxable under some heading, the next issue is valuing the profit generated. This is naturally a challenge, and indeed records of trades through various exchanges may be difficult, if not impossible to obtain. It is likely that this area will be the subject of further guidance from the Irish Revenue in due course, but in the interim, those dealings in cryptocurrencies should keep all relevant contemporaneous records to assist in the valuation.

No Irish VAT arises on the transfer of cryptocurrency, although if cryptocurrency is tendered in exchange for a good or service, the provision of the good or service would attract VAT in the normal way. Irish stamp duty should not arise, although as stamp duty is a tax on documents, the manner in which the transfer takes place would be worth monitoring to ensure that a stampable document has not been inadvertently created.

The territoriality aspect of cryptocurrencies is still an evolving area. In the case of an Irish resident (and for an individual ordinarily resident) person, they will usually be liable to tax in Ireland on their worldwide income and gains (subject to any reliefs or exemptions, including double tax treaty reliefs). A non-resident person will generally only be subject to tax on Irish-sourced income or gains, or profits of an Irish trade. (In the case of individuals, tax may also apply where amounts are remitted into Ireland.) It is evident therefore that understanding the source or *situs* of cryptocurrencies is of significance in international dealings. This is likely to be an area that will be developed further.

Money transmission laws and anti-money laundering requirements

There is a risk that certain ancillary services in connection with cryptocurrency could be subject to regulation as a form of money remittance or transmission under the Payment Services Directive (PSD) or, where PSD does not apply, under the Irish regulatory regime for money transmission. For example, the operator of a cryptocurrency platform who settles payments of fiat currency between the buyers and sellers of cryptocurrency could be viewed as being engaged in the regulated activity of money remittance/transmission. There are a number of exemptions which may be applicable; for example, where the platform operator is acting as a commercial agent or where the platform could be viewed as a securities settlement system. The application of the exemption would depend on the features of the trading platform.

The application of existing Irish anti-money laundering requirements to cryptocurrencies is unclear due to uncertainty surrounding the regulatory status of cryptocurrency. Where the cryptocurrency or any activity relating to it is subject to regulation (e.g. it has the characteristics of transferable security), then Irish anti-money laundering requirements will apply.

The 5th Anti-Money Laundering Directive (AMLD5) will impose new anti-money laundering requirements on cryptocurrency exchanges and custodians operating in Europe. AMLD5 has not yet been implemented in Ireland.

Promotion and testing

Ireland does not operate a regulatory sandbox, of which cryptocurrency or token issuers could avail themselves. The Irish Department of Finance is establishing an intra-departmental working group with a view to engaging with industry and overseeing

developments in virtual currencies and blockchain technology. The Industrial Development Authority, the government agency tasked with attracting inward investment, has led efforts by the Irish Blockchain Expert Group to establish Blockchain Ireland, to help promote and share information on blockchain in Ireland. Further, the CBI established an innovation hub in 2018 to allow companies to engage directly with the CBI in the areas of Fintech and innovation, including a dedicated page on its website and direct interactions with firms outside of the CBI's traditional formal processes.

Ownership and licensing requirements

In principle, there are no specific ownership and licensing requirements set out with regard to cryptocurrency. More specifically, while heavily regulated retail funds (e.g. UCITS funds) have specific restrictions on the type and diversity of assets they can hold, which restrictions would likely exclude cryptocurrencies, there are no generally applicable restrictions on investment managers owning cryptocurrencies for investment purposes. In addition, no specific licensing requirements are imposed on anyone who holds cryptocurrency as an investment advisor or fund manager.

However, in stating the above, it should be noted that the CBI has not, to date, confirmed its position on the status of cryptocurrencies as a security, a token or otherwise and, as such, until such time as that position is clear, the precise treatment of cryptocurrencies, and any rules that might apply to advising on the issuance of or dealing in the same, will ultimately depend on the CBI's determination of that analysis.

Particular areas that regulation might touch on include:

(a) Is the cryptocurrency itself a security, subject to securities regulations of all forms, or is it something else, a token, another form of right, etc.?

(b) The status of the issuer of a cryptocurrency – i.e. is it an issuer of a security, is it a collective investment scheme, or are the cryptocurrency and the issuer outside of these types of categories?

(c) Is a cryptocurrency an eligible asset for holding by certain regulated entities including UCITS, Insurance Company, Banks, etc.?

In relation to the last category above, this question is likely only to be answered by wider EU regulation, which is likely to follow only after an exhaustive analysis of the first two questions. As things stand, cryptocurrencies do not fall within the categories of eligible assets for the above.

In relation to the issuer status, the CBI has not yet provided any guidance as to their thoughts on whether certain coin offerings creating a cryptocurrency may effectively be structured to come within AIF or Investment Company definitions, i.e. be defined as a "Fund".

Applying Fund definitions to what is traditionally seen in ICOs, it would seem to be a difficult argument to make to suggest that the purpose of the undertaking was collective investment, and the entities do not usually seek to pool investors' funds to provide a pooled return, rather they are often a commercial undertaking. In addition, although it might be said that capital was being raised from a number of investors, it is not usually being invested in accordance with a defined investment policy, nor is that capital being invested for the benefit of those investors.

While tokens may ultimately be sold in a secondary market for profit, the schemes themselves do not seek to provide a pooled return as such and in addition, it does not appear that any eventual price for the token would be based on the value of the assets into which

investors' capital was invested and, furthermore, there is a case to say that the underlying assets are those of a normal commercial business developing its own products and services, rather than assets being bought, held and sold primarily to provide a pooled return.

Therefore, while this has not been the subject of a regulatory or other decision to date, traditional forms of initial coin offerings would not appear to be Funds (AIFs under the EU rules regarding the same).

Finally, the analysis of cryptocurrencies as a security may well be undertaken on a case-by-case basis, with the specific characteristics of individual currencies being key to a determination of whether they are a security issued by a company, and as such subject to the relevant securities laws, or if they are something else.

Mining

There are no restrictions in Ireland on the mining of cryptocurrency. As noted above in the "Cryptocurrency regulation" section, the regulatory status of cryptocurrency in Ireland is uncertain. It is likely that the focus going forward will be on securities law.

Mining of cryptocurrency is a technical process relating to the release of new cryptocurrency and the tracking of cryptocurrency transactions on a blockchain. Where the cryptocurrency is a form of transferable security, the mining activity could be viewed as a form of securities settlement system. However, as the mining is carried out on a decentralised basis, it does not fit neatly into any existing regime for securities settlement. On that basis, we would view mining as an unregulated activity under Irish law.

Border restrictions and declaration

In Ireland, there are no border restrictions or obligations which are specifically aimed at cryptocurrencies. The traditional reporting requirements for "cash" (which is defined as currency, cheques and money orders or promissory notes) when entering or leaving the European Union do not apply to virtual or cryptocurrencies. This is because they are deemed to be neither "cash" nor "currency".

Reporting requirements

In respect of financial regulation, there are currently no specific reporting requirements relating to cryptocurrencies. (See "Money transmission laws and anti-money laundering requirements".) Where the cryptocurrency or any activity related to it is subject to regulation, then Irish anti-money laundering requirements will apply. This will include obligations to submit suspicious transaction reports to the Garda Síochana and the Revenue Commissioners.

Estate planning and testamentary succession

As a general rule, a person can devolve their assets by a will in any jurisdiction, although it is common to have a complementary will or similar document in jurisdictions in which significant assets are located. As mentioned above, the *situs* of cryptocurrencies remains an area of discussion, so this will be a matter that will evolve in time.

From an inheritance tax perspective, Irish inheritance tax can arise if any of the following are relevant:

- Irish disponer;
- Irish beneficiary; or
- Irish property.

In the case of individuals with a presence but perhaps not fully within the tax net in Ireland, the *situs* of cryptocurrencies will be an important consideration.

* * *

Acknowledgments

The authors acknowledge with thanks the contribution to this chapter by:

Ian Dillon, Partner

Tel: +353 1 920 1788 / Email: ian.dillon@arthurcox.com

Ian is a partner in the firm's Asset Management & Investment Funds Group with experience in all aspects of Irish fund law and regulation. Ian's particular focus is on alternative investments including all aspects of AIFMD as well as hedge, real asset, credit, private equity and liquid fund formation. In addition, Ian has advised on the funding of initial coin offerings and issuers including in relation to their regulatory status.

Declan McBride, Of Counsel

Tel: +353 1 920 1065 / Email: declan.mcbride@arthurcox.com

Declan is a senior member of the Financial Regulation Group. He advises a wide range of domestic and international financial institutions. Declan's experience includes providing advice on authorisation requirements, anti-money laundering, payment services, Central Bank of Ireland investigations and compliance with conduct of business rules.

Maura McLaughlin, Partner
Tel: +353 1 920 1182 / Email: maura.mclaughlin@arthurcox.com

Maura advises international and domestic listed public and private companies, as well as public sector bodies, on all aspects of company law and a wide range of commercial matters, as well as advising listed companies on compliance and governance issues. She has extensive experience of advising on public and private mergers and acquisitions, with particular emphasis on takeovers, schemes of arrangement and mergers. Maura has employed this experience to achieve clients' strategic objectives, notably in the design and implementation of structures permitting the inversion or migration of holding companies to Ireland. Equity capital markets work is another area of focus: Maura regularly advises on Irish securities laws, and has acted for companies, investors and underwrites on listings and fundraisings. Prior to joining the firm, Maura worked for Linklaters' London office.

Pearse Ryan, Consultant
Tel: +353 1 920 1180 / Email: pearse.ryan@arthurcox.com

Pearse is a consultant in the Technology & Innovation Group and member of the firm's cross-departmental FinTech Group and Cyber Security Group. Pearse specialises in the areas of digital transformation/cloud computing, commercialisation of technology innovation/technology-related IPR, computer security/fraud, cyber insurance, e-commerce and Fintech. Pearse is a member of the Irish Blockchain Expert Group, as well as the new Lex Mundi Blockchain Group. Pearse is a frequent writer and speaker on Fintech and cyber security topics. This includes recurring speaking slots with the Incorporated Law Society of Ireland (PPCII and Diploma courses) and The Honorable Society of King's Inns (Advanced Diploma in White Collar Crime). Pearse was a part-time lecturer 2017/2018 on the National College of Ireland new MSc in Fintech.

Caroline Devlin, Partner
Tel: +353 1 920 1224 / Email: caroline.devlin@arthurcox.com

Caroline is a partner in the firm's Tax Group, and is an experienced partner in taxation in particular in financial services issues. She is a member of the Law Society Taxation Committee, and represents the Law Society in many of its dealings with the Irish Revenue Commissioners. She is editor and co-author of the Institute of Tax publication, *The Law and Practice of Stamp Duty*. Caroline advises domestic and international clients on tax planning, including in particular financial services, also involving cryptocurrencies and ICOs, along with other raising capital products for companies and financial institutions. She is very experienced in advising clients in the most efficient manner on establishing in Ireland.

Arthur Cox

Ten Earlsfort Terrace, Dublin 2, D02 T380, Ireland
Tel: +353 1 920 1000 / Fax: +353 1 920 1020 / URL: www.arthurcox.com

Japan

Taro Awataguchi & Takeshi Nagase
Anderson Mōri & Tomotsune

Government attitude and definition

General overview

With the steep rise of the price of Bitcoin and the increasing enthusiasm for initial coin offerings ("**ICO**"), the Japanese cryptocurrency market has seen explosive growth in 2018.

In actual fact, Japan was the first country in the world to have enacted a law defining Virtual Currency as a legal term, and requires an entity to register as a Virtual Currency Exchange Service Provider ("**Exchange Provider**") in order to provide Virtual Currency Exchange Services ("**Exchange Services**") to residents in Japan. The definition of these terms will be discussed in detail in the below section entitled "**Cryptocurrency regulation**".

The purpose of the above legislation is to: (i) protect customers of cryptocurrency exchanges; and (ii) combat money laundering and the financing of terrorism ("**AML/CFT**").

The need for the above legislation can be traced to recent developments in the Japanese market. One such development is the civil rehabilitation, in February 2014, of MTGOX Co, Ltd ("**MTGOX**"), a Japanese company that provided convertible Exchange Services between cryptocurrencies and fiat currencies, which was the world's largest cryptocurrency exchange at that time. This case highlighted the urgent need for regulatory protection of cryptocurrency exchange customers.

In addition, following the Leaders' Declaration at the G7 Elmau Summit, the Financial Action Task Force published the "Guidance for a Risk-based Approach to Virtual Currencies" in June 2015, which recommended that virtual currency exchanges be registered and/or licensed, and that they comply with regulations on money laundering and terrorist financing, including customer identification obligations.

Given these circumstances, a bill to amend the Payment Services Act ("**PSA**") and the Act on Prevention of Transfer of Criminal Proceeds ("**APTCP**") was submitted to the Japanese Diet on March 4, 2016, and was passed on May 25, 2016. The amended laws came into force on April 1, 2017.

Recent developments

In January 2018, Coincheck, Inc., one of the largest cryptocurrency exchanges in Japan, announced that it had lost approximately US$530 million worth of cryptocurrencies through a hacking attack on its systems. In addition, it has also become apparent that cryptocurrencies are being increasingly used for speculative reasons, rather than as a means of settlement.

In light of these developments, in March 2018 the Financial Services Agency of Japan ("**FSA**") established a "Study Group on Virtual Currency Exchange Business, etc." ("**Study Group**"), to assess the adequacy of regulatory measures in addressing issues relating to

Exchange Services. This was followed by the publication of the Study Group's report ("**Report**") on December 21, 2018. Besides summarising the results of the Study Group's deliberations, the Report also proposes a new legal framework to govern Virtual Currencies, which has led to the introduction of a bill for the revision of certain legislation governing Virtual Currencies ("**Bill**"). Tabled before the Diet on March 15, 2019, the Bill contains proposed revisions to the PSA ("**PSA Revisions**"), based mainly on the proposals contained in the Report. At the same time, the Bill proposes revisions to the Financial Instruments and Exchange Acts ("**FIEA Revisions**"), primarily for the purposes of strengthening the regulatory framework surrounding Virtual Currencies.

The following is a summary of the key revisions proposed under the Bill.

- **PSA Revisions**
  - (a) Revision of the term "Virtual Currency" to "Crypto Asset".
  - (b) Enhancement of regulation of crypto asset custody services.
  - (c) Tightening of regulations governing Exchange Services.
- **FIEA Revisions**
  - (a) Establishment of ERTRs and regulations applicable thereto.
  - (b) Introduction of regulations governing crypto asset derivative transactions.
  - (c) Introduction of regulations governing unfair acts in crypto asset or crypto asset derivative transactions.

The Bill was passed by both chambers of the Diet on May 31, 2019, and the Bill will come into force within a year of its introduction. The Bill will significantly reshape the regulatory landscape surrounding Virtual Currencies in Japan.

Central Bank's attitude toward cryptocurrencies

Under Japanese law, cryptocurrency is neither treated as "money" nor equated with fiat currency. There is no cryptocurrency that is supported by the Japanese government or the central bank of Japan (the Bank of Japan, "**BOJ**"). According to the working paper "Information Technology Innovation/Data Revolution and Central Bank Digital Currency" published by the BOJ on February 2019, the BOJ does not have any plans to issue its own digital currency at this juncture. However, the working paper indicates that the BOJ considers that digital information technology may expand the utility of money in future.

Cryptocurrency regulation

Under Japanese law, "Virtual Currency" is not listed as a type of "Securities" as defined in the Financial Instruments and Exchange Act (please note, however, that a certain type of token may be subject to the regulation of the Act, as discussed later in the below section entitled "**Sales regulation**"). The PSA defines "Virtual Currency", and requires a person who provides Exchange Services to be registered with the FSA. A person conducting Exchange Services without registration will be subject to criminal proceedings and punishment.

Therefore, the respective definitions of Virtual Currency and Exchange Services are of crucial importance.

Definition of Virtual Currency

The term "Virtual Currency" is defined in the PSA as:

(i) proprietary value that may be used to pay an unspecified person the price of any goods purchased or borrowed or any services provided and which may be sold to or

purchased from an unspecified person (limited to that recorded on electronic devices or other objects by electronic means and excluding Japanese and other foreign currencies and Currency Denominated Assets; the same applies in the following item) and that may be transferred using an electronic data processing system; or

(ii) proprietary value that may be exchanged reciprocally for proprietary value specified in the preceding item with an unspecified person and that may be transferred using an electronic data processing system.

Though the definition is complicated, in short, a cryptocurrency which is usable as a payment method to an unspecified person and not denominated in a fiat currency falls under the definition of Virtual Currency.

"Currency Denominated Assets" means any assets which are denominated in Japanese or other foreign currency, and which do not fall under the definition of Virtual Currency. For example, prepaid e-money cards usually fall under Currency Denominated Assets. If a coin issued by a bank is guaranteed to have a certain value of a fiat currency, such a coin will likely be treated as a Currency Denominated Asset rather than a Virtual Currency. Please note that, under Article 2, Paragraph 5 of the revised PSA amending the term "Virtual Currency" to "Crypto Asset", the existing definition of "Virtual Currency" will remain unchanged. Accordingly, it is generally understood that the change in reference from "Virtual Currency" to "Crypto Asset" will result in no substantive change to the legal interpretation of the term. Therefore, please note that, hereafter, when we refer to the relevant provisions under the PSA Revisions, we use the term "Crypto Asset" instead of "Virtual Currency" for the purposes of this article.

Definition of Exchange Services

Under the PSA, the term "Virtual Currency Exchange Services" means any of the following acts carried out as a business:

(i) sale and purchase of Virtual Currency or exchange of Virtual Currency for other Virtual Currency;

(ii) intermediary (*bai-kai*), brokerage (*tori-tsugi*) or delegation (*dai-ri*) for the acts listed in (i) above; or

(iii) management of users' money or Virtual Currency in connection with the acts listed in (i) or (ii) above.

Please note that it was highlighted in the Report, that crypto asset custody services ("**Crypto Asset Custody Service**") share common risks with Exchange Services. These risks include leakage of users' crypto assets ("**User Crypto Assets**"), bankruptcy of service providers, and risks associated with money laundering and terrorism financing. To address this, the PSA Revisions provide that managing crypto assets for the benefit of another person constitutes an Exchange Service, "unless otherwise specifically stipulated under any other law, in cases where the relevant management activity is performed in the course of a business". As a result of this provision, a Crypto Asset Custody Service would also constitute an Exchange Service, even if the Crypto Asset Custody Service does not involve any of the acts listed in items (i) and (ii) above.

Registration process for the Exchange Provider

The applicant must be (i) a stock company (*kabushiki-kaisha*), or (ii) a Foreign Virtual Currency Exchange Service Provider which has an office(s) and representative in Japan. Accordingly, any foreign entity wishing to register as an Exchange Provider must establish either a subsidiary (in the form of *kabushiki-kaisha*) or a branch in Japan.

In addition, the applicant must have: (a) a sufficient financial basis (minimum capital amount of JPY10 million and positive minimum net assets); (b) a satisfactory organisational structure and certain systems to conduct the Exchange Service appropriately and properly; and (c) certain systems to ensure compliance with relevant laws and regulations.

The applicant must submit a registration application containing: (i) its trading name and address; (ii) capital amount; (iii) director's name; (iv) the name of the Virtual Currencies to be handled; (v) contents and means of Exchange Services; (vi) name of outsourcee (if any) and its address; and (vii) method of segregation management and other particulars.

The registration application must be accompanied by documents including: (i) a document pledging that there are no circumstances constituting grounds for refusal of registration; (ii) extract of the certificate of residence of its directors, etc.; (iii) a résumé of the directors, etc.; (iv) a list of shareholders; (v) financial documents; (vi) documents containing particulars regarding the establishment of a system for ensuring the proper, secure provision/performance of Exchange Services; (vii) an organisational chart; (viii) internal rules; and (ix) a form of the contract to be entered into with users.

During the registration process, the FSA requests applicants to fill in the checklist, which consists of approximately 400 questions, in order to confirm that the applicants have established systems to properly and securely perform the Exchange Service. In addition, the FSA separately prepares a detailed progress chart to confirm the checking process. The registration process is a kind of due diligence by the FSA, and the FSA deliberates on whether to approve the registration. In substance, the "registration" process is akin to the issuance of a "licence".

Upon registration, the registry of Exchange Service Providers will be made publicly available.

Principal regulation on Exchange Provider

An Exchange Provider must: (i) take measures necessary to ensure safe management of information; (ii) provide information to users such as the content of transactions, outline of each crypto asset handled by the provider, fees, the amount of cash or crypto asset which the provider has received from the user, the date of receipt, transaction records, etc.; (iii) take measures necessary for the protection of users and proper performance of its services; (iv) segregate users' property from its own property (with respect to cash, bank deposit or trust; with respect to crypto assets, clear distinction in a manner such that the User Crypto Assets is immediately identifiable), and regularly undergo an audit of the status of such segregated management by a certified public accountant or audit firm; and (v) establish an internal management system to make fair and appropriate responses to customer complaints and take measures to resolve any disputes through financial ADR proceedings.

Additional regulations applicable to Exchange Providers under the PSA Revisions

The PSA Revisions propose the following changes to the current regulatory system governing Exchange Providers in order to enhance protection of users and to clarify the rules relating to Exchange Providers:

(i) expansion of the grounds upon which applications for registration as an Exchange Provider may be rejected;

(ii) introduction of a system of advance notification for any proposed amendment to certain matters in respect of the relevant crypto asset, such as the name thereof;

(iii) introduction of regulations governing advertisement and solicitation in respect of Exchange Services;

(iv) introduction of disclosure requirements where crypto assets are exchanged (or where certain similar transactions are undertaken) via the grant of credit to users;

(v) enhancement of the obligation on Exchange Providers to preserve users' assets; and

(vi) grant of rights to users to enable their receipt of preferential payments when claiming for the return of crypto assets.

However, with respect to (v) "enhancement of the obligation on Exchange Providers to preserve users' assets" above, under the PSA Revisions, an Exchange Provider is required to both manage the money of users separately from its own money, and to entrust users' money to a trust company or other similar entity that will act as trustee over users' money, in accordance with the provisions of the relevant Cabinet Office Ordinance.

In addition, the PSA Revisions require an Exchange Provider to manage User Crypto Assets separately from other User Crypto Assets in such manner as is specified in the relevant Cabinet Office Ordinance, in order to enhance the protection of users. Although the relevant Cabinet Office Ordinance has not yet been issued, we understand from the explanatory material prepared by the FSA that an Exchange Provider will be required "to manage the crypto assets of users (other than crypto assets required for the smooth performance of Exchange Services) through highly reliable mechanisms, such as cold wallets".

Further, pursuant to the PSA Revisions, an Exchange Provider is required to (i) hold for its own account, crypto assets of the same kind and quantity as the User Crypto Assets that are subject to "requirements specified by the relevant Cabinet office Ordinance as being necessary for ensuring users' convenience and the smooth performance of crypto asset exchange services" ("**Performance Assurance Crypto Assets**"), and (ii) manage Performance Assurance Crypto Assets separately from its own crypto assets (other than Performance Assurance Crypto Assets). In other words, when an Exchange Provider manages its User Crypto Assets in hot wallets, the Exchange Provider would likely be required to (i) hold its own crypto assets of the same kind and quantity as the User Crypto Assets that are managed in hot wallets, and (ii) manage Performance Assurance Crypto Assets in cold wallets separately from its own crypto assets (other than Performance Assurance Crypto Assets).

Sales regulation

Overview

Cryptocurrencies (including Virtual Currencies) do not fall within the definition of "Securities" under the Financial Instruments and Exchange Act of Japan ("**FIEA**"), and the sale of Virtual Currencies or tokens (including ICO) are not specifically or directly regulated by the FIEA (please note that a certain type of token may be subject to regulation of the Act as discussed below).

There are various types of tokens issued by way of ICO, and Japanese regulations applicable to ICOs vary according to the respective schemes.

Main types of tokens and applicable regulations

1. *Virtual Currency type*

   If the token falls under the definition of Virtual Currency, the Virtual Currency regulation under the PSA is applicable. In accordance with the prevalent current practice, (i) if the tokens issued via ICO are already dealt with by Japanese or foreign exchanges, such tokens would be considered as falling within the definition of Virtual Currency under the PSA based on the rationale that exchange markets for such tokens

must already be in existence, and (ii) even if certain tokens are not yet dealt with by Japanese or foreign exchanges, in the case where the token issuer does not give substantial restrictions prohibiting such tokens from being exchanged with Japanese or foreign fiat currencies or Virtual Currencies, such tokens would likely fall within the definition of Virtual Currency under the PSA.

In addition, on June 25, 2019, the Japan Virtual Currency Exchange Association ("**JVCEA**"), which is a self-regulatory organisation established under the PSA, published the draft of the self-regulatory rule and guideline regarding ICOs for Virtual Currency-type tokens, named the "Rules for Selling New Virtual Currency" ("**ICO Rule**"). According to the ICO Rule, there are two types of ICO, which can be described as follows: (i) an Exchange Provider issues new tokens and sells such tokens by itself; or (ii) a token issuer delegates Exchange Providers to sell the newly issued tokens. Generally speaking, the ICO Rules stipulates the following requirements for each type of ICO:

(i) maintenance of a structure for review of a targeted business which raises funds via ICO;

(ii) information disclosure of the token, the token issuer's purpose for the funds, or the like;

(iii) segregated management of funds (both fiat and crypto assets) raised by ICO;

(iv) proper account processing and financial disclosure of funds raised by ICO;

(v) safety assurance of the newly issued token, its blockchain, smart contract, wallet tool, and the like; and

(vi) proper valuation of newly issued tokens.

2. *Securities (equity interest in an investment fund) type*

The FIEA Revisions introduced the concept of "Electronically Recorded Transferable Rights" ("**ERTRs**"), which clarify the scope of tokens governed by the FIEA. The concept of ERTRs relates to the rights set forth in Article 2, Paragraph 2 of the FIEA that are represented by proprietary value that is transferable by means of an electronic data processing system (but limited only to proprietary values recorded in electronic devices or otherwise by electronic means), excluding those rights specified in the relevant Cabinet Office Ordinance in light of their negotiability and other factors. Although Article 2, Paragraph 2 of the FIEA refers to rights of various kinds, tokens issued in "security token offerings" ("**STOs**") are understood to constitute, in principle, "collective investment scheme interests" ("**CISIs**") under the FIEA. CISIs are deemed to have been formed when the following three requirements are met: (i) investors (i.e., rights holders) invest or contribute cash or other assets to a business; (ii) the cash or other assets contributed by investors are invested in the business; and (iii) investors have the right to receive dividends of profits or assets generated from investments in the business. Tokens issued under STOs would constitute ERTRs if the three requirements above are satisfied.

To put it simply, rights treated as "Paragraph 2 Securities" (i.e., rights that are deemed as securities pursuant to Article 2, Paragraph 2 of the FIEA) and represented by negotiable digital tokens will be treated as Paragraph 1 Securities unless they fall under an exemption. As a result of the application of disclosure requirements to ERTRs, issuers of ERTRs are in principle required, upon making a public offering or secondary distribution, to file a securities registration statement and issue a prospectus. Any person who causes other persons to acquire ERTRs or who sells ERTRs to other

persons through a public offering or secondary distribution must deliver a prospectus to such other persons in advance or at the same time.

As ERTRs are expected to constitute Paragraph 1 Securities, registration as a Type I Financial Instruments Business Operator will be required for the purposes of selling, purchasing or handling the public offering of ERTRs in the course of a business. In addition, any ERTR issuer who solicits acquisition of such ERTR (i.e., undertaking an STO), will be required to undergo registration as a Type II Financial Instruments Business Operator, unless such issuer qualifies as a specially permitted business for qualified institutional investors.

3. *Prepaid card type*

   If the tokens are similar in nature to prepaid cards and can be used as consideration for goods or services provided by token issuers, they may be regarded as "Prepaid Payment Instruments" (*maebarai-shiki-shiharai-shudan*), which are subject to the relevant regulations under the PSA (in this case, regulation on Virtual Currency under the same Act would not be applicable).

Introduction to regulations governing crypto asset derivative transactions

Currently, Virtual Currency margin trading services are offered by many Exchange Providers. However, even though Virtual Currency derivatives transactions are regulated in several countries, they are not regulated in Japan.

The FIEA Revisions regulate crypto asset derivatives transactions to the FIEA in order to protect users and ensure that such transactions are conducted appropriately, by establishing certain regulations of crypto asset derivatives transactions. Specifically, for the purposes of subjecting derivatives transactions involving "Financial Instruments" or "Financial Indicators" to certain entry regulations and rules of conduct issued under the FIEA, the FIEA Revisions have included "crypto assets" and "standardized instruments created by a Financial Instruments Exchange for the purposes of facilitating Market Transactions of Derivatives by standardizing interest rates, maturity periods and/or other conditions of (crypto assets)" in the definition of "Financial Instruments". Further, the FIEA Revisions have incorporated the prices, interest rates, etc. of crypto assets into the definition of "Financial Indicators".

Since crypto assets will be included in the definition of Financial Instruments, the conduct of Over-the-Counter Derivatives Transactions related to crypto assets or related intermediary (*baikai*) or brokerage (*toritsugi*) activities will also constitute Type I Financial Instruments Business. Accordingly, business operators engaging in these transactions will need to undergo registration as Financial Instruments Business Operators in the same way as business operators engaging in foreign exchange margin trading.

Introduction to regulations governing unfair acts in crypto asset or crypto asset derivative transactions

The FIEA Revisions contain the following prohibitions against unfair acts (the conduct of which is punishable by penalties) in respect of crypto asset spot transactions and crypto asset derivative transactions, regardless of the violating party:

(a) prohibition of wrongful acts;

(b) prohibition on dissemination of rumours, usage of fraudulent means, assault or intimidation; and

(c) prohibition on market manipulation.

These prohibitions are intended to enhance protection of users and to prevent unjust enrichment.

However, insider trading is not regulated under the FIEA Revisions at this moment in time, due to difficulties in formulating a clear concept of crypto asset issuers, as well as the general inherent difficulties associated with the identification of undisclosed material facts.

Taxation

One of the most important issues in Japanese taxation of cryptocurrencies has been the treatment of consumption tax. Under Japanese tax law, sale of cryptocurrencies has been subject to consumption tax in cases where the office of the transferor is located in Japan. However, the relevant tax law was amended in 2017. As such, if the sold cryptocurrency can be considered as Virtual Currency (such as Bitcoin) under the Payment Services Act, consumption tax will not be imposed (from July 1, 2017 onwards). The National Tax Agency of Japan also announced that gains realised by the sale or use of Virtual Currency shall be treated as "miscellaneous income" (*zatsu-shotoku*) where the taxpayer is unable to utilise losses elsewhere to offset gains realised by the sale or use of Virtual Currency. Furthermore, inheritance tax will be imposed upon the estate of a deceased person in respect of Virtual Currency that was held by such person.

Money transmission laws and anti-money laundering requirements

Money transmission

Under Japanese law, only licensed banks or fund transfer business operators are permitted to engage in the business of money remittance transactions. Money remittance transactions means, according to Supreme Court precedent, "to undertake the task of transferring funds requested by customers utilising the systems of fund transfer without transporting cash between distant parties, and/or to carry out such task". Technically speaking, Virtual Currency does not fall under the definition of "fund". However, if the remittance transaction of a Virtual Currency includes the exchange of fiat currencies in substance, such transaction will likely be deemed as a money remittance transaction.

Anti-money laundering requirements

Under the APTCP, Exchange Providers are obligated to: (i) verify identification data of the customer and a person who has substantial control over the customer's business for the purpose of conducting the transaction and occupation of business; (ii) prepare verification records and transaction records; (iii) maintain the records for seven years; and (iv) report suspicious transactions to the relevant authority, and so forth.

Promotion and testing

On June 15, 2018, the "Basic policy of Regulatory Sandbox scheme in Japan" was announced by the Cabinet Office of Japan. The Regulatory Sandbox is a scheme to implement new outstanding technology such as AI, IoT, big data and blockchain, and welcomes new ideas for the "testing project" involving any industrial sector, inside and outside Japan.

Ownership and licensing requirements

There is no restriction on an entity simply owning cryptocurrencies for its own investment purposes, or investing in cryptocurrencies for its own exchange purposes. As a general rule,

the Virtual Currency regulation under the PSA will not be applicable unless an entity conducts Exchange Services as a business. Please note, however, that the sale of certain types of tokens may be subject to regulation under the PSA or the FIEA, as applicable, as discussed in "**Sales regulation**" above.

Mining

The mining of cryptocurrencies is not regulated. Mining in itself does not fall under the definition of an Exchange Service. Please note, however, that if the mining scheme is formulated as a collective investment scheme and contains the sale of equity interest in an investment fund, it is subject to the relevant regulations by the FIEA.

Border restrictions and declaration

Border restrictions

Under the Foreign Exchange and Foreign Trade Act of Japan, if a resident or a non-resident has received a payment exceeding JPY30 million made from Japan to a foreign country or made from a foreign country to Japan, the resident or non-resident must report it to the Minister of Finance. If a resident has made a payment exceeding JPY30 million to a non-resident either in Japan or in a foreign country, the same reporting requirement applies.

Recently, this rule has been extended to receiving or making payments via Virtual Currency. On May 18, 2018, the Ministry of Japan announced that the receipt of payment of Virtual Currency or the making of a payment of Virtual Currency, the market price of which exceeds JPY30 million as of the payment date, must be reported to the Minister of Finance.

Declaration

There is no obligation to declare cryptocurrency holdings when passing through Japanese Customs.

Reporting requirements

As explained above, a certain payment or receipt of payment exceeding JPY30 million, either by fiat currencies or Virtual Currencies, is subject to a reporting obligation to the Minister of Finance under the Foreign Exchange and Foreign Trade Act.

A Virtual Currency Exchange Service Provider must report to the relevant authority if it detects a suspicious transaction.

Estate planning and testamentary succession

There has been no established law or court precedent with respect to the treatment of cryptocurrencies under Japanese succession law. Under the Civil Code of Japan, inheritance (i.e., succession of assets to heir(s)) occurs upon the death of the decedent. Theoretically, cryptocurrencies will be succeeded to by heir(s). However, given the anonymous nature of cryptocurrencies, the identification and collection of cryptocurrencies as inherited property would be a material issue unless the relevant private key or password is known to the heir(s). On the other hand, even if the private key or password is unknown, to the extent that the inherited property can be identified, theoretically, inheritance tax may be imposed. An enclosed and notarised testament may be one of the solutions for these issues. However, from the perspective of Japanese law, the legal framework must be improved so that these new issues can be adequately dealt with.

Taro Awataguchi
Tel: +81 3 6775 1104 / Email: taro.awataguchi@amt-law.com

Taro Awataguchi, a fintech partner at Anderson Mōri & Tomotsune ("AMT"), has extensive experience in advising clients, including Virtual Currency Exchange Service Providers (i.e., registered providers) and applicants for the registration, on various matters related to fintech and cryptocurrencies. AMT is one of the largest legal firms (Big Four) in Japan, and Taro, as a member of AMT's fintech team which has one of the leading fintech practices in Japan, provides innovative, up-to-date legal advice to clients in this fast-growing and cutting-edge industry.

In addition, Taro was appointed by the Tokyo District Court as the trustee in bankruptcy proceedings of a Bitcoin-related company, where various legal issues and disputes related to Bitcoin were involved. He is a frequent speaker and author in the fintech field. For example, he made a speech on "Cryptocurrencies" at the American Bar Association ("ABA") Section of International Law 2016 Fall Meeting held in Tokyo, and he is a co-author of the Japan chapter of *The International Comparative Legal Guide to: Fintech 2017* and *2018*.

Taro already has extensive experience in the field of banking, financing, financial regulation and insolvency. He is one of the pioneers of Asset-Based Lending practice in Japan, and serves as the head of managing committee of the ABL Association. He is recognised by *Best Lawyers* (banking and financing law). He is noted for successful creditor representations in various cross-border insolvency matters, including representation of Japan's first-ever secured creditors' committee in getting full recovery from the corporate reorganisation proceedings of Spansion Japan Limited.

Takeshi Nagase
Tel: +81 3 6775 1200 / Email: takeshi.nagase@amt-law.com

Takeshi Nagase handles finance and corporate transactions, and has considerable experience advising on all legal aspects of public and private mergers and acquisitions, joint ventures, fintech, and other corporate and financial advisory matters. His clients range from prominent financial institutions to crypto asset start-ups. Between 2013 and 2014, Takeshi served on secondment in the Disclosure Department of the Financial Services Agency of Japan, where he was an instrumental part of the team that revised the laws and guidelines governing disclosure by listed companies, and prepared the Japanese Stewardship Code. Additionally, he handled a broad range of finance and corporate transactions on a secondment stint with the legal department of a major Japanese securities firm from 2015 to 2017. As a result of the unique perspective he has gained from these professional experiences, Takeshi is often sought for his advice on finance-related matters, particularly by clients seeking to evaluate transactions from the regulator's point of view. Recently, Takeshi has extended his focus to crypto asset laws, including regulatory requirements applicable to registration of crypto asset exchange service providers, initial coin offerings, and the like.

Anderson Mōri & Tomotsune

Otemachi Park Building, 1-1-1 Otemachi, Chiyoda-ku, Tokyo, 100-8136, Japan
Tel: +81 3 6775 1000 / URL: www.amt-law.com

Jersey

Christopher Griffin, Emma German & Holly Brown
Carey Olsen Jersey LLP

Government attitude and definition

Jersey continues to embrace fintech including blockchain and distributed ledger technology ("**DLT**") as a pioneer in fintech regulation. Jersey enjoys a sophisticated legal, regulatory and technological infrastructure, supporting development and innovation in fintech, including:

- cryptocurrency exchanges and security token exchanges;
- security token and non-security token issuances;
- electronic identification;
- online payment solutions; and
- fintech funds and other vehicles.

Jersey recognised cryptocurrencies as a separate asset class long before the "ICO Craze" of 2017, when the island's regulator, the Jersey Financial Services Commission (the "**JFSC**") licensed the world's first Bitcoin-focused, regulated fund (GABI Plc). From that point onwards, the island has seen a surge of interest in exchange vehicles, token issuers and fintech funds choosing Jersey; including the world's largest investment fund (The SoftBank "Vision Fund" which raised $97bn over two years). Both GABI and Softbank were advised by Carey Olsen Jersey LLP ("Carey Olsen").

The JFSC is a member of the Global Fintech Innovation Network and participates in the cross-border testing pilot.

Jersey has an exceptional pool of blockchain expertise, developed from the JFSC's forward-thinking attitude combined with Jersey's flexible range of corporate vehicles and favourable tax regime.

Examples of structures that have recently used Jersey (advised in each case by Carey Olsen) include:

- CoinShares Fund I, a venture capital fund investing in Ether (a cryptocurrency used as a payment on the Ethereum blockchain platform) and Initial Coin Offerings ("**ICOs**"); and
- Binance, the world's largest cryptocurrency exchange, which has established a Jersey exchange platform.

Jersey strives to promote fintech development by supporting local fintech talent. Digital Jersey, a government-backed economic development agency and industry association dedicated to the growth of the digital sector, aims to do this.

Blockchain and cryptocurrency/digital asset regulation

To date, Jersey has not needed to introduce blockchain-specific legislation because the prevalent fintech matters (set out below) have not necessitated it. These can be grouped as follows:

(i) Initial Coin Offerings; ("**ICOs**");[1]

(ii) Security Token Offerings ("**STOs**");

(iii) non-security token issuances;

(iv) Cryptocurrency Exchanges (so-called Virtual "Currency Exchanges");

(v) Security Token Exchanges;

(vi) arrangements clearly falling within the existing regulatory framework such as custody; and

(vii) Jersey funds investing in digital assets.

The regulatory treatment of each of these is set out below:

(i) ICOs

Jersey has seen a large number of ICOs. This is in part because the JFSC recognised that ICOs with proper substance and backed by a credible promoter should be nurtured.

ICOs involve the issuance of a coin. Consideration must be given as to whether such coin/token/asset constitutes a "security" under Jersey law, and therefore whether it falls within the existing regime regulating securities and their issuances. To assist with this analysis, the JFSC issued guidance on the interpretation of the various categories of digital assets and their corresponding treatment, entitled ***Guidance Note on the Application Process for Issuers of Initial Coin Offerings*** (the "**JFSC Guidance**").[2]

In short, the JFSC Guidance outlines the three key areas of the JFSC's regulatory focus, being:

- the economic function and purpose of the digital assets to be issued;
- their underlying purpose; and
- whether they are tradeable and transferable.

Against this backdrop, Carey Olsen advised on the launch of Jersey's first ICO in December 2017, ARC Reserve Currency. ARC is an asset-backed "stablecoin" cryptocurrency, which is designed to act like a currency without the volatility spikes one sees in other cryptocurrencies such as Bitcoin. Carey Olsen worked closely with the JFSC to ensure that the ARC coin launched ahead of time and with a degree of regulatory scrutiny that should give prospective purchasers a degree of comfort not available in other jurisdictions. Subsequently, Carey Olsen built on its ICO expertise by advising on AX1 token, an ICO designed to raise capital for investment in a cryptocurrency mining operation based in the UK.

In both instances, the JFSC adopted a purposive and pragmatic approach to approving the ICOs, focusing on consumer protection and anti-money laundering whilst recognising that ICO promoters use a Jersey-incorporated issuer due to Jersey's reputation as a well-regulated and reputable jurisdiction.

In order to give prospective ICO investors a degree of disclosure and comfort that may not be available in many other jurisdictions, the JFSC sets out certain requirements on an ICO issuer.

The ICO issuer is required to:

- be a Jersey incorporated company;
- receive the JFSC's consent before undertaking any form of activity;
- comply with the JFSC's Sound Business Practice Policy (see below);
- apply relevant AML/CFT requirements to either purchase tokens from or sell tokens back to the issuer;
- appoint a Jersey-licensed administrator;
- appoint and maintain a Jersey-resident director on the board;
- be subject to an ongoing annual audit requirement;
- have procedures and processes in place to (i) mitigate and manage the risk of retail investors investing inappropriately in the ICO, and (ii) ensure retail investors understand the risks involved;
- prepare an information memorandum which complies with certain content requirements required under Jersey company law; and
- ensure that any marketing material is clear, fair and not misleading, and include in any such materials certain prescribed consumer warnings.

(ii) Security Token Offerings

Whilst there is no universally recognised terminology for the classification of tokens, as mentioned above, the JFSC Guidance distinguishes between digital assets for Jersey purposes by considering whether they are a "security" or not. This is particularly important for the purposes of Jersey law under the Island's statutory instrument governing the raising of capital, the Control of Borrowing (Jersey) Order 1958 ("**COBO**").

Before a security token issuer can undertake any activity, it requires consent from the JFSC under COBO and the type of COBO consent granted by the JFSC will depend on whether the token is categorised as a "security" under COBO.

The JFSC Guidance stipulates that a token which has one or more of the following characteristics will be regarded by the JFSC as a "security":

- a right to participate in the profits/earnings of the issuer or a related entity;
- a claim on the issuer or a related party's assets;
- a general commitment from the issuer to redeem tokens in the future;
- a right to participate in the operation or management of the issuer or a related party; and
- an expectation of a return on the amount paid for the tokens.

If the issuance constitutes a security and is to be an STO, the usual Jersey considerations for the issuance of a security apply including COBO, the Companies (General Provisions) (Jersey) Order 2002 regarding the issuance of a prospectus and the Companies (Jersey) Law 1991 and activities related to the securities, including dealing under the Financial Services (Jersey) Law 1998 (the "**FSJL**").

(iii) Non-security token issuances

Coin and token issuances that do not constitute "securities" do not fall under the ambit of the FSJL.

The JFSC Guidance contains a helpful statement that the JFSC will not treat a utility token (i.e. a token conferring a usage right and with no economic or voting rights) as a "security"

token solely by reason of the fact that it might be traded in the secondary market (e.g. listed on an exchange).

The application for a non-security token issuer's COBO consent is to be accompanied by analysis prepared by the issuer's legal advisers, outlining:

- the proposed activity, including relevant timelines;
- details of the issuer;
- rationale for the proposed activity, amount to be raised and use of proceeds;
- a summary of the features of the tokens;
- a summary of the token purchase and redemption processes;
- the service providers to the issuer;
- the relationship between issuers and holders of the tokens;
- the management of underlying assets and security rights over such assets (if any) for holders of the tokens;
- how the activity will be wound up/dissolved and assets (if any) distributed to the holders of the tokens; and
- a Jersey legal and regulatory analysis, including consideration of relevant legislation or other regulatory laws.

Following grant of the COBO consent, the issuer must seek the prior consent of the JFSC to any material change to the matters contained in the application.

(iv) Virtual Currency Exchanges ("**VCEs**")

At an early stage, the JFSC saw an increase in the volume and value of trading in cryptocurrencies as they were exchanged into fiat currencies and *vice versa*. In 2016 and in recognition of the regulatory gap, the JFSC brought the provision of VCE services in Jersey under Jersey's regulatory umbrella by extending the scope of existing laws and regulations.

As a result, the Proceeds of Crime (Jersey) Law 2009 ("**POCJL**") requires VCEs to comply with the Island's laws, regulations, policies and procedures aimed at preventing and detecting money laundering and terrorist financing. POCJL also categorises VCEs as "supervised business" and consequently introduces a requirement for VCEs to register with, and be subject to, the supervision of the JFSC. The JFSC also allows VCEs with turnover of less than £150,000 per calendar year to test VCE delivery mechanisms in a live environment without the full registration requirements and associated costs. As such, Jersey's VCE regulation balances the need to provide robust regulation with a desire to foster the development of the Island's burgeoning crypto-credentials.

(v) Security Token Exchanges

Jersey has recently seen an influx of potential security token exchange platforms and Carey Olsen is working closely with credible promoters to advise on these matters. The JFSC have indicated that security token exchange businesses will be required to be regulated under the FSJL to undertake "investment business" (the "**IB Licence**").

A standard application for an IB Licence will take approximately eight weeks. An application for a digital assets-related matter may take a little longer. A full regulatory application to the JFSC will be required and will include the following documents:

- a regulatory application form;
- a business plan; and
- a business risk assessment.

In terms of regulatory capital requirements, the main requirement to be aware of is that an exchange platform will be required to maintain at all times:

- a net liquid assets position of 130% of its projected quarterly expenditure;
- a minimum of £25,000 paid-up share capital; and
- a minimum net assets position of £25,000 at all times.

In addition, a Jersey security token exchange must be audited and the composition of the board must comply with the Jersey regulatory and economic substance requirements, being:

- there must be a minimum of two Jersey resident directors;
- the board must meet with adequate frequency having regard to the amount of decision making being undertaken;
- at meetings there must be a quorum of directors physically present in Jersey; and
- the directors of the company must have the necessary knowledge and expertise to discharge their duties (this is assessed on a whole-board basis).

Once an IB Licence has been obtained, the holder will need to observe the provisions of the JFSC's Code of Practice for Investment Business.

There are locally regulated administrators in Jersey who can assist by providing "incubation" services to entities and groups that are new to Jersey.

There is no requirement to have electronic clearing and settlement or for clearing of security tokens to be carried out by a clearing house or central depositary.

(vi) Applications under the existing regulatory framework

JFSC's Sound Business Practice Policy

The JFSC will treat transactions with digital assets and cryptocurrencies as a "sensitive activity" under the JFSC's Sound Business Practice Policy.

The practical consequence of this is that certain AML/CFT obligations are imposed on the issuer, such as to carry out checks on: (i) the purchasers of the tokens who purchase coins directly from the issuer; and (ii) the holders of tokens issued by the issuer in the event they are sold back to the issuer. In such circumstances, the issuer will be required to obtain information to: (a) establish and obtain evidence to verify identity; and (b) establish and, depending on the level of risk, obtain evidence to verify the source of funds and source of wealth.

Custody services and arrangements for holding digital assets

For VCEs and security token exchanges, services related to the custody of the digital assets need to be considered. There are two models: (i) custody services provided by the exchange itself (or a related entity) to investors and exchange users; or (ii) custody services outsourced to a third party custody provider to be provided to investors and exchange users.

In both models, where digital assets will be stored offline or where the investor or exchange user is not provided with the keys to access the digital asset, the investor/exchange user will no longer have control over the digital assets they have invested in. In this way, it is likely that the relevant custodian entity will be providing trustee services and will need to be regulated for "trust company business" under the FSJL. However, where the storage of digital assets is incidental or ancillary to the main purpose of the entity and where there was no separate remuneration, an exemption may apply. Early advice should be sought on this point, and this is something Carey Olsen has experience of advising on.

(vii) Jersey Private Funds and Jersey Expert Funds

Jersey fund structures are used in the digital assets space. Such entities will be required to comply with the existing regulatory framework, as set out in brief below.

Jersey regulatory classifications provide a "safe harbour" with three-day approval from the JFSC for the majority of non-retail funds.

Jersey Private Funds are fast and flexible to set up, with minimal requirements for funds with fewer investors (only up to 50 investors). Jersey Private Funds are not regulated and must not be listed on a stock exchange. There is no limit on fund size, no investment or borrowing restrictions, they can be open or closed for redemptions by investors and are open to "professional" investors and those investing £250,000 or more. There is a "Fast track" approval by self-certification by the fund administrator.

Expert Funds are attractive for non-retail schemes aimed at "Expert Investors". Expert Funds can be established quickly and cost-effectively and must comply with the Jersey Expert Fund Guide (the EF Guide).

The definition of "Expert Investor" is crucial. An investor must fall within any one of the 10 categories, which include a person or entity: in the business of buying or selling investments; with a net worth of more than US $1m, excluding principal place of residence; with at least US $1m available for investment; connected with the fund or a fund service provider (there is a flexible approach to carried-interest arrangements); or (the simplest category) making an investment or commitment of US $100,000 or more (or currency equivalent).

The investment manager/adviser must be: established in an OECD member or any other state or jurisdiction with which the JFSC has entered into a Memorandum of Understanding or equivalent; regulated in its home jurisdiction (or, if not required to be, approved by the JFSC, which usually occurs on an expedited basis); without convictions or disciplinary sanctions; solvent; and experienced in using similar investment strategies to those adopted by the Expert Fund. If the investment manager/adviser does not meet these requirements, it may approach the JFSC on a case-by-case basis. Of course, if permission is granted then, absent any material change, the investment manager/adviser will not need specific approval to establish further Expert Funds. An investment manager/adviser is not required for certain self-managed funds, such as direct real estate or feeder funds.

All Jersey funds (other than notification only funds) are eligible to be marketed into the European Union and European Economic Area ("**EU/EEA**") in accordance with the Alternative Investment Fund Managers Directive ("**AIFMD**") through national private placement regimes and (once available) through the passporting regime. Jersey funds with a Jersey manager which are not actively marketed into the EU/EEA fall outside the scope of AIFMD.

Taxation

Jersey is a low-tax jurisdiction.

There are currently no laws in Jersey specifically regulating the taxation of cryptocurrencies or digital assets. Accordingly, it is likely that such assets will be taxed in accordance with general Jersey taxation principles and provisions.

Promotion and testing

Jersey promotes and tests fintech firms' products and service in a number of ways.

In terms of testing products and services, the JFSC has proven itself to be a pro-active and forward-thinking regulator in becoming a member of the Global Fintech Innovation Network (a group of international regulators and observers committed to supporting innovative products and services) and participating in the cross-border testing pilot which launched in January 2019 offering firms the opportunity to test their products and services in multiple jurisdictions.[3]

Jersey also operates a sandbox run through Digital Jersey, supporting local fintech firms and fintech firms seeking to relocate to Jersey.[4]

In terms of promoting fintech and thought-leading in Jersey, the Digital Assets Working Group (the "**DAWG**") works hard to raise awareness and interest in Jersey. Combining representatives of the States of Jersey, representatives of the JFSC and other interest groups on the Island, the DAWG is a group of individuals knowledgeable in the fintech space promoting digital assets and blockchain technologies in Jersey. Carey Olsen is a founder member of the DAWG and is an active participant and contributor.

Mining

Mining cryptocurrencies is not covered by any specific piece of legislation or regulation in Jersey. However, depending on the manner in which mining activities are conducted, it may fall within the existing regulatory framework for funds (mentioned above).

Border and reporting restrictions

At present, there are no border restrictions in place on declaring cryptocurrency holdings. Equally, there are currently no specific reporting requirements triggered for cryptocurrency payments.

The future of blockchain and DLT in Jersey

As a nascent technology, international industry practices around blockchain and DLT are still evolving and its applications and use cases (including outside the finance industry) being asserted. To maintain its place as a respected well-regulated international finance centre, Jersey is cognisant, and encouraging, of the advantages blockchain and DLT brings to Jersey's finance industry.[5]

As a long established well regulated international finance centre, Jersey boasts a host of industry experience and local expertise in Jersey,[6] making Jersey an ideal jurisdiction to launch new blockchain and DLT initiatives.

Leveraging this existing expertise and the low-tax environment, we expect to see Jersey and Jersey vehicles continue to be used in both established areas of finance as they embrace blockchain solutions (such as proptech, online settlement solutions e-ID and regtech, etc.) and new areas of finance and other sectors as blockchain and DLT use cases are established.

The JFSC's considered and measured approach to fintech regulation to date should equip Jersey to be a leading blockchain and DLT jurisdiction of the future by ensuring regulation in Jersey remains appropriate and commensurate to the product or service in question.

We would be happy to discuss any blockchain or DLT initiatives backed by persons of substance. Please do contact us using the details below.

* * *

Endnotes

1. In the fintech space, the ICO terminology has now largely been superseded by reference to security and non-security tokens, a reflection of the evolving regulatory backdrop. We retain reference to ICOs in this article because we, Carey Olsen, have advised in relation to a number of ICOs and that was the terminology used at that time. The settled approach now is to determine whether a coin or token or other digital asset issued constitutes a security or not and therefore whether it is a "security token" or not. We have addressed STOs and non-security token issuances separately.
2. It has been confirmed that this JFSC Guidance has a wider application and can be used to inform how digital assets and cryptocurrencies more generally will be treated. Available at jerseyfsc.org/media/2003/2018-07-12_jfsc-issues-ico-guidance-note.pdf.
3. The window for applications to participate in the January 2019 pilot has now closed.
4. See: www.digital.je.
5. Such as: (i) real time settlement; and (ii) greater transparency as to origination or provenance of the asset in question. For example, as Jersey currently has no restrictions or requirements around financial settlement, Jersey is an ideal jurisdiction from which to launch securities and cryptocurrency exchanges.
6. Including in banking, international payments, compliance, funds, capital markets, real estate and company administration.

Christopher Griffin
Tel: +44 1534 822 256 / Email: christopher.griffin@careyolsen.com

Christopher spearheads Carey Olsen's crypto practice and digital assets team, advising on the launch in 2017 of Coinshares Fund I (a venture cap fund investing in crypto assets) and ARC Reserve Currency, Jersey's first initial coin offering or "ICO". Christopher was instrumental in the launch of the Jersey platform for Binance, the world's largest cryptocurrency exchange. Christopher also advises on all aspects of fund and corporate transactions, including the legal and regulatory aspects of fund launches, and joint ventures. He also has considerable experience in dealing with the Jersey Financial Services Commission in navigating investment vehicles through the Jersey regulatory approval process. Christopher has broad experience of both general international corporate and funds work with particular expertise in private equity and hedge funds, having spent 10 years in the City at Ashurst, RAB Capital plc and most recently at SJ Berwin.

Emma German
Tel: +44 1534 822 474 / Email: emma.german@careyolsen.com

Emma is a senior associate in the Carey Olsen Jersey digital assets team and has advised in relation to a number of blockchain- and digital asset-related matters including in relation to: the establishment of virtual currency exchanges and security token exchanges; the use of Jersey vehicles for token issuances; and digital company administration in Jersey. Emma has a keen interest in blockchain and the adoption of fintech solutions in Jersey. Emma has a background in international corporate and finance transactions and her expertise includes the raising of finance through the issuance and listing of Eurobonds and other securities on The International Stock Exchange and looks forward to listing digital representations of securities in the coming years.
Emma is an advocate of the Royal Court of Jersey. She is a barrister of England and Wales (non-practising) and an English solicitor. She was educated at King's College, London University. Emma joined Carey Olsen in 2005. In 2016, she was seconded to The Royal Bank of Scotland International Limited.

Holly Brown
Tel: +44 1534 822 231 / Email: holly.brown@careyolsen.com

Holly is an associate in Carey Olsen's corporate department. She is a member of the digital assets team and has assisted with various matters related to cryptocurrencies/digital assets and blockchain, including the launch of Binance's Jersey exchange platform. Holly also advises on the raising of finance by issuers and the listing of Eurobonds and other securities on The International Stock Exchange ("TISE") (formerly the Channel Islands Securities Exchange), having completed a secondment at TISE. She is now excited to advise on the listing of digital representations of securities.
Holly is an advocate of the Royal Court of Jersey. She was educated at King's College, London University. Holly joined Carey Olsen in 2013.

Carey Olsen Jersey LLP

47 Esplanade, St Helier, Jersey JE1 0BD, Channel Islands
Tel: +44 1534 888 900 / Fax: +44 1534 887 744 / URL: www.careyolsen.com

Korea

Jung Min Lee, Samuel Yim & Joon Young Kim
Kim & Chang

Government attitude and definition

There is no statute or guidance from the Korean regulatory authorities that provides a coherent insight on how cryptocurrencies would be classified under Korean law. The Financial Supervisory Service (the "FSS") issued a press release on June 23, 2017 where it announced its views on what cryptocurrencies are *not* from a financial regulatory perspective. Namely, the FSS's position was that cryptocurrencies are not considered: (i) fiat currencies; (ii) prepaid electronic means or electronic currencies; or (iii) financial investment instruments. Unfortunately, the FSS press release did not provide any guidance on how cryptocurrencies *are* classified and in what legal form.

However, the Supreme Court of Korea ruled on May 30, 2018 that cryptocurrencies can be confiscated as criminal proceeds. This decision represents the first time the Supreme Court recognised cryptocurrency as property. However, given the narrow scope of its interpretation, it is unclear what impact this ruling will have on subsequent cryptocurrency regulations in Korea.

The classification of cryptocurrencies from a legal perspective has just begun in Korea and will likely develop in the near future. Other Korean regulatory authorities may have a different view from the FSS's announcement and the legal classification of cryptocurrencies. As a result, there is currently no law or clear guidance from any regulatory authority in Korea that provides clarity on the legal issues relating to cryptocurrencies and how they will be treated under Korean law.

Based on recent events, the Korean government has shown a mixed view on its attitude toward cryptocurrencies. Set forth below are key announcements by the Korean government regarding cryptocurrency.

Margin trading

On September 1, 2017, the Financial Services Commission (the "FSC") banned individuals from borrowing funds or cryptocurrency from cryptocurrency exchanges in order to sell them. The FSC declared that such practice violated existing Korean lending/credit laws. The FSC also directed financial institutions to halt all transactions and partnerships that enabled these practices.

ICO ban

On September 4, 2017, the FSC issued a press release banning initial coin offerings ("ICOs") that violate the Financial Investment Services and Capital Markets Act (the "FSCMA"), the main securities law in Korea. However, this press release did not explain how and in what context ICOs would be a violation of the FSCMA. The financial regulators' initial position was to penalise ICOs where the tokens are offered in the form of a securities issuance (i.e.,

the token is classified as a security). Thereafter, on September 29, 2017, the financial regulators announced through a press release that any type of ICOs, including those in the form of securities, would be prohibited.

If coins or tokens are classified as "securities" under the FSCMA, ICOs or token offerings will be subject to the offering restrictions in Korea under the FSCMA. Where the coins or tokens are not classified as "securities" under the FSCMA, though there are no legal grounds for the prohibition and/or enforcement unless there is a violation of existing Korean laws and regulations, there is a possibility that Korean regulators could challenge the legality of the ICO or token offering based on this press release.

More recently, the FSS issued a press release on January 31, 2019 regarding its investigations conducted on 22 different ICOs from September to November 2018 and its plan to notify the Prosecutors' Office of any illegal activities involved in such ICOs.

Real name verification

On September 4, 2017, the FSC announced it would initiate an identification policy for accounts in cryptocurrency exchanges that required cross-checking usernames and account numbers. Accordingly, a "Real Name Verification System" was introduced from January 30, 2018. Under this system, existing anonymous account users can only withdraw money and not make any further deposits. All new users would have to provide actual identification information to open cryptocurrency accounts.

Central bank-backed cryptocurrency

On January 9, 2018, the Bank of Korea (the "BOK") launched a task force on cryptocurrency and is reviewing a central bank-backed cryptocurrency as part of the project. In addition, various local governments in Korea are exploring the option of issuing their own cryptocurrency.

Cryptocurrency regulation

There is no existing regulatory regime or statute that specifically regulates cryptocurrency. However, the Korean regulators are likely to apply and/or enforce the existing Korean laws and regulations for cryptocurrencies.

Existing laws

For example, in an ICO, if tokens are classified as "securities" under Korean law, the tokens will then be subject to the offering restrictions in Korea under the FSCMA. Or, even if the tokens are not classified as securities, if the marketing of the tokens in an ICO raises funds from the public with a promise to return the original investment amount, or an amount exceeding such investment in the future, the ICO could be regulated by the Act on the Regulation of Conducting Fundraising Business without Permission.

Pending bills

Currently, there are several cryptocurrency bills proposed at the National Assembly. These bills generally cover, among others, licensing requirements for cryptocurrency businesses, anti-money laundering requirements, consumer protection, cybersecurity requirements for cryptocurrency exchanges, and damage compensation for consumer losses. It is unclear when or if these pending bills, in their current form, will be enacted into law in Korea.

Sales regulation

As explained above, if tokens are classified as "securities", the tokens will be subject to the offering or sales restrictions in Korea under the FSCMA. Whether a token will be classified

as a security will depend on the facts and circumstances of the offering of the tokens. Under the FSCMA, an offer or sale of securities (tokens) to 50 or more non-accredited investors (excluding professional investors) would be regarded as a public offering and be subject to offering restrictions under the FSCMA. However, even if such an offer and sale is made to fewer than 50 investors, it may still be deemed a public offer for the purposes of the FSCMA where the securities may be transferred to more than 50 investors within one year from the issuance. In a public offering of securities (tokens) in Korea, an onshore or offshore issuer must file a securities registration statement for the securities (tokens) to be offered in Korea with the FSC.

However, cryptocurrencies such as Bitcoin have not been classified as securities at this time, and have not been subject to the FSCMA. Also, cryptocurrencies are not yet explicitly subject to the commodities laws in Korea. Therefore, it is unclear which laws would regulate the sale of Bitcoin or other tokens since there has not been any application of Korean laws thus far to the sale of Bitcoin or other tokens.

Taxation

The Ministry of Strategy and Finance has announced that plans for the taxation of cryptocurrency are being developed but no decisions have been made. Meanwhile, the National Tax Service (the "NTS") published its preliminary assessment of taxation on cryptocurrency after its 2017 annual forum. This assessment is not official policy but is the only published position/research on cryptocurrency taxation by the Korean government.

NTS Preliminary Assessment on Cryptocurrency Tax

Type	Rate	Assessment
Corporate Income Tax	11%–27.5%	Taxable under current law
Corporate or Individual VAT	10%	Undecided
Income Tax	6.6%–46.2%	Taxable under current law
Capital Gains Tax	6.6%–46.2%	Undecided, but for retail investors, levying Capital Gains Tax is advisable
Inheritance and Gift Tax	10%–50%	Taxable under current law

Money transmission laws and anti-money laundering requirements

Cryptocurrency exchanges are not subject to Korea's anti-money requirements under the Act on Reporting and Use of Certain Financial Transaction Information (the "AML Act"). There is, as discussed above, a pending bill at the National Assembly that would require anti-money laundering obligations for cryptocurrency exchanges under the AML Act. Currently, anti-money laundering obligations of cryptocurrencies are enforced through financial institutions linked with cryptocurrency exchanges.

From January 30, 2018, financial institutions doing business with companies that handle cryptocurrencies (e.g., cryptocurrency exchanges) must comply with the Anti-Money Laundering Guidelines for Cryptocurrencies, as amended (the "AML Guidelines"), issued by the Korea Financial Intelligence Unit. The notable requirements in the AML Guidelines are as follows:

1. Real-name verification required for fiat withdrawal from and deposit to cryptocurrency exchanges

   Fiat withdrawals from and deposits to a cryptocurrency exchange are available only if the exchange user's bank account is verified under the Real Name Verification System provided by financial institutions (e.g., banks), as explained above. Financial institutions may decline transactions with cryptocurrency exchanges that do not comply with this requirement. It also bans minors under the age of 18 and foreigners from opening new cryptocurrency accounts.

2. Customer due diligence

   Financial institutions must implement a due diligence process to confirm whether any of their customers is a cryptocurrency exchange. Financial institutions must verify certain additional information enumerated in the AML Guidelines by conducting due diligence of the cryptocurrency exchange at least every six months.

   Examples of such additional information include whether the cryptocurrency exchange: (i) checks the identity of its users; (ii) maintains a separate transaction record for each user; and (iii) is in compliance with the cryptocurrency-related policies issued by the government.

3. Suspicious transaction reports

   If there is a transaction which falls under the suspicious transaction types, financial institutions must review and file a suspicious transaction report. Financial institutions must also appoint a staff member dedicated to monitoring suspicious cryptocurrency transactions. Suspicious transaction types include: (i) financial transactions between cryptocurrency exchanges and corporate entities or organisations; (ii) if the amount of financial transactions between a cryptocurrency exchange and a single user is KRW 10 million or more within one day or KRW 20 million or more within a seven-day period; and (iii) if the number of financial transactions between a cryptocurrency exchange and a single user is five times or more within a day, or seven times or more within a seven-day period.

Promotion and testing

The Korean government conceptually differentiates cryptocurrency from blockchain technology. While some regulations to curb speculative investment in cryptocurrency have been introduced, the Korean government has highlighted the innovative nature of blockchain technology in many different industries. The Korean government has also expressed its interest in fostering, promoting, and investing in blockchain technology as part of its strategic and economic plans for Korea to be a leader in the 4th Industrial Revolution.

Ownership and licensing requirements

Fund managers

Though there is no specific law that prohibits the registration of cryptocurrency-related investment funds, it is unclear whether the Korean financial regulators will be receptive to cryptocurrency-related investment funds. As a result, currently, there are no cryptocurrency-based investment vehicles and funds registered with the Korean financial regulatory agencies.

Investment advisors

Investment advisors need to be licensed in Korea to provide investment advice on financial

investment products. Nevertheless, since the financial regulatory agencies have announced the position that cryptocurrencies are not financial investment products, there are currently no licensing requirements for investment advisors on cryptocurrency investments.

Licensing requirements

Korean financial authorities have taken the position that as cryptocurrency (or a cryptocurrency asset) is not a financial investment product, financial institutions (including fund managers and investment advisors) licensed under FSCMA may not invest in cryptocurrencies. If such regulatory position becomes law, a cryptocurrency investment fund is unlikely to require a licence from the FSC under the FSCMA. However, the current regulatory perspective by the Korean regulatory agencies on such characterisation of cryptocurrency assets may change, or other agencies may announce contradicting views. Or, there may be court decisions that are contrary to the current views by the Korean regulatory agencies.

Mining

There are no explicit laws and regulations that regulate "mining" of bitcoins or other cryptocurrencies in issued a press release Korea. However, based on an actual case in Korea, it is illegal for mining companies to move in and mine at industrial complexes to take advantage of discounted electricity fees for certain manufacturing companies.

Border restrictions and declaration

There are no explicit border restrictions or obligation to declare cryptocurrency holdings. However, for fiat currencies, remittance of funds out of Korea to an overseas account is governed under the Foreign Exchange Transaction Act (the "FETA") and the Foreign Exchange Transactions Regulations. As a general principle under the FETA, there must be a "legal basis" (e.g., loan repayment, dividend payments, sale proceeds payment, etc.) along with supporting documents as prescribed under the FETA to repatriate funds overseas. The FETA prescribes certain procedures and documents for each type of transaction listed in the FETA for both the remitter of funds and the bank handling the remittance. Each type of transaction has different procedures and requirements to remit funds overseas.

Nonetheless, there are no guidelines under the FETA for cryptocurrency transactions. As a result, it is not permitted to remit fiat currency funds from cryptocurrency transactions overseas. Generally, any person engaging in a cross-border capital transaction must file a foreign exchange report under the FETA with, and obtain approval from, the BOK or a designated foreign exchange bank for all remittances exceeding the limit of US$ 3,000 per transaction, or a yearly aggregate limit of US$ 50,000 from Korea to other countries. In practice, however, Korean banks have declined to process wire transfers overseas when they are related to cryptocurrency trading, even if the amounts do not exceed the monetary limits and would not trigger reporting requirements to the BOK/designated foreign exchange bank.

Reporting requirements

No. There are no explicit laws and regulations for cryptocurrency payments. For overseas payments using cryptocurrencies, there are no reporting requirements at this time to any Korean regulatory agency. However, there are requirements being developed by the Korean financial regulators that may include a filing requirement with the BOK for foreign exchange purposes.

Estate planning and testamentary succession

As discussed in the Taxation section above, cryptocurrency is taxable under current Korean law for inheritance and gift tax. The tax rate would be 10%–50%. The NTS, however, has indicated the need to develop accounting standards for cryptocurrencies to further develop their taxation.

Jung Min Lee
Tel: +82 2 3703 1671 / Email: jungmin.lee@kimchang.com

Mr Lee is the head of the FinTech group at Kim & Chang. With expansive experience in areas spanning E-Finance & FinTech, blockchain and cryptocurrency, privacy and data security, banking, and finance disputes, he has acted for various private and public clients on the most cutting edge FinTech matters in the market.

As one of the leading experts in the field, Mr Lee has served on a number of government committees including the Legal Interpretation Committee Board (Korea Ministry of Government Legislation) and the Task Force on P2P Loan Plan of the Financial Services Commission. He is trusted by the Korean government to advise on key FinTech-related issues and to develop and implement key government initiatives in the field.

Samuel Yim
Tel: +82 2 3703 1543 / Email: samuel.yim@kimchang.com

Mr Yim is a senior foreign attorney in Kim & Chang's FinTech group and his practice focuses primarily on blockchain and cryptocurrency matters. He regularly represents token sellers, cryptocurrency exchanges, venture, hedge and private equity funds and their portfolio companies, token marketers and broker-dealers, funds interested in trading digital assets, major global investment banks, financial institutions and asset managers, and others in the space.

He has advised foreign and domestic clients on major industry-defining matters such as, among others, ICOs and reverse ICOs, token private placements, listing Bitcoin ETFs on the Korean stock exchange, gaming licences for decentralised apps, establishing or acquiring cryptocurrency exchanges, cryptocurrency arbitrage, and establishing cryptocurrency not-for-profit foundations.

Joon Young Kim
Tel: +82 2 3703 1824 / Email: joonyoung.kim@kimchang.com

Mr Kim is one of the key members of the FinTech practice group at the firm. In addition to E-Finance & FinTech, his practice focuses on insurance, non-bank financial companies, corporate governance, mergers & acquisitions and foreign direct investment. He has a strong reputation in the area and is praised by clients for his expertise and knowledge. Mr Kim regularly advises clients on legal issues relating to the latest innovations and technology such as blockchain technology, cryptocurrency and cloud computing.

As one of the leading experts in the field, Mr Kim has been actively involved in publishing on various Korean and international journals and conducting lectures related to E-Finance & FinTech, blockchain technology and cryptocurrency. Mr Kim has served as an external expert member of the Financial Dispute Settlement Committee of Financial Supervisory Service.

Kim & Chang

39, Sajik-ro 8-gil, Jongno-gu, Seoul 03170, Korea
Tel: +82 2 3703 1114 / URL: www.kimchang.com

Liechtenstein

Dr Ralph Wanger
BATLINER WANGER BATLINER Attorneys at Law Ltd.

Government attitude and definition

The Liechtenstein Government is very open to financial innovation and consequently also to cryptocurrencies. To demonstrate this, in 2016 the Government founded a working group that has developed a draft "Blockchain Act" over recent months. It is apparent that the new law aims to offer the best-possible conditions for a token economy as an expression of trustworthy financial technologies. In this regard, the law is not limited merely to cryptocurrencies, but instead covers any possible tokenisation of assets as well as further innovations that go beyond blockchain technology. Within this context, the Liechtenstein Government is keen to create fertile conditions for cryptocurrencies as well as associated token generation events ("TGEs").

As in Austria and Switzerland, Liechtenstein defines money and monetary assets to mean not just legal tender (bank notes as well as coins in the respective currency), but also book-entry money. This legal definition of money does not cover cryptocurrencies, though.

Last year, however, following the amendment of the Liechtenstein Law on Professional Due Diligence to Combat Money Laundering, Organised Crime and Terrorist Financing (*Gesetz über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismus-finanzierung*, Due Diligence Act – "*Sorgfaltspflichtgesetz*", "SPG", LGBl. 2017/161), Liechtenstein lawmakers attempted for the first time to formulate a legal definition of virtual currencies. Pursuant to Art. 2 Para. 1 lit. l SPG, virtual currencies (e.g. Bitcoin) are deemed to be digital monetary units that can be exchanged for legal tender, used to obtain goods or services or to store assets, meaning that they can assume the function of legal tender. As a consequence, this excludes those virtual currencies that can be redeemed or used to obtain goods or services only to a limited extent (e.g. bonus programmes). Against this backdrop, it is also clear that legal tender and cryptocurrencies are not to be treated equally, even though they serve the same purposes.

By contrast, the Liechtenstein Financial Market Authority (hereinafter called "FMA"), views cryptocurrencies essentially as "commodities", whereby other classifications may also be used, depending on the configuration of the token representing the cryptocurrency.

At the current time there are no cryptocurrencies that are supported or backed by the Government or a bank in Liechtenstein.

In the beginning of June 2019, the so-called "Liechtenstein Token and Trusted Technologies Law" or "Token Act" was deliberated by the Parliament in a first session. This law is supposed to come into force on 1 January 2020. This law is the basis for a comprehensive token economy in Liechtenstein. The law serves the efforts of the government to make Liechtenstein an interesting FinTech location.

Cryptocurrency regulation

Insofar as cryptocurrencies exclusively fulfil a payment function or are issued and used solely as a payment token, they are deemed to be commodities and are accordingly not regulated. However, as soon as additional functions are included, tokens may represent financial instruments that are covered by financial market law and can accordingly trigger FMA supervision as well as a corresponding licensing obligation (FMA Factsheet on the Initial Coin Offering of 10 September 2017, https://www.fma-li.li/files/fma/fma-faktenblatt-ico.pdf). This may, for example, include tokens that exhibit features of equity securities or have an investment character (e.g. security, asset or equity-backed tokens). Activities relating to financial instruments are generally subject to a special statutory licensing obligation by the FMA and may therefore be subject to the prospectus requirement.

This means that a special statutory licensing obligation may exist on a case-by-case basis, depending on the configuration of the specific business model (FMA Factsheet on Virtual Currencies of 16 February 2018, https://www.fma-li.li/files/fma/fma-faktenblatt-virtuelle-waehrungen.pdf). For this reason, it is necessary to clarify on an individual basis which licensing obligations need to be adhered to for each business model. The relevant criteria in each case are the specific configuration and the effective function of the token. At any rate, there is no general ban on cryptocurrencies.

As soon as the new Token Act comes into force at the beginning of 2020, certain blockchain service providers will be subject to registration. There will also be regulations on the publication of base information by ICOs. Furthermore, cryptocurrencies as tokens will be regulated by the fact that the law defines what a token is and how it can be disposed of.

Sales regulation

On the basis of the above assumption, tokens that are classified purely as a means of payment are not covered by the scope of statutory capital market provisions. This consequently means that, in general terms, the use of virtual currencies as a means of payment is not subject to any special statutory licensing obligation for the time being (FMA Factsheet on Virtual Currencies of 16 February 2018, https://www.fma-li.li/files/fma/fma-faktenblatt-virtuelle-waehrungen.pdf). After the entry into force of the new Token Act, any token issuer has to apply for a regulation with the FMA and must comply with disclosure regulations. However, for the time being the purchase or sale of cryptocurrencies is thus equivalent to a commercial transaction in goods and is covered by the General Civil Code (*Allgemeines Bürgerliches Gesetzbuch* – "ABGB") that is applicable in Liechtenstein.

Taxation

In Liechtenstein, the tax treatment of cryptocurrencies is such that every natural person subject to unlimited tax liability must declare their holdings of cryptocurrencies at the beginning of the respective tax year and convert them into Swiss francs (like foreign exchange). At the same time, speculative profits arising out of trade in cryptocurrencies are tax-exempt and do not need to be declared.

With regard to legal entities, changes in value realised through investments in cryptocurrencies must be declared for tax purposes. This consequently means that investments in cryptocurrencies are not covered by the tax exemptions provided by Art. 48 of the Liechtenstein Tax Act (*Steuergesetz* – "SteG"). In addition to the income tax rate of

12.5%, the effective tax amount also depends on the deductible equity interest rate, which reduces the assessment basis for income tax.

The equity interest deduction is calculated on the modified equity, whereby the interest rate is redefined annually and currently amounts to 4%. Insofar as the corporate purpose also includes the holding of cryptocurrencies and the investment in cryptocurrencies falls under the operating assets, the corresponding investment is subject to the equity interest deduction and thus leads to a reduction in the effective tax burden.

Money transmission laws and anti-money laundering requirements

In Liechtenstein, subjection to the Due Diligence Act (*Sorgfaltspflichtgesetz* – "SPG") focuses on financial intermediaries. In the absence of a connection of this nature, there is essentially no subordination to the Due Diligence Act. On a case-by-case basis, however, the Due Diligence Act may indeed be applicable. For this reason, individual clarification by the FMA in respect of a possible due diligence obligation is recommended (FMA Factsheet on Virtual Currencies of 16 February 2018, https://www.fma-li.li/files/fma/fma-faktenblatt-virtuelle-waehrungen.pdf).

An obligation to report to the FMA as a person subject to due diligence may arise, for example, if a commercial exchange from fiat funds to cryptocurrencies is performed. Against the backdrop of the current Liechtenstein legal situation, the corresponding activity would have to be qualified as a currency exchange activity and would accordingly open up the scope of application of the Due Diligence Act. On the other hand, from a technical legal perspective, trade between cryptocurrencies is viewed as a normal exchange within the meaning of §§ 1045 *et seq*. ABGB, meaning that this is essentially not subject to the Due Diligence Act.

In principle, however, it is important to note that compliance with Anti Money Laundering Guidelines ("AML") and the Know-Your-Customer Principle ("KYC") is recommended in any case for reasons of practicability, as this facilitates cooperation with the financial institutions involved or is generally required by them. This means it is therefore advisable, within the context of a planned TGE, to discuss this in advance with the financial institution involved, in order to compare requirements in the AML/KYC field with the existing in-house guidelines that are confidently deemed to be sufficient on account of the fact that the financial institution is subject to the Due Diligence Act.

As soon as the Token Act has come into force, certain blockchain service providers will be subject to the due diligence regime – even if the business is not directly connected with financial services or financial intermediaries.

Promotion and testing

On account of the large number of enquiries received in the FinTech field relative to the small size of the country (98 enquiries in 2018 up to 28 June), the FMA has established a dedicated unit called "Regulatory Laboratory/Financial Innovation" that collects know-how in this field, and also aims to promote these topics by organising corresponding workshops. All enquiries in the blockchain technology field (incl. ICOs) should be addressed to this unit.

Ownership and licensing requirements

There is currently no special law in Liechtenstein that would impose restrictions or supervisory obligations on investment advisors or fund managers when investing in

cryptocurrencies. It would, however, be necessary to assess on a case-by-case basis whether the holding of cryptocurrencies by the corresponding professional groups might be subsumed under one of the classic statutory capital market laws. In particular, the Asset Management Act (*Gesetz über die Vermögensverwaltung*/*Vermögensverwaltungsgesetz*, "VVG") would need to be taken into account.

As already stated, this will change with the upcoming Token Act that should come into force in the beginning of 2020.

Mining

The production of virtual currencies as a means of payment (so-called "mining") is not currently subject to any specific statutory licensing obligation (FMA Factsheet on Virtual Currencies of 16 February 2018, https://www.fma-li.li/files/fma/fma-faktenblatt-virtuelle-waehrungen.pdf). This means the mining of Bitcoin or other cryptocurrencies is permitted.

In February 2018, the Liechtenstein Tax Administration agreed that mining is regarded as a taxable gainful activity. This consequently means that mining is subject to income tax, whereby the associated overheads (e.g. IT costs, rent of business premises, etc.) are tax-deductible.

Border restrictions and declaration

As Liechtenstein forms a customs and currency union with Switzerland, reference may be made to the relevant passages in the Swiss chapter.

Reporting requirements

From a statutory supervisory perspective, as far as the authors are currently aware, there are no value-related limits that would entail a reporting obligation.

Estate planning and testamentary succession

Due to the novelty of cryptocurrencies as a heritable asset, it has yet to be clarified how to proceed with a testamentary disposition of virtual currencies. Practical and legal problems arise, for example, with regard to the associated private keys, since their availability at the time of inheritance is a key prerequisite for the transfer of ownership within the context of legal succession under inheritance law. The storage of cryptocurrencies (cold/warm storage) or the corresponding keys as access codes will therefore play a crucial role when it comes to the transfer of virtual assets across generations. The Token Act, which is currently going through the process of consultation, will also address this issue and provide for corresponding regulations to establish the necessary legal certainty.

Dr Ralph Wanger
Tel: +423 239 78 78 / Email: ralph.wanger@bwb.li

Dr Ralph Wanger, LL.M., CAS Blockchain, Attorney-at-Law, born 1969, Liechtenstein citizen.

He graduated in law from the University of Zurich (*lic. iur.*) in 1994. He completed his doctorate (*Dr. iur.*) at the University of Zurich in 1997. He passed the bar exam in 1999. Two years later, he completed post-graduate studies at New York University, School of Law, with a Master in Comparative Jurisprudence (LL.M.).

Having completed his studies, he performed various internships at the Princely Court of Justice, at the Princely Government as well as in the fiduciary field, and worked at a Liechtenstein law firm.

He began working as a self-employed attorney-at-law in 2000. In 2002, he joined and was made a partner at BATLINER WANGER BATLINER Attorneys at Law, which was converted into a stock corporation in 2008. He has been a member of the Board of Directors ever since.

From 2005 to 2015, he acted as a Substitute Judge at the Constitutional Court of the Principality of Liechtenstein.

Dr Ralph Wanger is currently focusing on the topic of blockchain, and has taken part in the (Swiss) CAS Blockchain programme at the University of Lucerne. In the meantime, he is a lecturer at the University of Lucerne as well as at the University of Liechtenstein with regard to Distributed Ledger Technology (DLT) and Liechtenstein law. In addition, Dr Ralph Wanger is also a founder and member of the Board of Directors of the company Blockstar AG (www.blockstar.li). He is head of the FinTech Department at BWB and advises clients in the DLT and ICO fields.

BATLINER WANGER BATLINER Attorneys at Law Ltd.

Am Schrägen Weg 2, LI-9490 Vaduz, Liechtenstein
Tel: +423 239 78 78 / URL: www.bwb.li

Malta

Malcolm Falzon & Alexia Valenzia
Camilleri Preziosi Advocates

Government attitude and definition

Following the much-anticipated promulgation of Distributed Ledger Technology ("**DLT**")-related laws during 2018, Malta has continued to establish itself as a key player in the cryptocurrency and blockchain sphere.

The Government of Malta, local regulators and other stakeholders have adopted an open and collaborative approach towards this sphere, rooted in striking the right balance between maintaining Malta's perception as a jurisdiction of repute, integrity and financial stability, and the desire to foster a business and legal environment conducive of innovative technologies, products and services.

The successful completion of the Digital Innovation Framework (see below) arose as a result of Malta's clear determination to promulgate regulation that is the first of its kind. A collective effort, spearheaded by the Parliamentary Secretariat for Financial Services, Digital Economy and Innovation together with the Malta Financial Services Authority (the "**MFSA**"), has enabled Malta to carry out the necessary reforms to formulate an innovative yet robust regulatory and legal framework designed to meet the commercial, technical and technological peculiarities inherently characterising blockchain technology and cryptocurrencies. The Government of Malta has led by example and has expressly stated that it is resolute in fulfilling Malta's roadmap to becoming the "Blockchain Island". To this end, it has set up a number of blockchain-related innovative projects with the intention of attracting big industry players to the island (see "Promotion and testing", below).

Following a series of public consultations with the industry throughout the course of 2018, the willingness of the Government of Malta to digitalise Malta's economy and cement its position as a jurisdiction of choice for innovators has culminated in the formal enactment of a comprehensive set of three complementary legislative acts at the beginning of July 2018. These acts are:

(i) the Malta Digital Innovation Authority Act (the "**MDIA**");

(ii) the Innovative Technology Arrangements and Services Act (the "**ITAS**"); and

(iii) the Virtual Financial Assets Act (the "**VFAA**"),

(collectively hereinafter referred to as the "**Digital Innovation Framework**").

In essence, this means that market participants in the blockchain and cryptocurrencies industries may establish or operate in or from Malta, and benefit from a higher degree of legal certainty – which will have a knock-on beneficial impact through enhanced trust, marketability, legal certainty and consumer adoption.

Cryptocurrency treatment in Malta

Cryptocurrency is not treated as "money" in Malta. As will be explained in greater detail in the next question below, Malta's Digital Innovation Framework sets out four possible categories of cryptocurrencies, and more generally Distributed Ledger Technology Assets ("**DLT Assets**"). These are:

(i) Electronic Money (albeit that are intrinsically dependent on, or utilise, Distributed Ledger Technology);

(ii) Financial Instruments (albeit that are intrinsically dependent on, or utilise, Distributed Ledger Technology);

(iii) Virtual Tokens (more commonly referred to as Utility Tokens); or

(iv) Virtual Financial Assets ("**VFAs**")

The classification of the DLT Asset in question into one of the four categories listed above will be mutually exclusive.

Cryptocurrency backing by the government/central bank

As at the date of writing, there are no cryptocurrencies that are backed by the Government of Malta or the Central Bank of Malta. On a more general note, cryptocurrency is not treated as money or given equal recognition with domestic or foreign fiat currency in Malta.

Cryptocurrency regulation

Following the enactment of the VFAA, cryptocurrencies may be regulated under the VFAA or existing financial services legislation, including but not limited to the Markets in Financial Instruments Directive II ("**MiFID II**"), the Investment Services Act (Chapter 370 of the Laws of Malta) (the "**ISA**") and the Financial Institutions Act (Chapter 376 of the Laws of Malta). Which regulatory regime (if any) will apply is dependent on the classification of the asset in question.

As indicated above, Malta's Digital Innovation Framework sets out four possible categories of DLT Assets, which may include cryptocurrencies.

The VFAA introduces a mandatory regulatory regime that regulates DLT assets and related service providers, including, amongst others, Initial Virtual Financial Asset Offerings ("**IVFAOs**") issuers (more commonly known as ICOs), and Virtual Financial Asset Exchanges ("**VFA Exchanges**") (more commonly referred to as Crypto-Exchanges). The VFAA also introduces a new class of intermediaries, to be known as Virtual Financial Asset Agents ("**VFA Agents**"). VFA Agents act as gate-keepers to the MFSA, wherein they are tasked with performing a number of regulatory checks on the prospective IVFAO issue and VFA Exchanges. To this end, the MFSA, being the applicable regulatory authority in this regard, has registered nine Virtual Financial Asset Agents ("**VFA Agents**") and is, at the time of writing, assessing at least nine other VFA Agent applications.

The crux of the matter is determining whether the asset in question falls within the scope of the VFAA and is therefore prone to being regulated thereunder. In this respect, the MFSA has introduced a test, known as the Financial Instrument Test (the "**Test**"), for the purpose of classifying a DLT Asset as one of the aforementioned classes of DLT Assets and thereby determining whether the DLT Asset would be regulated under the VFAA, existing financial services laws or neither of the two (remaining unregulated). The Test was published in July 2018 along with a guidance note on how to interpret and apply its steps. The Test must be carried out on a case-by-case basis. The VFAA indicates that it will be the task of the VFA

Agent (along with the VFA issuer if the Test is being carried out in relation to an IVFAO) to carry out this assessment with respect to a DLT Asset when:

(i) an issuer intends to launch an IVFAO to the public in or from within Malta;

(ii) an issuer admits the VFA to trading; and/or

(iii) a service provider intends to conduct VFA-related services.

The Test will firstly determine whether the DLT Asset is to be classified as a Virtual Token and therefore fall outside the scope of regulation. A Virtual Token is defined as being a form of digital medium recordation whose utility, value or application is restricted solely to the acquisition of goods or services, either solely within the DLT platform on, or in relation to which, it was issued or within a limited network of DLT platforms (but not DLT exchanges).

If the DLT Asset is determined not to be a Virtual Token, one must move on to the second stage of the Test wherein it will be determined whether the DLT Asset falls within the scope of existing financial services legislation. If the VFA Agent determines that the DLT Asset does indeed fall within the scope of existing financial services legislation, then the issuer or service provider in question would be required to comply with the regulatory regime applicable to financial instruments or electronic money, depending on the characteristics of the asset. On the other hand, if it is determined that the DLT Asset does not fall within the scope of existing financial services laws (or would be considered a Utility Token as aforesaid), the token automatically falls into the last stage of the Test, whereby the token would be deemed to be a VFA and therefore due to be regulated by the VFAA.

If a DLT Asset is determined to be a VFA, VFA-related service providers will be required to adhere to the provisions of the VFAA. For example, an issuer of an IVFAO offered to the public in or from Malta must register its white paper with the MFSA, and the white paper must comply with the conditions set out in the First Schedule of the VFAA. Furthermore, a VFA service provider as listed in the Second Schedule of the VFAA (such as VFA exchanges) offering a VFA service in or from Malta will be required to obtain a licence from the MFSA before it may commence its operations.

Sales regulation

The sale of cryptocurrencies such as Bitcoin or other tokens may be regulated by securities laws. In order to determine whether the sale of tokens would be regulated by securities laws, according to the VFAA each DLT Asset must be assessed to determine whether the said DLT Asset falls within the scope of (i) existing securities laws, or (ii) the VFAA, or be unregulated. Should the DLT Asset fall within the scope of existing securities laws by virtue of it being classified as a Financial Instrument following completion of the Test, then that token must comply with securities laws.

There are no commodities laws regulating the sale of cryptocurrencies or other tokens as at the date of writing.

Taxation

In November 2018, the Commissioner for Revenue (the "**CfR**") issued three guidelines on the treatment of DLT transactions from a taxation perspective (collectively referred to as the "**Guidelines**"). The Guidelines provide guidance on the application of the Income Tax Act (Chapter 123 of the Laws of Malta), the Value Added Tax Act (Chapter 406 of the Laws of Malta) (the "**VAT Act**") and the Duty on Documents and Transfers Act (Chapter 364 of the Laws of Malta) (the "**DDTA**") respectively to DLT transactions. The Guidelines are in their preliminary stages and are subject to change.

The Guidelines distinguish between Coins and Tokens, with Tokens being further divided into two sub-categories: Financial Tokens and Utility Tokens. In instances where a Token has the features of both Financial and Utility Tokens, such Tokens are referred to as Hybrid Tokens.

Coins are defined as those assets utilising DLT that are designed to be used as a means of payment, medium of exchange and a store of value and do not have any of the characteristics of a security. They represent the cryptographic equivalent of fiat currencies.

Financial Tokens are defined as those assets utilising DLT which exhibit qualities that are similar to equities, debentures, units in collective investment schemes, or derivatives, including financial instruments. Conversely, Utility Tokens are those assets utilising DLT whose utility, value or application is restricted solely to the acquisition of goods or services either within the DLT platform on which they are issued or within a limited network of DLT platforms.

The CfR made it clear that it is the purpose and context of the Coins and Tokens which will determine their taxation. Furthermore, general tax principles apply to the transactions involving Coins and Tokens and each transaction must be analysed in the same manner as any other transaction, provided that due regard is being given to the following issues:

(i) the nature of the activities;

(ii) the status of the parties; and

(iii) the specific facts and circumstances of the particular case.

Transactions involving Coins

Below are some important highlights relating to the taxation of transactions involving Coins:

- tax treatment of corresponding transactions involving Coins is regarded to be the same as the tax treatment of transactions involving a fiat currency;
- the profits realised from the business of exchanging Coins are treated similar to the profits derived from the business of exchange of fiat currency;
- proceeds from the sale of Coins held as trading stock in a business are treated as ordinary income;
- gains or profits on revenue account from mining of cryptocurrency also represent income; and
- Coins do not fall within the scope of the taxation of capital gains.

Transactions involving Tokens

The returns derived by the owner of Tokens on his holdings, such as payments equivalent to dividends, interest and premiums, are to be treated as income for the purposes of the Income Tax Act. The tax treatment of a transfer of Tokens will heavily depend on whether the transaction is a trading transaction or a transfer of a capital asset. In the former case, the consideration will be treated as a receipt on revenue account and to the extent that the transfer is made in the ordinary course of business, it shall be taxed as a trading transaction and shall be bound by the ordinary income tax provisions and principles. However, since the trading or non-trading nature of a transaction may not always be clear, the badges of trade tests may need to be used for this purpose. These are indicative tests utilised in order to determine whether a given transaction, or a series of transactions, give rise to income derived from the activity in the nature of a trade or a capital receipt. On the other hand, in relation to the tax treatment of the latter, due attention must be paid to whether such Tokens could meet the definition of "securities" under Article 5 of the Income Tax Act. If the Token falls within

the said definition, the transfer would be taxed according to the provisions on capital gains found therein.

Income tax treatment of ICOs

The proceeds of an initial offering of Financial Tokens will not typically be treated as income of the issuer and the issue of new tokens is not treated as a transfer for the purposes of taxation of capital gains. In an initial offering of Utility Tokens, the gains or profits realised from the provision of the services or the supply of the goods will represent income.

Any tax-relevant value in transactions involving Coins or Tokens will be determined with reference to the market value of the Coins or Tokens, which is deemed to be the rate provided by the relevant Maltese Authority or in lack of this, by reference to the rate at reputable exchanges on the date of the relevant transaction, or any other methodology to the satisfaction of the CfR.

Stamp duty determination

It is important to observe the intrinsic nature and effects of a particular DLT transaction to which the DDTA refers, without regard to the apparent title or form. Consequently, where transfers involve Coins or Tokens that have the same characteristics as "marketable securities" as defined in the DDTA, such transfers shall be subject to duty in accordance with the applicable provisions of the DDTA.

VAT rules applicable to cryptocurrencies

In light of the established case-law of the CJEU (C-264/14 – *Skatteverket vs Hedqvist*), instruments whose purpose is none other than to serve as means of payment accepted by certain operators must, for VAT purposes, be treated like traditional currency used as legal tender, and thus would be taxable unless an exemption applies. The exchange of cryptocurrencies for other cryptocurrencies or for fiat money where such exchange constitutes a supply of services for consideration would likely be covered by said exemptions, though each transaction would need to be considered on a case-by-case basis.

VAT treatment of Tokens

Raising finance through the issuance of Tokens does not trigger VAT implications as this activity does not constitute a supply of goods or provision of services for consideration.

Where a Token issued against consideration carries an obligation to be accepted as consideration or part consideration for a supply of goods or services and where the goods or services to be supplied or the identity of the supplier is known, such token could be treated as a voucher (as defined by the VAT Act). The VAT Act differentiates Simple-Purpose Vouchers ("**SPVs**") and the Multi-Purpose Vouchers ("**MPVs**"). The former is where the underlying good or service, the place of supply and VAT due (if any) are known at the time of issuing the voucher, the consideration with respect to such a voucher would trigger VAT under the terms of 4th Schedule to the VAT Act. Accordingly, consideration payable to a taxable person for the issuance and transfer of an SPV representing taxable supplies of goods or services taking place in Malta would be immediately subject to Maltese VAT in terms of the 4th Schedule to the VAT Act and Part Nine of the 14th Schedule to the VAT Act. With respect to MPVs, the place of supply and VAT due on an underlying good of service is not known at the time of issuance and therefore, VAT, if any, would become due at the time of redemption of the MPV.

VAT treatment of ICOs

Considering that at the time of the initial offering the service or good is not identified, nor is it possible to know if the investors would receive a return, the ICO may not necessarily

constitute a chargeable event for VAT purposes. On the other hand, in the event that the Tokens issued would give rights to identified goods or services for a specified consideration, a chargeable event for VAT purposes could arise.

VAT treatment of digital wallets

Insofar as the digital wallet provider requires fees for allowing Coin users to hold and operate a cryptocurrency and create rights and obligations in relation to the means of payment, and such cryptocurrency qualifies as currency for VAT purposes, such service is exempt without credit. Otherwise, the service could be taxable.

VAT treatment of mining

Mining falls outside the scope of VAT given that there is no link between the compensation received and service rendered. However, other services provided by the miner may still be considered as taxable.

VAT treatment of exchange platforms

The VAT treatment (as taxable or exempt) of trading or exchange platform services would depend on the nature of the service supplied, which would have to be determined on a case-by-case basis.

Money transmission laws and anti-money laundering requirements

Malta's main legislation regulating anti-money laundering and the countering of the funding of terrorism ("**AML/CFT**") are: (i) the Prevention of Money Laundering Act (Chapter 373 of the Laws of Malta) ("**PMLA**"); and (ii) the Prevention of Money Laundering and Funding of Terrorism Regulations (Subsidiary Legislation 373.01) ("**PMLFTR**"). These legislative instruments transpose the requirements of the Fourth Anti-Money Laundering Directive (Directive (EU) 2015/849).

Persons carrying out either a "relevant financial business" or "relevant activity" will be considered to be a subject person under the PMLA and PMLFTR and, therefore, they must adhere to the obligations therein relating to subject persons. In addition, subject persons shall also comply with the Implementing Procedures, and other guidance, as issued and updated from time to time by the AML/CFT regulator in Malta, the Financial Intelligence and Analysis Unit ("**FIAU**").

With specific reference to issuers of cryptocurrencies and related service providers, the VFAA provides that: (i) an issuer; (ii) a VFA licence holder; and (iii) a VFA Agent under the VFAA, shall be considered as a subject person. Finally, in the white paper required to be registered with the MFSA for the purposes of an IVFAO to the public, or the admission thereof on a DLT Exchange, the issuer is required to include a description of the issuer's adopted white-listing and anti-money laundering and counter financing of terrorism procedures in terms of the PMLA and any regulations made and rules issued thereunder. VFA issuers, licence-holders and agents are also required to abide by any sector-specific guidance that may be issued by the FIAU from time to time.

Promotion and testing

MFSA Vision 2021 and Fintech Regulatory Sandbox

The MFSA launched 'Vision 2021' in January 2019. This seeks to both strengthen the position of the MFSA in the realm of innovative financial services and propel Malta's stance as a leader in the global fintech hub. At its inception, Vision 2021 presents six pillars which

the MFSA believes will create a holistic long-term approach to catalyse innovation, growth and competition in the financial services sector, whilst also ensuring robust investor protection, market integrity and financial soundness. These pillars are: (i) regulations; (ii) ecosystem; (iii) architecture; (iv) international links; (v) knowledge; and (vi) security.

As part of its Vision 2021, the MFSA issued a consultation paper on its Fintech Strategy in January 2019 and provided feedback to stakeholders in May 2019. The Fintech Strategy states that the MFSA is proposing to encourage and support financial institutions by setting up incubator and accelerator programmes for start-ups, amongst other initiatives. The Fintech Strategy was met with an overall positive response from participants.

One of the main goals of the MFSA through this project is to create the Fintech Regulatory Sandbox (the "**Sandbox**") which would allow entities to operate in a controlled yet fully functional financial services environment. This regulatory environment would provide innovative products, services and business models with the opportunity to be tested and monitored and allows them to enhance their functional capacity through feedback they would receive from the market and the MFSA.

The Sandbox provides financial services providers with an environment within which to observe the commercial and regulatory viability of their innovative products, services, business models and delivery mechanisms. Moreover, the Sandbox would allow the MFSA to concurrently build its technical capacity while identifying the potential risks for market integrity, consumer protection and regulatory response.

Malta Gaming Authority Sandbox

In March 2018, the Malta Gaming Authority ("**MGA**") released guidance on the use of DLTs and the acceptance of Virtual Currencies ("**VCs**") in the gaming sector through the implementation of a sandbox environment. The first phase of the sandbox commenced on 1 January 2019 and is set to last for a period of 10 months. The principal objective of the MGA's sandbox is to consider allowing the use and implementation of DLTs and VCs by gaming and gambling operators licensed by the MGA.

In order to safeguard players and the gaming ecosystem, either of two distinct implementation scenarios is deemed acceptable:

(i) a "single wallet system"– in the first scenario, the operator has a maximum of one wallet for every supported cryptocurrency. The players issue deposits to the address of that wallet and use their account with the operator to notify that they just made a deposit from a certain wallet's address. If the deposited amount respects the "maximum amount" and any deposit limit previously set by the player, the funds are kept in the operator's wallet and are made available to the player's account for gaming use. Otherwise, if the operator receives a transaction from a player's account without first being notified, the funds are sent back to the originating wallet. In this scenario, the operator does not assign an individual wallet to each player. Instead, every player is assigned ownership of a balance virtually segregated within one of the operator's holding wallets; and

(ii) a "multiple wallet system"– in the second scenario, the operator assigns a gaming wallet for each currency to every player's account. The MGA only accepts this case if the operator has an intermediate wallet structure comprised of one or more wallets. Such an intermediate setup is used to accept deposits from the player's personal external source of funds. However, in contrast to that scenario, if the deposited amount is within the "maximum amount", the funds are forwarded to the player's respective

VC gaming wallet rather than allocating players a share of the operator's wallet. The intermediate wallet reverses incoming transactions if they exceed the "maximum amount" and/or if the funds come from a wallet that is not expected to make a deposit. The player uses the account with the operator to inform of an incoming deposit and get feedback from the operator of the deposit being awaited.

Malta Stock Exchange MSX Fintech Accelerator

In June 2018, the Malta Stock Exchange announced its MSX Fintech Accelerator, an initiative endorsed by Binance and Thomson Reuters, which is an accelerator providing a programme designed to mentor and support start-ups and entrepreneurs in the crypto and blockchain space, matching them with international technology and business leaders.

Other stakeholder initiatives

From a broader perspective, Malta has also experienced a flurry of collaborative activity amongst various stakeholders, with a variety of associations and interest groups being formally established to further the development of the cryptocurrency community in Malta, sharing the common goal of providing a mutual educational and learning experience and fostering a business environment that is conducive to these innovations. Examples include:

- BitMalta;
- the Blockchain Malta Association;
- the Blockchain Research Group, University of Malta; and
- the Malta Information Technology Agency (MITA) – YouStartIT Accelerator.

Finally, in April 2018, Malta joined another 23 European Union Member States in establishing the European Blockchain Partnership ("**EBP**"). The EBP is intended to act as a vehicle for co-operation among 27 EU Member States in terms of exchanging experience and know-how in technical and regulatory fields.

Ownership and licensing requirements

Owning cryptocurrencies for investment management purposes

As set out above, according to the provisions of the VFAA, a licensing requirement is triggered under the VFAA where an entity provides a service set out in the second schedule of the VFAA in relation to a VFA, whether such services are provided in or from within Malta (note that the VFAA does not define the phrase '*in or from within Malta*'; however, we interpret this to mean: (i) the provision of a VFA service by an entity from within Malta; or (ii) the provision of services by an entity to clients in Malta on a cross-border basis).

Investment management is one of the services listed in the second schedule to the VFAA. Accordingly, where such service is provided in respect of VFAs in or from Malta, this would trigger a licensing requirement under the VFAA and such person would be required to obtain a licence under the VFAA to carry out this activity.

It is pertinent to note that according to Subsidiary Legislation 590.01 (Virtual Financial Assets Regulations) ("**SL**"), exemptions are available whereby persons providing VFA services may be exempt from the requirement to obtain a licence. For example, persons dealing on own account in terms of the VFAA and not providing any other VFA service are (subject to limitations) exempt from the requirement to obtain a VFA licence. For the purpose of this exemption, dealing on own account means trading by a person in his own name and against proprietary capital resulting in conclusion of transactions in one or more VFAs.

Licensing requirements for advisors and fund managers

Investment advice

Investment advice is also listed in the second schedule to the VFAA. Accordingly, a licensing requirement would be triggered under the VFAA where such service is provided in relation to one or more VFAs in or from Malta. However, a person providing investment advice under the VFAA in the course of providing another professional activity not covered by the VFAA shall be exempt from VFA licensing, provided that the provision of such advice is not specifically remunerated.

Fund management

As a preliminary matter, please note that, in terms of Maltese law, it is possible for a Maltese domiciled fund to be structured as: (i) a UCITS fund; (ii) an alternative investment fund ("**AIF**"); or (iii) a professional investor fund ("**PIF**"). At the time of writing, Maltese domiciled AIFs and UCITS are not permitted to invest in cryptocurrencies. Therefore, it is currently only possible for Malta-domiciled collective investment schemes to invest in cryptocurrencies when structured as PIFs (which are subset of AIFs available to managers which fall within the *de minimis* thresholds set out in the AIFMD (Directive 2011/61/EU)).

The licensing requirements for the management of a Malta-domiciled PIF will depend on whether the management company is established in or outside Malta.

Fund managers which manage PIFs investing in cryptocurrencies through a management company established in Malta are required to be licensed under the ISA. This notwithstanding, a person licensed to provide the services of management of investments in terms of the ISA to a collective investment scheme or holding an equivalent authorisation issued by a European regulatory authority providing services in Malta in exercise of a European right shall be exempt from having to obtain a VFA licence, provided that such person shall solely be exempt from the provisions of the VFAA for the purposes of providing portfolio management and/or investment advice to a collective investment scheme. Where the exemption applies, such fund manager would not require a separate licence under the VFAA to manage a PIF investing in cryptocurrencies.

Fund managers which manage PIFs investing in cryptocurrencies through a management company established outside Malta are not required to be licensed under the ISA. However, in order for the foreign-based entity to manage the PIF, the MFSA must be satisfied that such management company has the necessary skills, competence and expertise to manage the PIF. A fund manager domiciled overseas which is managing a Malta-domiciled PIF would not require a separate licence under the VFAA.

Mining, border restrictions, reporting requirements and estate planning/ testamentary succession

Other than as set out under 'Taxation' above, cryptocurrency mining activities are, at the time of writing, unregulated.

There are no border restrictions or obligations to declare cryptocurrency holdings, nor any reporting requirements for cryptocurrency payments made in excess of a certain value.

As at the time of writing, there are no laws regulating the treatment of cryptocurrencies for the purposes of estate planning and testamentary succession; general laws such as the relevant provisions found within the Civil Code (Chapter 16 of the Laws of Malta) would apply.

Malcolm Falzon
Tel: +356 2123 8989 / Email: malcolm.falzon@camilleripreziosi.com

Malcolm Falzon is the partner at Camilleri Preziosi responsible for the firm's insurance, gaming and aviation practices. His areas of specialisation also comprise corporate and M&A, capital markets, securitisation, asset finance and pensions. He regularly advises local and international clients on legal, regulatory, operational and licensing matters as well as related corporate and commercial and dispute resolution issues across various industry sectors. Malcolm also leads Camilleri Preziosi's Blockchain Taskforce, which was set up in order to study the technology and its potential application to the industry sectors serviced by the firm. He regularly acts as an examiner at the University of Malta and lecturer at the Malta Stock Exchange Institute and is a speaker at seminars and conferences relating to his areas of expertise. Following his traineeship at the firm and return from postgraduate studies at University College, London, Malcolm returned to the firm as an associate in 2005 and was admitted to partnership in 2013.

Alexia Valenzia
Tel: +356 2123 8989 / Email: alexia.valenzia@camilleripreziosi.com

Alexia forms part of Camilleri Preziosi's Technology, Media and Telecoms department and the firm's Blockchain Taskforce. Her areas of specialisation include fintech regulation, technology, intellectual property and data protection. She often works on DLT-related matters, specifically within the field of cryptocurrencies, initial coin offerings and related services. Her interests lie in the development of nascent technologies such as artificial intelligence and the internet of things, and the legal implications which arise as a result of their development. She frequently contributes to Camilleri Preziosi's publications on the applicability of these technologies to various industry sectors. She also regularly assists clients with data protection and intellectual property-related matters. Alexia graduated from The City Law School in London in 2016 after completing the Graduate Diploma in Law course. Prior to this, Alexia obtained a first-class honours degree in Pharmacology from the University of Portsmouth in 2015.

Camilleri Preziosi Advocates

Level 3, Valletta Buildings, South Street, Valletta, VLT 1103, Malta
Tel: +356 2123 8989 / URL: www.camilleripreziosi.com

Mexico

Miguel Ángel Peralta García, Pedro Said Nader &
Patrick Seaver Stockdale Carrillo
Basham, Ringe y Correa, S.C.

Government attitude and definition

In Mexico, financial regulators have formally recognised cryptocurrencies. As such, new rules and regulations have been introduced to limit their use in order to curtail the potential use of cryptocurrencies for money laundering and the financing of terrorism. Taking into consideration that the cryptocurrency market in Mexico has been rapidly expanding, measures had to be taken in order fortify the Mexican financial system with respect to the cryptocurrency market. As a result of the implementation of several new laws and regulations, the Mexican financial authorities are very vigilant of any irregularities that may arise from the market.

Moreover, the Financial Technology Institutions Law (*Ley de Instituciones de Tecnología Financiera*) (hereinafter, the "Fintech Law") defines digital assets (cryptocurrencies) as the representation of the electronically registered value used by the general public as a means of payment for all types of legal transactions, and which transfer may only be made by electronic means.

In that sense, the Mexican Central Bank (*Banco de México*) ("Banxico") must first expressly authorise the digital assets being used by Financial Technology Institutions ("Fintechs") and other financial institutions. Furthermore, and for the determination of digital assets, Banxico will consider, among other aspects, the use that the public may give to digital units as a means of exchange, the treatment other countries are giving to such particular digital units as digital assets, as well as the agreements, mechanisms, rules or protocols that will allow the generation, identification and division of the digital assets and control the replication of such digital assets.

This, in turn, will aim to isolate cryptocurrency transactions from the more traditional financial transactions. As such, cryptocurrencies are not a currency of legal tender in Mexico and, thus, are not supported by either the federal government or by Banxico.

Cryptocurrency regulation

In Mexico, cryptocurrencies are regulated by the Fintech Law; published in the Federal Official Gazette (*Diario Oficial de la Federación*) ("DOF") by the federal Executive branch in March 2018.

The main purpose of the Fintech Law is to regulate Collective Financing Institutions (*Instituciones de Financiamiento Colectivo*) (crowdfunding), Electronic Payment Funds (*Instituciones de Fondos de Pago Electrónico*) (electronic wallets), Innovative Models (sandbox models), and regulate the use of cryptocurrencies which have been previously

authorised by Banxico. In that sense, below is a brief summary of the Fintechs regulated by the Fintech Law:

(i) **Collective Financing Institutions (crowdfunding)**: their purpose is to connect applicants with investors, through computer applications, interfaces, internet pages or any other means of electronic or digital communication, so that investors may finance applicants under the following schemes:

  (a) Collective Debt Financing (*Financiamiento Colectivo de Deuda*): investors grant loans, credits, accommodations or any other financing generating a direct or contingent liability for applicants to be paid with interest;

  (b) Collective Capital Financing (*Financiamiento Colectivo de Capital*): investors buy or acquire equity securities from applicants; and

  (c) Collective Financing of Co-Ownership or Royalties (*Financiamiento Colectivo de Copropiedad o Regalías*): investors and applicants will enter into profit-sharing agreements or into any other type of agreements whereby the investor acquires a *pro rata* share or participation in a present or future property or in any income, royalties or losses derived from one or more activities or from any applicant's projects.

(ii) **Electronic Payment Funds (electronic wallets)**: their purpose is the issuance, management, redemption and transmission of electronic payments, including those in Mexican currency, foreign currency or digital assets (cryptocurrencies), through computer applications, interfaces, internet pages, or any other means of electronic or digital communication. Their main activities include, among others:

  (a) opening and maintaining one or more electronic payment accounts for each customer;

  (b) transferring electronic payments, either in Mexican or foreign currency or in digital assets (cryptocurrencies) previously approved by Banxico among its customers and the customers of other Electronic Payment Funds or financial institutions (banks); and

  (c) depositing money or digital assets (cryptocurrencies) in the same amounts of the electronic payments in an electronic payment account, by charging such account.

In this regard, Fintechs are overseen and supervised by Banxico, the National Banking and Securities Commission (*Comisión Nacional Bancaria y de Valores*) ("CNBV"), and an Interinstitutional Committee, formed by designated officials of Banxico, the Ministry of Finance (*Secretaría de Hacienda y Crédito Público*) ("SHCP") and CNBV.

The Fintech Law includes a third category of Fintechs called "Innovative Models", defined as those entities which use technological tools or media, different from the methods provided in the Fintech Law, to provide financial services. Commercial entities providing financial services as described above, and which are not financial technology institutions or banks, shall obtain an authorisation known as an "Innovative Model" authorisation. Such authorisations shall be granted on a temporary basis and will not exceed a period longer than two years – depending on the particularities of the specific project. During the life of the temporary authorisation, entities must obtain a definitive authorisation, adhering to the terms and conditions provided by the financial authorities in the temporary authorisation. Under "Promotion and testing" below, a more detailed analysis of these Innovative Models is provided.

Finally, as will be explained below, the Fintech Law also provides the basis for cryptocurrencies.

Sales regulation

As a result of the enactment of the Fintech Law, several modifications were made to other financial regulations in Mexico, including but not limited to, the Securities Market Law (*Ley del Mercado de Valores*) ("LMV") in March 2018, which provides that the LMV shall regulate:

(1) the offer and intermediation of securities, except in the case of securities offered through Fintechs; and

(2) the development of securities trading systems, allowing transactions with said systems, except in the case of systems offered through Fintechs.

Derived from the above, the sale of bitcoins or other tokens is not regulated by the LMV.

Taxation

Cryptocurrency is currently not taxed in Mexico. The Mexican tax authorities have some plans to tax cryptocurrency and their digital platforms; however, they are still in process of review.

In this sense, up until this day, there is no tax scheme currently established to regulate their transactions.

Money transmission laws and anti-money laundering requirements

The Federal Law to Prevent and Identify Operations with Illicit Resources ("AML Law") was amended in March 2018 to include the habitual and professional offer of exchange of virtual assets by subjects other than financial institutions, which are carried out through electronic platforms, digital or similar, as a "vulnerable activity".

In terms of the AML Law, given their own nature, vulnerable activities are considered to be of a higher risk for money laundering and the financing of terrorism, thus they are subject to enhanced scrutiny by the Financial Intelligence Unit of the Ministry of Finance ("UIF").

Any entity or individual rendering vulnerable activities must comply with additional identification and reporting requirements. For the trade of virtual assets, companies who render said service on a habitual and professional basis must:

(a) have an AML policy;

(b) identify their clients through a robust KYC format for which the minimum content standards are specified in the AML Law and its regulations;

(c) request and keep on file a copy of the official identification documents of the clients and a valid proof of address;

(d) protect and safeguard the identification information for at least five years;

(e) register electronically before the UIF through a specific website for AML reporting; and

(f) file an electronic report for any transactions that exceed 645 times in value the Update and Measurement Unit[1] (MXN 54,496.05 – approx. USD 2,725 – for 2019).

The Ministry of Finance is authorised to audit individuals and organisations who carry out vulnerable activities from time to time, to determine their level of compliance.

Non-compliance with the AML Law may lead to administrative and/or criminal sanctions, with fines ranging from MXN 16,898 to MXN 5,491,850 (approx. USD 945 to USD 274,592.50) and criminal sanctions from two to eight years. Criminal sanctions are only applicable for scenarios in which the company knowingly facilitated the illicit transactions.

Promotion and testing

Yes. As mentioned above, the Fintech Law regulates, among others, Innovative Models (sandbox models). In order to properly implement activities through "Innovative Models" that require an approval, registration or concession in accordance with the Fintech Law or by a distinct financial law, Mexican business entities other than Fintechs, financial entities and other supervised or regulated entities must first obtain a temporary approval.

The Fintech Law defines "Innovative Models" as those which, for the provision of financial services, use technological means or tools, with features other than those existing in the market at the time the temporary approval is granted in terms of the Fintech Law.

Thus, for the granting of said temporary approval, the corresponding financial authorities will evaluate, among other aspects, the fulfilment of the criteria and following conditions:

(i) that the proposal be an "Innovative Model";

(ii) the product to be offered or the service to be provided to the general public must first be tested in a controlled environment;

(iii) the way in which the activity is intended to be developed must represent a benefit to the client of said product or service with regards to what already exists and is operational in the market;

(iv) the project must be developed to such a stage that implementation and beginning transactions can be carried out immediately;

(v) the project must be tested with a limited number of clients; and

(vi) those determined by financial authorities by means of general provisions (secondary laws).

In addition, the temporary approval may not exceed two years. However, in the event that the authorised entity is taking the proper actions to obtain definitive approval, registration or concession in accordance with the Fintech Law, the competent financial authorities may extend the temporary approval, at their own discretion, for up to one additional year.

This extension period is granted so that all necessary actions may be carried out in order to obtain the definitive approval, as mentioned above.

Ownership and licensing requirements

Article 33 of the Fintech Law provides the following:

> "**Article 33.-** Financial Technology Institutions will be prohibited from selling, assigning or transferring their property, lending or guaranteeing or affecting the use or enjoyment of the virtual assets that they guard and control on behalf of their Clients, except in the case of the sale, transfer or assignment of said assets by order of their Clients.
>
> …"

Derived from the abovementioned Article, Fintechs are forbidden from selling, assigning or transferring ownership. They may only participate in the transaction, design or commercialisation of derivative financial instruments that possess underlying virtual assets, subject to the requirements and authorisations of Banxico by means of general provisions.

Additionally, and as mentioned above, the Fintech Law provides that only licensed entities may carry out transactions and become organised as Fintechs. Such authorisation will be granted by the CNBV, with the prior approval of the Interinstitutional Committee, as

mentioned above. It is equally important that Fintechs and other financial institutions are only allowed to carry out transactions with cryptocurrencies expressly authorised by Banxico.

Moreover, on March 8, 2019, the DOF published Circular 4/2019, issued by Banxico. The purpose of Circular 4/2019 is focused on the following:

(i) to define the virtual assets, as well as to identify its characteristics, through which financial institutions and Fintechs may operate;

(ii) to set the terms, conditions and restrictions of the transactions that financial institutions and Fintechs may perform with virtual assets, or cryptocurrencies;

(iii) to establish deadlines, terms and conditions to be observed by financial institutions and Fintechs, in cases where the virtual assets with which they deal are converted into other sorts of virtual assets or their characteristics are modified;

(iv) to ascertain the information regarding virtual asset transactions that financial institutions and Fintechs are required to submit to Banxico in order to obtain its authorisation to operate with virtual assets; and

(v) to define the characteristics of the permissions required to execute transactions with virtual assets.

As mentioned above, Circular 4/2019 is addressed to financial institutions and Fintechs, with regards to their transactions with cryptocurrencies. Pursuant to Circular 4/2019, Banxico will seek to exploit the use of such cryptocurrency technology, under the condition that they are used for internal transactions in these institutions. However, they are not to be used to provide customers with exchange, transfer or custody services.

"Internal transactions" are defined as the activities conducted internally by financial institutions and Fintechs to perform their clients' passive, active and service transactions with or on their own behalf. This includes the activities undertaken by financial institutions and Fintechs to support their international transfers of funds.

In addition, financial institutions and Fintechs intending to perform transactions with virtual assets must submit their authorisation request to Banxico. This request must be accompanied, among others, by the following information:

(i) a description of the virtual assets trading model that the financial institutions and the Fintechs intend to use to conduct such trading;

(ii) a comparative table to allow the identification of the requirements of the applicable regulation and the measures that financial institutions and Fintechs will establish in order to comply with said regulation;

(iii) the benefits of conducting transactions with virtual assets; and

(iv) operating manuals that financial institutions and Fintechs have elaborated in relation to the virtual assets' transactions for which the said institutions request the authorisation of Banxico, among others.

Mining

As previously mentioned, Banxico must first expressly authorise the cryptocurrencies being used by Fintechs and other financial institutions. Furthermore, the Fintech Law is not aimed to govern the issuance of cryptocurrencies, but rather the financial services provided by Fintechs, as well as their organisation and operation, and financial services subject to special regulation that are offered or performed by innovative means.

Given the very nature of Bitcoin mining, and the lack of the verification/authorisation process from Banxico for these types of transactions, this activity is currently not subject to the regulation set forth in the Fintech Law.

Border restrictions and declaration

In terms of customs regulation and foreign trade, intangible goods are not subject to express regulation, since tariffs and regulations and non-tariff restrictions are set in terms of the tariff fraction of the goods and intangible goods are not likely to be classified by tariff.

In this sense, in terms of foreign trade, there is no express regulation for the treatment of cryptocurrencies.

Reporting requirements

As mentioned above, from an anti-money laundering perspective, companies and individuals that exchange virtual assets must habitually and professionally file an electronic report for any transactions that exceed 645 times the value of the Update and Measurement Unit (MXN 54,496.05 – approx. USD 2,725 – for 2019).

In order to do so, companies must first register before the Ministry of Finance as an entity which carries out vulnerable activities through a specific website;[2] furthermore, the company shall also appoint an individual as responsible for reviewing and uploading the information.

Notices should be filed electronically, in the format provided within the website for the specific vulnerable activity, every 17th day of the month.

If the entity is registered but did not carry out any "reportable" activities within a one-month period, then the entity shall report said non-occurrence as well.

Furthermore, Fintechs shall establish the minimum measures and procedures which they must observe to prevent and detect acts, omissions or transactions that could favour, provide help, assistance or cooperation of any kind for the commission of the crimes provided for in the Federal Criminal Code (*Código Penal Federal*), as well as specify the characteristics of transactions and services which must be reported by Fintechs to the corresponding authorities.

Estate planning and testamentary succession

Electronic Payment Funds clients must appoint beneficiaries, which may be replaced at any given time, as well as modify the percentage corresponding to each beneficiary, where appropriate.

In this regard, in the event of a client death, the Electronic Payment Fund institution shall grant the amount of the Electronic Payment Funds to whom the client himself has expressly and in writing designated as beneficiaries, in the percentage determined for each beneficiary.

Finally, if no beneficiaries have been appointed, the amount corresponding to the Electronic Payment Funds must be delivered to the client's succession, as per the applicable Mexican laws.

* * *

Acknowledgment

The authors would like to thank Julio J. Copo Terrés, a lawyer specialised in regulatory law, compliance, and anticorruption, for his invaluable assistance in the preparation of the chapter.

Endnotes

1. The Update and Measurement Unit is an economic reference in pesos, updated annually, and is used to determine the total amount for payments and sanctions provided in federal and local laws.
2. https://sppld.sat.gob.mx/pld/index.html.

Miguel Ángel Peralta García
Tel: +52 55 5261 0474 / Email: peralta@basham.com.mx
Mr Miguel A. Peralta has over 23 years of experience in finance, banking, capital markets, insurance and mergers & acquisitions transactions.

Pedro Said Nader
Tel: +52 55 5261 0574 / Email: psaid@basham.com.mx
Mr Pedro Said has over 15 years of experience in finance, banking, capital markets, corporate law, and insurance transactions.

Patrick Seaver Stockdale Carrillo
Tel: +52 55 5261 0602 / Email: pstockdale@basham.com.mx
Mr Patrick Seaver is an associate of the Firm in the Banking & Finance practice area, focused on national and international transactions, financing, securities, incorporations, project finance, M&A and debt restructuring, among other corporate transactions.

Basham, Ringe y Correa, S.C.

Paseo de los Tamarindos No. 400-A, Piso 9, Bosques de las Lomas, C.P. 05120, Ciudad de México, Mexico
Tel: +52 55 5261 0400 / URL: www.basham.com.mx

Montenegro

Marija Vlajković & Luka Veljović
Moravčević Vojnović i Partneri AOD Beograd in cooperation with Schoenherr

Government attitude and definition

Cryptocurrencies are not regarded as an official means of payment in Montenegro, although their use is not prohibited. In a recent informal statement published on its website, the Central Bank of Montenegro restated that as virtual currencies are not a legal means of payment in Montenegro, any transaction facilitated through virtual currencies is performed at one's own risk. The Central Bank also confirmed that they do not have information on how many individuals and companies are issuing and managing these currencies, including conversion services to conventional currency and *vice versa*.

Given the country's strong desire to join the European Union, the Central Bank of Montenegro and other competent state authorities tend to align their official positions with the current European position and legislation concerning cryptocurrencies, which still remain reserved and to a certain extent doubtful, mostly due to the anonymity surrounding cryptocurrencies, which may lead to potential money laundering, terrorist financing and tax evasion.

Cryptocurrency regulation

There is no relevant legislation regarding cryptocurrency in Montenegro. However, there have been several proposals to regulate particular aspects of cryptocurrency, in particular those relating to money transmission and anti-money laundering. For more details please see under "Money transmission laws and anti-money laundering requirements" below.

Sales regulation

There is no legislation regarding the sale of bitcoins or other tokens in Montenegro.

Taxation

Cryptocurrency is not subject to special tax law procedures in Montenegro. Accordingly, Montenegrin tax rules do not include any special tax rules for income, profits or gains arising from transactions involving cryptocurrencies. In fact, all transactions performed in Montenegro using cryptocurrencies have had their values expressed in euros as well.

Namely, there have been several transactions concerning the purchase and sale of immovable property in Montenegro using cryptocurrencies as a means of payment (in particular, bitcoins). However, all such contracts contained a price in euros in parallel. The Tax Authority of Montenegro applied taxes only on the corresponding value of the property expressed in euros, and not in bitcoins. Concerning these several cases, the Tax Authority

explained that the trade of real estate, goods and services in Montenegro can be performed using virtual currencies, but that the corresponding value needs to be stated not only in bitcoins but in the official currency as well in order to enable the calculation and collection of the value added tax or real estate transfer tax.

Money transmission laws and anti-money laundering requirements

Currently, there is no money transmission and anti-money laundering regulation concerning cryptocurrencies in Montenegro. The currently applicable Prevention of Money Laundering and Financing of Terrorism Act does not specifically regulate cryptocurrencies, though by wider interpretation it could be concluded that cryptocurrencies should also be included under the term 'assets' and should therefore come within the scope of this act.

However, in 2018 the Government proposed the Amendments to the Prevention of Money Laundering and Financing of Terrorism Act (*Prijedlog izmjena i dopuna Zakona o sprječavanju pranja novca i finansiranju terorizma*), which, among others, provide that all legal and natural persons shall report transactions with cryptocurrencies exceeding the equivalent value of EUR 15,000. However, these amendments have not yet been adopted.

Promotion and testing

At the moment we are not aware of any "sandbox" or other programmes intended to promote research and investment in cryptocurrency in Montenegro.

Ownership and licensing requirements

In Montenegro, there are no restrictions on investment managers owning cryptocurrencies for investment purposes, nor are there any licensing requirements imposed on someone who holds cryptocurrency as an investment advisor or fund manager.

Mining

The mining of bitcoins and other cryptocurrencies is also not regulated in Montenegro. Having that in mind, it should not be considered as prohibited. However, there is a complete lack of regulatory framework and supervision over mining activities in Montenegro.

Border restrictions and declaration

There are no border restrictions nor obligations to declare cryptocurrency holdings.

Reporting requirements

Please see under "Money transmission laws and anti-money laundering requirements" above.

Estate planning and testamentary succession

There is no legislation, nor case law, confirming and explaining the use of cryptocurrencies for the purposes of estate planning and testamentary succession in Montenegro.

Marija Vlajković
Tel: +381 11 3202 600 / Email: m.vlajkovic@schoenherr.rs

Ms Vlajković is a partner with a strong track record in employment and corporate/commercial law in Serbia and the wider region. She enjoys many long-standing relationships with clients who she advises on a daily basis, including United Group, CBRE, Sitel, Mastercard, OMV and Cooper Standard. Her assignments also include representing clients in labour disputes. Marija also manages Schoenherr's office in Montenegro. In addition, Marija is a data protection expert and heads Schoenherr's data protection practice in Serbia, Bosnia and Herzegovina, North Macedonia and Montenegro. Marija gives advice on data protection matters to clients like Nepi, Sitel, Immofinanze, Mastercard, Ingram Micro and Ball Corporation. She has held numerous conferences and training on data protection, especially concerning GDPR and its extended application to Serbia, and as well on the newly adopted Data Protection Act.

Luka Veljović
Tel: +382 20 228 137 / Email: l.veljovic@schoenherr.me

Luka Veljović is an associate in Moravčević Vojnović and Partners in cooperation with Schoenherr. Based in the Montenegro office, he is a member of the corporate/commercial practice group, with a track record in real estate and construction, energy and regulatory law in Montenegro and Serbia. He is engaged in corporate and regulatory matters in construction, energy and financial services industries, and some of the clients that he has advised include Shanghai Electric Power, Enemalta plc, Rakita Exploration, EPCG, Ludwig Pfeiffer, United Group and Adient Automotive. Luka graduated from the University of Montenegro, Faculty of Law, while spending a part of his studies at the University of Maribor (Slovenia), the University of Zagreb (Croatia) and the University of Nice (France). He speaks Montenegrin natively, and is fluent in English, French and Spanish.

Moravčević Vojnović i Partneri AOD Beograd
in cooperation with Schoenherr

Bulevar Džordža Vašingtona 98, Atlas Capital Plaza, II Floor, ME-81000 Podgorica, Montenegro
Tel: +382 20 228 137 / Fax: +382 20 226 055 / URL: www.schoenherr.eu

Netherlands

Björn Schep, Willem Röell & Christian Godlieb
De Brauw Blackstone Westbroek

Note

In this chapter, we use "blockchain" as a generic term for all distributed ledger technology-based solutions. Likewise, we use the generic term "crypto" for all cryptocurrencies, tokens, etc. that are based on some sort of cryptography in relation to a blockchain.

Government attitude

Blockchain and distributed ledger technology

Dutch legislation is technology-neutral as a matter of principle. That being said, the Dutch government and the Dutch financial regulators – the Dutch Central Bank and the Authority for the Financial Markets ("**DNB**" and the "**AFM**", respectively) – have, in general, a positive attitude towards blockchain technology. The Dutch government has budgeted EUR 2.8 million for further research into blockchain technology in which it is also actively involved. Research into the practical application of blockchain technology is also a central part of the Digitalisation Strategy adopted by the Dutch Government in June 2018.

It follows from the Strategy that the Dutch Government wishes to encourage experiments in this area and for this purpose it has founded (together with others) the Dutch Blockchain Coalition. In 2019, this Coalition received the assignment to do further research into a regulatory governance framework for blockchain and smart governance for smart contracts.

Furthermore, the Dutch government is exploring whether current legal frameworks are sufficiently flexible to allow companies to make use of the opportunities provided by blockchain technology and whether it enables sufficient mitigation of relevant risks and issues. The Dutch government is exploring the following five use cases: (i) registration of ships (the register is managed by the government); (ii) automating administrative and compliance processes in relation to public grants for social use; (iii) use of smart contracts by private parties; (iv) tracking waste transport on the basis of the European Waste Shipment Regulation; and (v) the recording and sharing of sensitive personal data by the government within the framework of the Social Support Act (*Wet maatschappelijke ondersteuning 2015*).

In addition, and specifically in relation to the financial sector, DNB and the AFM took the initiative to support market parties with their innovations, by setting up an InnovationHub and a Regulatory Sandbox (see the section titled '*Promotion and testing*' below). According to DNB and the AFM, they regularly receive questions from market parties related to blockchain technology, which they are happy to answer. Furthermore, together with the Ministry of Finance, DNB is looking into whether blockchain solutions can increase efficiency in payments and securities transactions.

Cryptos and Initial Coin Offerings

The focus of the Dutch government and the financial regulators with regard to cryptos and Initial Coin Offerings ("**ICOs**") is two-pronged. On the one hand, it is eager to mitigate risks associated with cryptos and ICOs, such as the use of cryptos for criminal purposes, such as fraud and money laundering, and the lack of proper protection afforded to consumers who want to invest in cryptos.

An example of this stance is a report published by DNB and the AFM in December 2018, in which the financial regulators pleaded for the introduction of a licensing regime for providers offering crypto-to-fiat exchange services and custodian wallet providers, much like that which exists for financial undertakings (see the section titled '*Money transmission laws and anti-money laundering requirements*' below).

On the other hand, the Dutch government and financial regulators acknowledge the potential of specific functionalities of cryptos. As an example, they have indicated potential in cryptos for the funding of small and medium-sized enterprises ("**SMEs**") – a condition to which being that investors receive clear and enforceable rights in return, as is the case with, *e.g.*, shares and bonds. To this end, DNB and the AFM have recommended an amendment of the European regulatory framework to enable blockchain-based development of SME funding, and to reconcile the national and the European regulatory definitions of security (see the sections titled '*Crypto regulation*' and '*Sales regulation*' below).

Crypto regulation

Crypto is not considered to be money or fiat by the Dutch government or financial regulators. To reach that conclusion, DNB has applied the common economic theory of the uses of money, meaning that money should be a unit of account, a store of value and a medium of exchange. DNB has stated multiple times that cryptos fulfil these requirements poorly, due to their high volatility and their relative lack of adoption.

Regarding financial regulation, the Dutch financial regulatory framework is laid down in the Dutch Financial Markets Supervision Act ("**FMSA**"). The FMSA is, in principle, built upon the Dutch national regulatory framework, but has, over the years, been significantly influenced by European legislation.

The FMSA regulates activities and services pertaining to financial products. Whether cryptos or activities or services in relation to cryptos fall within the scope of financial regulation therefore depends on whether cryptos fall within the definition of a financial product. The most relevant financial products in the context of defining cryptos are crypto investment objects, electronic money and financial instruments such as shares and bonds.

No specific law, regulation or guidance exists that designates cryptos by definition as any of these products. However, cryptos might still fall within the scope of these definitions based on its specific traits and characteristics. For example, cryptos that are pegged to a fiat currency (stable coins) and that are accepted as a means of payment by other persons than the issuer, might well fall in the scope of electronic money. Similarly, cryptos qualify as securities and (therefore) as financial instruments under Dutch law if they are transferable (*i.e.* negotiable on the financial markets) and represent either (i) a share or equivalent right or instrument, (ii) a bond or other debt instrument, or (iii) any other instrument that can be converted into a share, bond or equivalent or that can be settled in cash (discussed further in the section titled '*Sales regulation*' below).

Furthermore, certain financial products that use crypto as the underlying value – such as shares in crypto investment funds and derivative products – fall within the definition of a

financial product. This is due to the fact that shares in investment funds and derivative products are by themselves considered financial instruments, regardless of the type of asset used as underlying value. Any person wishing to offer these types of products is required to obtain prior authorisation from the AFM (see also the section titled '*Sales regulation*' below).

Finally, it is possible for activities and services related to cryptos to be offered in tandem with other activities and services that *do* fall within the scope of financial supervision. The AFM has provided an example of a crypto services provider that enables its retail clients to exchange their crypto to fiat which is subsequently held by that provider in name of the clients, resulting in the provider providing the regulated activity of attracting redeemable funds from the public.

As such, for the time being, cryptos and activities and services relating to cryptos, other than described above, fall outside the scope of financial regulation. However, at the time of writing, the Dutch government has published its legislative proposal to implement the amendment of the Fourth Anti-Money Laundering Directive (commonly referred to as the Fifth Anti-Money Laundering Directive, the "**AMLD5**"). Although the provisions of the AMLD5 are in principle exclusively aimed at mitigating risks pertaining to money laundering and terrorist financing (discussed in further detail in the section titled '*Money transmission laws and anti-money laundering requirements*' below), the AMLD5 does include some provisions that are clearly meant to subject crypto services providers to some form of general financial regulation. For example, policy-makers for these providers will need to be assessed for suitability and integrity. They are deemed suitable if they possess sufficient relevant knowledge and skills to be able to adequately perform their duties as a policy-maker for a crypto services provider. This includes an assessment of the adequacy of the composition of the managing body as a whole, focusing *inter alia* on the division of tasks and the specific role of the relevant policy-maker. Furthermore, in assessing suitability of a policy-maker, consideration is given to the function, nature, size and the risk profile of the relevant crypto services provider.

Furthermore, the Dutch legislative proposal includes additional provisions, which require these providers to have in place sound and prudent business operations. In the explanatory notes to the legislative proposal, the Dutch legislature has indicated that these requirements are similar to the requirements of sound and prudent business operation stipulated by the FMSA for financial undertakings.

Finally, holders of 10% or more of the issued capital (or a comparable financial interest or a comparable controlling interest) in a crypto services provider will need to be assessed for suitability and integrity by DNB.

Therefore, and despite the fact that cryptos and crypto services providers do not fall within the scope of the Dutch financial regulatory framework, the era in which cryptos could be considered 'unregulated' is definitely over and it should only be a matter of time before more extensive legislation – pertaining to, for example, consumer protection – is developed.

Sales regulation

The sale of cryptos as such is not regulated in the Netherlands. However, an entity issuing or selling cryptos in the Netherlands may fall within the scope of the Dutch financial regulatory framework depending on the characteristics of the crypto that is offered (*e.g.* in case the crypto qualifies as security or investment object), and the manner in which the cryptos are offered (*e.g.* indirectly through an investment fund, or directly through payment in fiat currency).

The regulatory qualification of cryptos is therefore of great importance, as the consequences of both compliance with regulations (*e.g.* governance & transparency requirements) and non-compliance (fines and prosecution) can have a significant impact. Cryptos are assessed based on their characteristics – regulators look at the actual characteristics, not the name given to it by the issuer. If a crypto qualifies as a security, its issuer, the involved brokers, and the exchanges where it has been listed, will generally have to comply with financial markets regulations. Like the qualification of the crypto, the impact of these regulations and the applicability of possible exemptions depends on the specific characteristics of the crypto.

In previous years, issuers of cryptos tended to avoid all types of regulations – with varying degrees of success. We now see the market is starting to embrace the advantages of clarity and certainty that come with regulation (*e.g.* the rise of security token offerings), including making use of legal exceptions and exemptions. In our opinion, this marks the next phase for cryptos in becoming mature market instruments.

Issuers of security cryptos

As a general rule, offering cryptos that qualify as securities (*e.g.* bonds and shares) to the public is not allowed in the Netherlands without prior publication of a prospectus that has been approved by the AFM. However, several exemptions from the obligation to issue a prospectus exist, depending on the type of investment (*e.g.* whether the total consideration of the offer exceeds EUR 5 million or if the denomination per unit exceeds EUR 100,000) and the type of investor (*e.g.* whether the offer is made to consumers or qualified investors). Most of these exemptions stem from European legislation and can be utilised in multiple jurisdictions in the EU.

Service providers and exchanges

As security cryptos fall within the definition of financial instrument, parties rendering financial services in relation to security cryptos (*e.g.* executing orders on behalf of clients or receiving and transmitting orders) qualify as investment firms and must comply with specific ongoing regulations, including those related to governance (*e.g.* the suitability and integrity assessment for prospective board members), market conduct rules (*e.g.* best execution, know-your-customer requirements, informing consumers about the risk of the products and a sound and proper business operation) and prudential rules (*e.g.* minimum capital requirements).

For the same reasons, crypto exchanges that allow listings of security cryptos on their platform that target the European market will also be subject to regulation. The regulatory burden as a result of accepting security cryptos is often the reason that exchanges exclude such cryptos in their listing requirements.

Selling cryptos as investment objects

Cryptos may also qualify as investment objects, the selling of which is a regulated service requiring a licence from the AFM. The entity selling the crypto would need to comply with ongoing regulations on governance (*e.g.* fitness of board of directors and supervisory board) and market conduct rules (*e.g.* information requirements and a sound and proper business operation).

Selling cryptos through fund structures

If cryptos are offered through a fund structure, the manager of this fund requires a licence from the AFM as an alternative investment fund manager ("**AIFM**"). For small funds (with assets under management below EUR 100 million or, if no leverage is used and the fund is

closed-end for a period of at least five years, with assets under management below EUR 500 million) which are offered only to professional investors, there is an exemption to the licence requirement and to certain ongoing requirements applicable to AIFMs.

Taxation

The Dutch Secretary of State of the Ministry of Finance has indicated that it is unlikely that earnings from mining or trading cryptocurrencies by individual tax residents in the Netherlands not acting in a business or professional capacity will be qualified – for taxing purposes – as (taxable) income. This is, of course, different in cases where a natural person receives salary in the form of cryptocurrencies. In such cases, the cryptocurrencies' value in euro at the moment of payout is taxable as income.

Consequently, cryptocurrencies held by an individual tax resident in the Netherlands will generally be taxed under the regime for savings and investments (*inkomen uit sparen en beleggen*). Irrespective of the actual income and capital gains realised, the annual taxable benefit of all the assets and liabilities of such an individual that are taxed under this regime, including cryptocurrencies, is set at a percentage of the positive balance of the fair market value of these assets, including cryptocurrencies, and the fair market value of these liabilities. The percentage (2019), which is subject to an annual indexation, increases from approximately 1.9% to a maximum of 5.6%. No taxation occurs if this positive balance does not exceed a threshold of EUR 30,360 (*heffingvrij vermogen*). The fair market value of assets, including the cryptocurrencies, and liabilities that are taxed under this regime is measured exclusively on 1 January of every calendar year. The tax rate under the regime for savings and investments is a flat rate of 30%.

A corporate entity tax resident in the Netherlands is generally subject to corporate income tax at the statutory rate of 25% (20% up to EUR 200,000) with respect to any benefits, including any capital gains realised on the disposal thereof, derived or deemed to be derived from dealings involving cryptocurrencies, including mining and trading.

Money transmission laws and anti-money laundering requirements

The business of money transmission is regulated as 'money remittance services' under the FMSA. Providing money remittance services requires a licence from DNB (based on the European payment services directive; PSD2).

A money remittance service is defined as a service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee. It is relevant to note that for the purpose of this definition, 'funds' are defined as banknotes and coins, scriptural money or electronic money. By definition, cryptos are not banknotes and coins and, as indicated under the section titled '*Crypto regulation*' above, crypto is not considered to be (scriptural) money. Finally, only in specific cases are cryptos considered to be electronic money. As a result, money remittance laws are only applicable to a very limited number of crypto use cases.

As mentioned under the section titled '*Crypto regulation*' above, the Dutch government has published its legislative proposal to implement the AMLD5. The provisions of the AMLD5 are aimed at mitigating risks pertaining to money laundering and terrorist financing. For this purpose, providers offering crypto-to-fiat exchange services and custodian wallet

providers will be required to be registered at DNB. In order to be registered at DNB, these crypto services providers will need to demonstrate that they are able to comply with the provisions of the Dutch Money Laundering and Terrorist Financing (Prevention) Act (*Wet ter voorkoming van witwassen en financiering van terrorisme*). This means that these providers will need to apply risk-based client due diligence measures.

Client due diligence measures consist of (i) identifying the customer and verifying that identity on the basis of documents, data or information obtained from a reliable and independent source, (ii) identifying the ultimate beneficial owner of the customer, if any, (iii) assessing the business relationship with the customer and obtaining information on the purpose and intended nature of that relationship, and (iv) conducting ongoing monitoring of the business relationship, including scrutinising transactions undertaken throughout the course of the relationship.

Crypto services providers will need to apply these client due diligence measures when (a) establishing a business relationship, (b) there is an indication of involvement of the client with money laundering or terrorist financing activities regardless of any derogation, exemption or threshold, (c) there are doubts about the veracity or adequacy of previously obtained customer identification data, (d) there is reason to do so based on the risk of involvement of a current client with money laundering or terrorist financing, (e) the client has its residence, principal place of business or statutory seat in a country that represents a higher risk of money laundering or terrorist financing, or (f) carrying out an occasional transaction above EUR 15,000. If, in the future, crypto transfers will come to be qualified as a transfers of funds (meaning (i) a credit transfer, direct debit, money remittance or a transfer carried out using a payment card, an electronic money instrument, a mobile phone or any other digital or IT prepaid or post-paid device with similar characteristics, that is (ii) carried out through a payment services provider), the threshold amount under (f) will be reduced to EUR 1,000.

Note that a business relationship is assumed to be present fairly quickly. As such, a business relationship between a services provider and a client is considered to exist not only where a provider provides continuous services to a client, but also where a client engages the services provider for a second time. This includes situations in which a services provider, upon first engagement, has reasons to presume the client will make use of its services again and even those situations in which the services provider is unable to ensure that the client will not use its services for a second time. If the services provider is unable to ascertain whether a client engaging the services provider is, in fact, a new client, the services provider will have to assume it is a returning client – thus creating a business relationship and obligating the services provider to perform client due diligence measures. Crypto services providers should have in place procedures to assess and demonstrate whether a service provided to a client is incidental or whether it constitutes a business relationship.

The client due diligence measures will have to be applied to an extent that is adequate in relation to the services provider's exposure to money laundering or terrorist financing risks considering the type of client, business relationship, product or specific transaction. Factors to be considered when determining this exposure are factors and types of evidence stipulated by the AMLD5 or identified by Member States or other relevant bodies – the FATF and the G20, for example. The exposure assessment should furthermore take into account the results of a self-assessment of the crypto services provider, which focuses on, *inter alia*, the specific services provided, the distribution channels and the transaction size. Crypto services providers are required to have measures and policies in place to ensure that the exposure identified in this way is sufficiently mitigated and controlled.

In all cases, the transaction monitoring process, as part of the client due diligence measures, has to enable the crypto services provider to identify and report suspicious transactions of the client to the Dutch Financial Intelligence Unit. A suspicious transaction is any transaction that defers from the client's regular use and profile. This means that the services provider will need to apply know-your-customer measures to such an extent as to be able to create a profile of the relevant client. For this purpose, the services provider can make use of, for example, the amount of funds usually used by the client in a single transaction or the devices usually used by the client (*e.g.* a mobile phone).

If, following any of the above assessments, a crypto services provider concludes that it is not able to sufficiently mitigate and control the associated money laundering and terrorist financing risks, the relevant transaction may not be executed or the business relationship may not be established or, as the case may be, the existing business relationship will have to be terminated. Risks that cannot be sufficiently mitigated and controlled may exist where, for example, the identity of the client is not verifiable, where the source of funds and source of wealth of the client cannot be ascertained, or where the services provider is unable to discover the reasons for an intended or performed transaction.

As mentioned, the provisions discussed here apply to providers offering crypto-to-fiat exchange services and custodian wallet providers. Note, however, that in a recent publication on anti-money laundering measures, the Dutch government has made public plans to request the European Commission to propose further amendments to the European anti-money laundering legal framework, in order to extend the scope of the AMLD5 to providers of ICO services and to providers offering crypto-to-crypto exchange services. At the time of writing, these plans have not yet been followed up on.

Promotion and testing

Implementation of crypto products and, to a lesser extent, blockchain solutions, is sometimes impeded by the current financial regulatory framework. However, within the limits of their mandate, DNB and the AFM play an active and facilitating role through the InnovationHub, Regulatory Sandbox and the facilitation of partial authorisations.

InnovationHub

The InnovationHub supports market parties that seek to implement innovative financial business models, services or products to the market. In addition to offering a single point of access to the regulators, the InnovationHub enables market parties to understand the relevant regulatory framework.

Regulatory Sandbox

The Regulatory Sandbox provides a 'safe environment' in which tailor-made solutions can be created. This enables market parties to safely test innovative products and business models, without fear of regulatory enforcement measures, such as fines. In the context of the Regulatory Sandbox, the relevant regulators (DNB, the AFM and the Data Protection Authority) will assess whether the applicants and their innovative concepts comply with the underlying purposes of applicable regulations, rather than the strict letter of the law.

Partial authorisations

Market parties that, through their services, qualify as financial undertakings but do not wish to engage in all operations governed by a full authorisation, or are not yet able to meet all eligibility requirements for such an authorisation, have the possibility to obtain a partial authorisation from the regulators. Such authorisations may be granted on a temporary basis,

but may also have a more permanent nature. It allows businesses that are testing innovative services and products to develop a fully-fledged financial undertaking step-by-step.

In addition to the aforementioned facilities, and as mentioned in the first section '*Government attitude*', the Dutch government is also very receptive to fintech. Innovation is a key topic on the Minister of Finance's agenda for the financial sector. Priorities include measures to facilitate market access for fintechs, proportionality of regulations and research on the possibilities of blockchain for payments and securities.

Ownership and licensing requirements for funds managers

In the Netherlands, there are no restrictions on fund managers owning crypto. However, fund managers must be authorised to operate as an AIFM (by the AFM) if they manage an investment fund with assets under management above certain thresholds or if they offer participation rights to retail investors. This applies to managers of 'regular' investment funds and crypto investment funds alike (see also '*Sales regulation*' above). In June 2018, the AFM issued a communication on the management of crypto investment funds specifically, in which it highlights a number of requirements (based on European regulations) for authorisation and ongoing supervision that may present compliance difficulties for crypto fund managers; these requirements concern liquidity management, valuation, depositary, product approval and review processes, and anti-money laundering. When considering a licence application, the AFM is expected to pay special attention to these elements.

With regard to providing investment advice on crypto, it depends on the qualification of the crypto in which advice is provided, whether the person providing such as advice is regulated. Due to the fact that – currently – cryptos do not qualify as financial products as defined in the FMSA, advising investors on buying or selling cryptos as such does not fall within the scope of the Dutch financial regulatory framework. However, if the investment advisor advises on cryptos that qualify as financial instruments (securities), that advisor will fall within the scope of the definition of an investment firm and will need to be authorised as such by the AFM (see sections '*Crypto regulation*' and '*Sales regulation*' above).

A licence is also required when advising on cryptos that qualify as investment objects (see also '*Sales regulation*'). In addition, if the investment advisor holds retail client funds (fiat currency) in order for this retail client to exchange the purchased crypto, the advisor will again fall under the scope of another regulatory rule, as it is prohibited under the Dutch FMSA to attract, obtain or hold repayable funds from the public. There are several exceptions and exemptions to this prohibition, as well as the possibility of obtaining a dispensation, but these typically do not apply to an investment advisor that holds retail client funds.

Privacy regulation

Compliance with the European Union's General Data Protection Regulation ("**GDPR**") can be challenging for companies operating blockchains. The GDPR applies to organisations which process personal data. Processing is defined widely and includes collecting, storing and destroying data. The GDPR poses several challenges for blockchain solutions, most notably assigning the obligations of data controllers and processors to particular actors in blockchain systems and compliance with the individuals' rights to have personal data deleted or corrected. These GDPR requirements are at odds with a decentralised blockchain-based data governance model and the concept of immutability of data stored on a blockchain.

Minimising the risks of collision with the GDPR

If no personal data is processed on a blockchain, the GDPR does not pose a problem for its operator. However, personal data is a broad term that, under certain circumstances, can even include the colour of a car or a public key to a crypto wallet. To minimise GDPR compliance risks, blockchain operators should apply robust anonymisation techniques (*e.g.* by storing an encrypted anonymous hash of the personal data on-chain, with the underlying and identifying personal data being kept off-chain). Although the application of such technical solutions may not exclude the applicability of the GDPR altogether, it may substantially enhance the blockchain operator's means to meet the GDPR requirements. In practice, complete anonymisation is very difficult to achieve, especially in a public, permission-less blockchain, as its operator may not be able to control all data uploaded by the users of its blockchain.

Stay in control

The use of private, permissioned blockchains increases the chances of GDPR compliance because the operator can impose and enforce a governance framework for users via contracts setting out each actor's rights and obligations.

It is worth noting that ensuring GDPR compliance is specific to a particular use of blockchain, not the technology as such. Therefore, obtaining legal advice tailored to a particular use of blockchain is recommended, as the consequences of a GDPR violation can be severe, with fines of up to 4% of annual worldwide turnover or EUR 20 million (whichever is greater), criminal liability and damage claims by individuals or via class actions.

Mining

Mining of Bitcoin and other cryptos is unregulated and permitted in the Netherlands. Certain members of Parliament continue to share their concerns with regard to the electricity consumption related to crypto mining activities. However, at the time of writing, it seems unlikely that the Netherlands will prohibit or regulate mining of cryptos in the near future.

Border restrictions and declaration

If liquid assets with a value equivalent to an amount of EUR 10,000 are brought into the European Union through the Netherlands, the bearer of those liquid assets is required to file a declaration with Dutch Customs. However, cryptos do not currently qualify as liquid assets as referred to in the Liquid Assets Regulation (*i.e.* (foreign) banknotes or coins that are in circulation as a means of payment, securities to bearer, not registered by name, such as shares and bonds and travellers cheques that are not registered by name). Therefore, bringing crypto into the Netherlands does not trigger any filing obligation for the bearer, regardless of whether the crypto is held by the bearer through online storage or is brought into the Netherlands 'physically' using cold storage devices or facilities.

Reporting requirements

Please refer to '*Money transmission laws and anti-money laundering requirements*' above.

Björn Schep
Tel: +31 20 577 1358 / Email: björn.schep@debrauw.com

Björn Schep is a senior associate in the firm's Financial Markets Regulatory practice group and specialises in financial law and, in particular, investment management, insurance and financial markets regulation. Björn was seconded to Slaughter and May in London in 2012, where he worked in the Financial Regulation group. In October 2017, Björn completed the Executive Master Insurance Studies/Enterprise Risk Management at the Amsterdam Business School.

He regularly advises insurers, banks, investment firms and financial services providers on applicable financial regulatory requirements such as licence requirements, prudential requirements and market conduct requirements.

Björn has assisted large established banks and insurers in the Netherlands with their discussions with DNB and the AFM in connection to new innovative ideas. Björn has worked with several fintech startups, mostly advising them on market access issues.

Willem Röell
Tel: +31 20 577 1032 / Email: willem.roell@debrauw.com

Willem Röell specialises in financial markets regulation. He advises large financial groups on a broad range of regulatory matters, including licensing, conduct of business rules, capital requirements, recovery and resolution planning, and the governance and regulatory aspects of M&A transactions.

Willem especially focuses on assisting clients who would like to introduce innovative technologies into the financial sector. He assists them with issues related to market access, governance and the outsourcing of distributed ledger solutions, robo-advice and advanced analytics, and communication with regulators. As a member of the Fintech team, Willem regularly speaks and publishes on these topics.

Willem holds an LL.M. in financial law and a B.A. in Latin American Studies from Leiden University. He supports several charitable organisations with a focus on education, human rights and the arts.

Christian Godlieb
Tel: +31 20 577 1474 / Email: christian.godlieb@debrauw.com

Christian Godlieb is a senior associate in De Brauw's Financial Markets Regulation practice group. He specialises in Dutch and EU financial markets regulation, regularly advising banks, investment firms, payment institutions and pension providers on a broad range of regulatory matters, such as licence requirements, prudential requirements and ongoing market conduct obligations. Christian further specialises in innovation in the financial sector and regularly publishes on the topic of regulatory developments in that area.

De Brauw Blackstone Westbroek

Claude Debussylaan 80, 1082 MD Amsterdam / P.O. Box 75084, 1070 AB Amsterdam, The Netherlands
Tel: +31 20 577 1771 / URL: www.debrauw.com

Portugal

Filipe Lowndes Marques, Mariana Albuquerque & João Lima da Silva
Morais Leitão, Galvão Teles, Soares da Silva & Associados [Morais Leitão]

Government attitude and definition

Blockchain technology in general, and cryptocurrencies in particular, are some of the most closely followed topics in the financial technology industry amongst the Portuguese government and the relevant regulatory authorities, along with prevailing fintech trends in other jurisdictions. In particular, in the last five years these technologies have been brought to public attention largely due to the dramatic increase in the value of Bitcoin, the rise in the number of initial coin offerings (ICOs) globally, and their market capitalisation. This focus is also driven by some significant developments that the Portuguese market has seen in recent years in this sector, most notably the rise of tech-based companies and the steady increase in the use of cryptocurrencies in the last decade.

Notwithstanding, in Portugal, blockchain technology has not been implemented in a significant number of services and is yet to have a relevant impact on either private or public organisations. In fact, to date in Portugal, most blockchain technology has been used in the issuance of tokens, including in the context of ICOs. For these reasons, the government and regulatory authorities have been invested in studying blockchain technology and cryptocurrencies with a view to creating favourable conditions for the establishment and development of the sector, while protecting all market participants' interests.

For the purpose of this chapter, cryptocurrencies can be broadly defined along the European Central Bank's definition – to which the Portuguese authorities have largely subscribed – as a "digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money".[1] Other useful constructions have been developed by the European Securities and Markets Authority (ESMA) in its advice on Initial Coin Offerings and Crypto-Assets (January 2019)[2] and in a study requested by the European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance (June 2018).[3]

In Portugal, cryptocurrencies do not have legal tender and thus do not qualify as fiat currency, nor are they treated as "money" (whether physical or scriptural) or "electronic money". Nonetheless, they are largely seen as an alternative payment method with a contractual nature that results from private agreement between participants of cryptocurrency transactions and with intrinsic characteristics that somewhat replicate some of the core traits of traditional money: storage of value; unit of account; and medium of exchange. Taking this into consideration, contrary to other countries that have been developing trials for government-backed cryptocurrencies, including those which have successfully launched government-backed cryptocurrency, there is no public governmental

proposal to provide legal backing to cryptocurrencies. Cryptocurrencies are thus not backed by the Portuguese government and *Banco de Portugal* (Portugal's central bank).

Cryptocurrencies can also be seen under a different light concerning their functionality. In this context, there has been recognition of other types of tokens, such as utility tokens and security tokens, commonly marketed through ICOs. These may be differentiated by their distinctive function, since the former are largely linked to consumption and the latter to investment. For this reason they encompass or give rise to many other rights, including, among others, the right to receive a product or service or economic rights. In 2018, the Portuguese government actually issued a token – GOVTECH – which was used to cast votes by allocating those tokens to competing projects, thereby replicating investment choices, in a technological competition sponsored by the Portuguese government. The initiative was the first of its kind and goes to show the Portuguese government's willingness to apply the technology (although still in a risk-free setting).

In light of the above, these new technologies have inevitably drawn the attention of the relevant regulatory authorities, most notably the Portuguese banking authority (*Banco de Portugal*), the Portuguese securities authority (*Comissão do Mercado de Valores Mobiliários* or CMVM) and the Portuguese insurance and pension funds authority (*Autoridade de Supervisão de Seguros e Fundos de Pensões* or ASF).

Banco de Portugal, in its capacity as both central bank and national competent authority for the supervision of credit and payment institutions, has shown a clear interest in cryptocurrencies, notably from the perspective of consumer/investor protection, but has otherwise clarified that it will not take any immediate steps to regulate cryptocurrencies, having adopted instead a watchdog approach to the phenomenon and its development.

Nevertheless, since 2013, *Banco de Portugal* has issued a number of public statements and warnings in relation to cryptocurrencies, in line with the regulatory practices of other central banks of the eurozone and European regulatory authorities, such as the European Central Bank (ECB) and the European Banking Authority (EBA). We highlight, *inter alia*, *Banco de Portugal*'s publications which have included a warning focused on Bitcoin (Nov. 2013), where it cited the European Central Bank's study, *Virtual Currency Schemes* (Oct. 2012) (in which the ECB noted that it would be closely monitoring this phenomenon with a view to studying any necessary regulatory responses)[4], and a warning to consumers regarding the potential risks in using cryptocurrencies (October 2014).[5] *Banco de Portugal* has since also created a dedicated page headed 'virtual currencies' on its website, where it warns consumers, on the one hand, and credit institutions, payment institutions and electronic money institutions, on the other hand, on certain risks entailed in cryptocurrencies.

In the same manner, CMVM has published a warning to investors, in line with other European regulatory authorities, such as ESMA, alerting investors to the potential risks of ICOs in order to raise awareness to these risks (November 2017)[6] and has also issued a notice relating to a specific ICO for the issuance of Portuguese token Bityond (May 2018),[7] stating that it did not consider it a security and, accordingly, Bityond was not subject to the CMVM's supervision or compliance with securities laws and a notice alerting consumers to risks of cryptocurrency (*e.g.* Bitcoin, Ether and Ripple), notably inadequate information and lack of transparency (July 2018).[8]

In 23 July 2018, the CMVM issued a formal notice addressed to all entities involved in ICOs,[9] regarding the legal qualification of tokens. The CMVM stressed the need for all entities involved in ICOs to assess the legal nature of the tokens being offered under the

ICOs, in particular their possible qualification as securities with the application of securities laws as a consequence. In this context, the CMVM noted that tokens can represent very different rights and credits, and be traded in organised markets, thus concluding that tokens can be qualified, on a case-by-case basis, as (atypical) securities under Portuguese law, most notably considering the broad definition of securities provided under the Portuguese Securities Code, approved by Decree-Law no. 486/99, of November 13, as amended.

Notwithstanding, there still has not yet been any legislative impulse from either the Portuguese Government or Parliament or from any other regulatory authority with specific laws or regulations in relation to cryptocurrencies, which therefore remain vastly unregulated from a systemic and teleological perspective.

Cryptocurrency regulation

As previously mentioned, at present, there are no specific laws and regulations applicable to cryptocurrencies in Portugal, including in relation to their issuance and transfer. Hence, cryptocurrencies are not prohibited and investors are allowed to purchase, hold and sell cryptocurrencies.

Nevertheless, on 10 March 2015, *Banco de Portugal* issued a recommendation urging banks and other credit institutions, payment institutions and electronic money institutions, to abstain from buying, holding or selling virtual currency due to the risks associated with the use of virtual currency schemes identified by the European Banking Authority (the Bank of Portugal's Recommendation).[10] Pursuant to this recommendation, most of the aforementioned institutions in Portugal have stopped accepting any orders to process payments made to and by cryptocurrency platforms and exchanges, such as Coinbase, which in practice have restricted its clients to purchasing or selling cryptocurrencies through these platforms and exchanges.

In relation to other types of tokens in Portugal, the same can be said as there are also no specific regulations applicable to other forms of virtual tokens.

However, one cannot say that there is a regulatory vacuum in this context, since existing laws will need to be assessed on a case-by-case basis to determine if they apply to a particular ICO, token or related activity. In this regard, the laws applicable to tokens will vary greatly depending on the specific characteristics of each token.

Thus, from a legal framework perspective, the main concern when analysing an ICO and the respective tokens, will be to determine whether the ICO represents a utility token or a security token.

ICOs that aim to offer tokens that represent rights and/or economic interests in a specific project's results, use of software, access to certain platforms or virtual communities or other goods or services, may hypothetically overlap with consumer matters and become subject to certain regulations regarding consumer protection.

ICOs that aim to offer tokens that represent rights and/or economic interests in a pre-determined venture, project or company, such as tokens granting the holder a right to take part in the profits of a venture, project or company or even currency-type tokens, may potentially be qualified as securities and cross over to securities' intensively regulated world, becoming subject to existing securities regulations, most notably regulations applicable to public offerings of securities and/or securities trading venues. In this respect, it should be noted that subsequent to ESMA's position, in November 2017, stating that

ICOs qualifying as financial instruments may be subject to regulation under EU law,[11] as of 9 January 2019, ESMA has published advice on Initial Coin Offerings and Crypto-Assets.[12] Notably, under the heading "Regulatory implications when a crypto-asset qualifies as a financial instrument", ESMA provides advice on the potential application of, notably, the Prospectus Directive (Directive 2003/71/EC, as amended), the Transparency Directive (Directive 2013/50/EU), the Markets in Financial Instruments Directive (Directive 2014/65/EU), the Market in Financial Instruments Regulation (Regulation (EU) No. 600/2014) and respective implementing acts, the Market Abuse and Short-Selling Regulation (Regulation (EU) No. 596/2014 and Regulation (EU) No. 236/2012), the Settlement Finality Directive (Directive 2009/44/EC), the Central Securities Depository Regulation (Regulation (EU) No. 909/2014) and the Alternative Investment Fund Managers Directive (Directive 2011/61/EU).

It is also worth noting that, within the context of the information published regarding Portuguese cryptocurrency Bityond, mentioned above, the CMVM has already publicly stated that a token which allows its users to (i) participate in surveys related to the development of an online platform, and (ii) further donate tokens to the online platform for the develop of new tools, is not qualified as a financial instrument, i.e. is not a security token, and therefore is not subject to securities law and the supervision of the CMVM.

Additionally, in its formal notice addressed to entities involved in ICOs, dated 23 July 2018, and mentioned above, the CMVM clarified the elements that may, in abstract, implicate the qualification of security tokens as securities, namely: (i) if they may be considered documents (whether in dematerialised or physical form) representative of one or more rights of private and economic nature; and (ii) if, given their particular characteristics, they are similar to typical securities under Portuguese law. For the purpose of verifying the second item, the CMVM will take into account any elements, including those made available to potential investors (which may include any information documents – e.g. white paper), that may entail the issuer's obligation to undertake any actions from which the investor may draw an expectation to have a return on its investment, such as: (a) to grant the right to any type of income (e.g. the right to receive earnings or interest); or (b) undertaking certain actions, by the issuer or a related entity, aimed at increasing the token's value.

The CMVM thus concludes that if a token is qualified as a security and the respective ICO is addressed to Portuguese investors, the relevant national and EU laws shall apply, including, *inter alia*, those related to: the issuance, representation and transmission of securities; public offerings (if applicable); marketing of financial instruments for the purposes of MiFID II; information quality requirements; and market abuse rules. Finally, should the ICO qualify as a public offering, the CMVM further clarifies that a prospectus should be drafted and submitted, along with any marketing materials for the ICO, to the CMVM for approval, provided that no exemption applies in relation to the obligation to draw a prospectus. Lastly, in this notice the CMVM also alerts that where a token does not qualify as a security, its issuer should avoid the use, including in the ICO's documentation, of any expressions that may be confused with expression commonly used in the context of public offerings of securities, such as "investor", "investment", "secondary market" and "admission to trading".

Sales regulation

Considering the lack of exclusive regulation in relation to cryptocurrencies in Portugal, as

described under "Cryptocurrency regulation" above, the purchase and sale of cryptocurrencies *per se* is also not specifically regulated.

However, to the extent that a token sale may be qualified as, for example, an offer of consumer goods or services or an offer of securities to the public, the relevant existing laws and regulations on, respectively, (i) consumer protection (including national laws that transposed, among others, Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services, Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market), and (ii) securities and financial markets (including national laws that transposed, among others, the Prospectus Directive, Transparency Directive, MiFID II and AIMFD Directive), may apply by default, including their sanctions regime, subject to, in any case, an individual assessment. In these cases, both consumer protection law and securities law provide a number of obligations that must be complied with during and after the sale process. Therefore, existing regulations on the sale of consumers' goods or services and of securities can apply to certain types of tokens on a case-by-case basis, in accordance with an "as-applicable principle".

Taxation

In Portugal, there is no specific regime that deals exclusively with the taxation of cryptocurrencies. Nonetheless, the Portuguese Tax Authority has published two official rulings in the context of certain requests for binding information relating to cryptocurrencies; one in the context of personal income tax (December 2016),[13] and the other in the context of value added tax (February 2018).[14] In the absence of other laws and regulations that may clarify the taxation regime of cryptocurrencies, these rulings have an important weight and will work as precedents in relation to how the Portuguese Tax Authority will look into cryptocurrency and cryptocurrency-related activities when interpreting existing tax provisions and deciding whether or not a certain fact or action should be subject to Portuguese tax (corporate, individual, VAT or stamp duty). In any event, as these were given in the context of requests for binding information, the Portuguese Tax Authority may revoke these rulings in the future.

In the 2016 official ruling, the Portuguese Tax Authority analysed the possible classification of cryptocurrencies within certain types of income that are subject to Portuguese tax, notably capital gains, capital income and income from business activities, and decided that, as a general rule, natural persons should not be taxed in respect of gains derived from the valuation of cryptocurrency or sale of cryptocurrencies, except that, in the case of sale of cryptocurrencies, if they correspond to the individual's main recurrent activity, income obtained from such activity could be subject to Portuguese tax. It should also be noted that this was only a partial decision that did not elaborate on other types of income derived from other cryptocurrency-related activities (e.g. mining and farming activities).

In the 2018 official ruling, the Portuguese Tax Authority received a request to issue an opinion on the application or exemption of value added tax (VAT) to cryptocurrencies exchanges. The Portuguese Tax Authority invoked precedent from the Court of Justice of the European Union (Case C-264/14, *Skatteverket v. David Hedqvist*) to argue that although cryptocurrencies, such as for example Bitcoin, were analogous to a 'means of payment' and therefore subject to VAT, they were exempt by application of VAT exemption rules, which should be consistent across EU Member States considering existing VAT EU harmonisation.

Money transmission laws and anti-money laundering requirements

The Portuguese law on anti-money laundering and combating terrorist financing[15] (AML Law) imposes a general undertaking to obliged entities of risk management in the use of new technologies or products which are prone to favour anonymity.[16] This means that, under Portuguese law, obliged entities are legally required to monitor the risks of money laundering and terrorist financing arising pursuant to the use of new technologies or developing technologies, whether for new products or existing ones,[17] and, before launching any new products, processes or technologies, they will have to analyse any specific risks of money laundering or terrorist financing related to it, and to document the specific procedures adopted for their risk mitigation.

In addition, obliged entities must undertake identification procedures and customer due diligence whenever there is an occasional transaction of more than €15,000, as well as reinforce their identification procedures and customer due diligence when they identify an additional risk of money laundering or terrorist financing in business relationships, in occasional transactions or in the usual operations of the customer. Pursuant to the AML Law, an additional risk is presumed to exist in products or operations that favour anonymity, in new products or commercial activities, in new distribution mechanisms and payment methods and in the use of new technologies or developing technologies, whether for new products or existing ones. This has obvious implications for cryptocurrencies and cryptocurrency-related activities (including cryptocurrencies exchanges) in case those operations intersect with the activities and operations of entities that are covered by obligations imposed by anti-money laundering and combatting terrorist financing, since obliged entities should reinforce their identification procedures and customer due diligence when participating in any related operation.

In the banking sector, the Bank of Portugal's Recommendation, mentioned above, was driven also by concerns with the risks of money laundering, terrorist financing and other financial crime arising pursuant to the overall predominance of anonymity and lack of intermediaries that would communicate suspicious activities to the authorities.[18] This recommendation followed a previous warning to consumers issued in October 2014, as mentioned above, that was made in response to the fact that certain automated teller machines (ATMs) in Portugal, which were not integrated in the Portuguese payment system, were enabling exchange between bitcoins and euros.

Banco de Portugal's stance in respect of cryptocurrencies does not affect other market participants such as consumers, investors and other entities that wish to, respectively, hold, invest or develop cryptocurrencies, but it goes a long way towards reducing the participation of banks and other credit institutions, payment institutions and electronic money institutions that are traditional 'obliged entities' for the purposes of anti-money laundering and combating terrorist financing laws. It should be also noted that insofar as operations in cryptocurrencies are not undertaken by obliged entities (as legally defined), compliance with and enforcement of anti-money laundering and terrorist financing laws should be diluted, as cryptocurrencies and related activities are confined to virtual platforms and private relations.

Furthermore, considering the publication of AMLD 5,[19] additional obligations in relation to cryptocurrencies exchanges and custodian wallet providers are expected to come into force after 10 January 2020, when Member States, including Portugal, are required to implement and bring into force laws transposing AMLD 5.

Promotion and testing

The Portuguese government has launched a think-tank with the objective of promoting and fostering fintech generally – mostly by identifying and targeting entry barriers. The ultimate aim of the think-tank is to implement a regulatory 'sandbox' with the aid of the Portuguese financial regulators. Within the objectives of the think-tank, cryptocurrencies have been listed as one of the priorities.

Additionally, both the CMVM and *Banco de Portugal* have developed specific spaces for fintech on their webpages, http://www.cmvm.pt/en/ and https://www.bportugal.pt/en/, respectively, which include, *inter alia*, information regarding distributed ledger technology, initial coin offerings and tokens.

These fintech spaces were created with the intent to facilitate the provision and exchange of information and dialogue between these regulators and developers or sponsors of new financial technologies which cross over with the areas of regulatory competence of the CMVM and *Banco de Portugal*, and also to clarify the regulatory framework applicable to the same. These objectives are obtained mainly by having a dedicated contact within the CMVM and *Banco de Portugal* that deals solely with issues relating to fintech, and by being active in promoting conferences and workshops aimed at investors and the public in general with a formative and educational goal.

In 2018, a non-profit organisation, Portugal Fintech, and *Banco de Portugal*, CMVM and ASF joined efforts to create "Portugal FinLab – where regulation meets innovation", which created a direct communication platform for emerging tech companies working in Fintech-related subjects, incumbents and Portuguese regulators to engage and to provide guidance on a more clear path of action in terms of the application of the existing regulatory framework to those companies' activities.

Ownership and licensing requirements

As mentioned in "Cryptocurrency regulation" above, in Portugal there are no specific restrictions or licensing requirements when it comes to purchasing, holding or selling cryptocurrencies, except where they are qualified as securities.

Furthermore, insofar as cryptocurrencies are not qualified as financial instruments, advisory services that are made exclusively in relation to and the exclusive management of cryptocurrency portfolios are not subject to the same investment services laws and regulations as those applicable to securities. Thus, these types of activities, when undertaken solely in relation to cryptocurrencies, are not subject to any licensing requirements.

However, traditional advisory services and management services require licensing and are subject to the CMVM's supervision.

One thing to note is that, given the relative novelty of some of these instruments, the overall regulatory uncertainty and even some regulatory pushback (e.g. the Bank of Portugal's Recommendation), underpinned by the already existing and overarching obligations applicable to the provision of investment services, it is not at all likely for the time being that traditional investment advisors, including, among others, credit institutions and fund managers, will recommend or invest in cryptocurrencies.

Mining

There are no restrictions in Portugal on the development of mining of cryptocurrencies and the activity itself is not regulated.

Border restrictions and declaration

In Portugal there are no border restrictions or obligations to declare cryptocurrency holdings.

Reporting requirements

There is no standalone reporting obligation in case of cryptocurrency payments above a certain threshold, except in the case of transactions that may involve an obliged entity covered by anti-money laundering and terrorist financing laws, in which case such entity will have to report suspicious transactions or activities irrespective of the amounts involved.

Estate planning and testamentary succession

There is no precedent, specific rules or particular approach regarding the treatment of cryptocurrencies for the purposes of estate planning and testamentary succession in Portugal.

Notwithstanding, certain aspects of estate planning and testamentary succession should be highlighted. Inheritance tax does not exist in Portugal, but stamp duty may apply to certain transfers of certain assets (e.g. immovable property, movable assets, securities, negotiable instruments, provided they are located, or deemed to be located in Portugal) included in the deceased estate in case of succession.

However, in the absence of a legal amendment or binding information from the Portuguese tax authorities, it may be argued that the drafting of the relevant legal provisions does not expressly foresee assets such as cryptocurrencies, thus excluding the same from the scope of application of stamp duty, which *de facto* mitigates the need for estate planning with respect to cryptocurrencies. Estate planning and testamentary succession must therefore be analysed on a case-by-case basis, considering all variables involved.

* * *

Endnotes

1. *Cf.* European Central Bank, *Virtual currency schemes – a further analysis*, February 2015, available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf. See also the definition of virtual currency included in the fifth AML Directive (Directive (EU) 2018/843).
2. *Cf.* European Securities and Markets Authority, "Advice, Initial Coin Offerings and Crypto Assets", dated 9 January 2019, available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
3. *Cf.* Robby Houben, Alexander Snyers, "Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion", study at the request of the European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance, dated June 2018, available at http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.
4. *Cf.* Banco de Portugal's public statement regarding Bitcoin, dated 22 November 2013, available in Portuguese at https://www.bportugal.pt/comunicado/esclarecimento-do-banco-de-portugal-sobre-bitcoin.

5. *Cf.* Banco de Portugal's warning regarding the risks associated with cryptocurrencies, dated 3 October 2014, available in Portuguese at https://www.bportugal.pt/comunicado/alerta-aos-consumidores-para-os-riscos-de-utilizacao-de-moedas-virtuais.
6. *Cf.* CMVM's warning regarding the risks associated with ICOs, dated 3 November 2017, available in English at http://www.cmvm.pt/en/Comunicados/Comunicados/Pages/20180119.aspx.
7. *Cf.* CMVM's notice regarding the cryptocurrency Bityond, dated 17 May 2018, available in Portuguese at http://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20180517a.aspx.
8. *Cf.* CMVM's notice regarding risks of "virtual currencies", dated 5 July 2018, available in Portuguese at http://www.cmvm.pt/pt/CMVM/CNSF/ConselhoNacionalDeSupervisoresFinanceiros/Pages/20180705.aspx.
9. CMVM's notice addressed to all entities involved in ICOs, dated 23 July 2018, available in Portuguese at http://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20180723a.aspx?v=.
10. *Cf.* Banco de Portugal's Circular Letter no. 11/2015/DPG, dated 10 March 2015, *Recommendation relating to the buying, holding and selling virtual currencies*, available in Portuguese at https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/11-2015-dpg.pdf.
11. *Cf.* European Securities and Markets Authority, Statement "ESMA alerts firms involved in *Initial Coin Offerings* (ICOs) to the need to meet relevant regulatory requirements", dated 13 November 2017, available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.
12. See endnote 2 above.
13. *Cf.* Autoridade Tributária e Aduaneira, Binding Information provided in process no. 5717/2015, dated 27 December 2016.
14. *Cf.* Autoridade Tributária e Aduaneira, Binding Information provided in process no. 12904, dated 15 February 2018.
15. Law no. 83/2017, of August 18, transposing Directives 2015/849/EU, of the European Parliament and of the Council, of May 20, and 2016/2258/EU, of the Council, of December 6.
16. *Cf.* Article 15 of Law no. 83/2017.
17. *Cf.* Article 36 (5) and Annex III of Law no. 83/2017.
18. *Cf.* European Banking Authority, *EBA Opinion on 'virtual currencies'* (EBA/Op/2014/08), 4 July 2014, available at https://www.eba.europa.eu/.
19. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

Filipe Lowndes Marques
Tel: +351 213 817 400 / Email: flmarques@mlgts.pt

Filipe Lowndes Marques joined the firm in 2001. He is the coordinator of the banking and finance department and the restructuring & insolvency department.
Filipe has worked since 1995 in the area of loan and bond finance, representing lenders and borrowers, including restructurings of existing financings. In the project finance sector, he has worked on several types of project, including bridges, motorways, power plants, wind and solar farms, football stadia, LNG terminals and natural gas concessions.
He has also been active in the field of capital markets, having advised on several securitisation transactions (including the first securitisation transaction under the new law and the first synthetic securitisation), covered bonds issuances and worked on several IPOs of state-owned companies.
His investment fund team was considered by *Chambers Europe* as "Portugal's top practice in investment funds".

Mariana Albuquerque
Tel: +351 213 817 400 / Email: msalbuquerque@mlgts.pt

Mariana Albuquerque joined the firm in 2014. She is a member of the banking and finance team and of Team Genesis.
She develops her work primarily in the area of banking and finance law, with a special focus on compliance by providing legal advice and consultancy with regard to the regulation and supervision of banks and other financial institutions, in payment services, in securitisation transactions, in negotiating derivatives and other financial instruments, in structured finance, in corporate finance and project finance transactions.
As a member of Team Genesis, Mariana Albuquerque works primarily with Fintech- and Regtech-related subjects.

João Lima da Silva
Tel: +351 213 817 400 / Email: jlsilva@mlgts.pt

João Lima da Silva joined the firm in September 2014. He is a member of the banking and finance team, as well as of the private equity & investment funds team.
João develops his work primarily in the area of banking and finance law, with special focus in structure finance, project finance, debt restructuring, debt issues, credit facilities and non-performing loans transactions. João also regularly works in transactions involving investment funds and provides legal advice to management companies.
He also provides legal advice with regard to compliance and the regulation and supervision of banks and other financial institutions, most notably in the investment and payment services sector.

Morais Leitão, Galvão Teles, Soares da Silva & Associados
[Morais Leitão]

Rua Castilho 165, 1070-050 Lisbon, Portugal
Tel: +351 213 817 400 / URL: www.mlgts.pt/pt

Russia

Vasilisa Strizh, Dmitry Dmitriev & Anastasia Kiseleva
Morgan, Lewis & Bockius LLP

Government attitude and definition

In sum, cryptocurrencies are used in Russia in various contexts including as payment for goods or services or as some instrument analogous to securities. Despite the generally welcoming attitude of the government towards blockchain as a technology, Russian authorities continue to stand against cryptocurrencies due to the generally non-transparent nature of transactions with cryptocurrencies and the associated compliance and similar risks.

The Russian Civil Code was recently amended to introduce the notion of "digital rights", though there are still no laws that directly govern cryptocurrency. Russian legislators have been working on a set of laws to govern a special category of digital rights – so-called "digital financial assets" – in an attempt to bring regulation to token and coin offerings and transactions with these assets.

For several years, the Russian authorities have been giving attention to potential uses of blockchain technology and cryptocurrencies. The focus has been on compliance and anti-corruption and anti-money laundering measures. The Central Bank of the Russian Federation (the Bank of Russia) and the Ministry of Finance of the Russian Federation (the Ministry of Finance) are the key regulators that have paid specific attention to these issues.

There is no law at present that specifically allows cryptocurrencies, and there is no legal definition of cryptocurrency. On the contrary, there are laws that might be viewed as prohibiting cryptocurrencies in Russia. For example, under the Russian Constitution, the rouble is the only means of payment in Russia. Further, under the Federal Law on the Central Bank of the Russian Federation of 2002, the rouble is the only national currency, and the introduction of other currencies or the issuance of currency surrogates on the Russian territory is prohibited. Cryptocurrencies may fall under such prohibited currency surrogates. Moreover, a Deputy Minister of Finance recently expressed[1] a view that cryptocurrencies will be prohibited as a means of payment in the nearest future.

Further, there is a view that the use of cryptocurrencies is associated with illegal activities. In January 2014, the Bank of Russia issued an information letter[2] warning that the trading in goods or services for "virtual currencies", as well as the conversion of such currencies to *roubles* or foreign currencies, could be used for money laundering and terrorist financing. Therefore, any transactions involving cryptocurrencies are subject to heightened scrutiny.

In February 2019, the Russian Supreme Court amended a Supreme Court Plenum decree (a judicial act serving as guidance for lower courts) on court practice on crimes related to money laundering. The Supreme Court explicitly stated that virtual assets (cryptocurrencies) acquired as a result of crime-committing activity could be viewed as objects of crimes punishable under article 174 (*on legalization (laundering) of funds and other property illegally*

acquired by other persons) and article 174.1 (*on legalization (laundering) of funds and other property acquired by other persons by committing a crime*)[3] of the Russian Criminal Code. The Supreme Court specifically noted that this amendment is in line with FATF Recommendation 15: New Technologies.

There have been attempts to bring direct regulation to cryptocurrency. For example, the State Duma has adopted in the first reading a draft law on digital financial assets (see section "*Cryptocurrency regulation*" for further details). One of the initial versions of this draft proposed definitions of a "token", "cryptocurrency", and an umbrella definition for both tokens and cryptocurrency – a "digital financial asset". Now the draft uses an umbrella "digital financial asset" definition only.

Similarly to cryptocurrencies, there is no law at present specifically addressing blockchain technologies. However, the authorities do not view blockchain negatively. On the contrary, the use of blockchain technologies for the formation and implementation of "smart contracts" is of great interest in Russia. The Civil Code was recently amended to apply to smart contracts. Still, in many respects, Russia remains a tradition-bound market in which physical documents are essential. In particular, the transition to distributed ledger systems and virtual contracts will conflict with existing, centralised registers that are now legally required for certain activities and transactions.

Russia is moving toward digitalisation of many services and functions that government agencies perform. Governmental authorities are in the process of modernising their operations, allowing filings and document exchange via online platforms – including, for example, filing of tax declarations, accounting reports and licence and patent applications. These include the Federal Tax Service, the Federal Service for Intellectual Property, and the Federal Service for Supervision of Communications, Information Technology and Mass Media. Notary filings may be submitted electronically, and the register of the companies is also accessible online.

Cryptocurrency regulation

The Russian Civil Code was amended by a law "On Introduction of Changes to Parts One, Two and Four of the Civil Code of the Russian Federation" dated 18 March 2019; this law is commonly referred to as the **Digital Rights Law**, as it introduced the notion of "digital rights" and the regulation to cover smart contracts, and certain other rules. The amendments are in force from 1 October 2019. The Digital Rights Law appears to be the first attempt to adopt regulations covering cryptocurrencies although not naming them directly as such.

The Digital Rights Law introduces new article 141.1 to the Civil Code. Article 141.1 broadly defines "digital rights" as rights under obligations and other rights, named as such in the law, the contents and conditions for exercising of which are determined by the rules of an informational system which must comply with the requirements of the law.

The Digital Rights Law also amends article 128 of the Civil Code on the so-called "objects of civil rights", i.e., objects which could be subject to civil law entitlements and transactions. Such objects are things, including cash and certificated securities; other property including property rights which now will include digital rights in addition to non-cash money and book-entry securities; results of works and services; protected results of intellectual activity and means of individualisation equated to them (intellectual property); and intangible benefits. Therefore, the Civil Code recognises that digital rights are assets which could be owned, sold, purchased, encumbered or otherwise transacted with. Although the Digital Rights Law does not explicitly address cryptocurrencies, the digital rights definition is broad enough to cover many kinds of digital assets including coins and tokens.

The Digital Rights Law also amended articles 160 and 309 of the Civil Code governing the rules on fulfilment of obligations and forms of agreements. These articles (as amended) will allow the parties to enter into transactions using "electronic and other technical means" and to include a condition on fulfilment of the agreed terms automatically with the use of informational technologies, agreed upon by the parties, i.e., by using smart contracts, although the Digital Rights Law does not use the word "smart contract".

There are initiatives to address cryptocurrencies and related matters:

- A draft law "On Digital Financial Assets" that would introduce certain key rules with respect to issuance, offering or otherwise transacting with tokens including initial token offerings (also known as initial coin offerings or ICOs) and their exchange (the **Digital Financial Assets Law**).
- A draft law "On Attracting Investments with the Use of Investment Platforms" that would introduce regulation for crowdfunding activities including those involving token sales (the **Draft Investment Platforms Law**, and together with the Digital Financial Assets Law, the **Draft Laws**).

Unfortunately, at this stage, the Draft Laws do not seem to be fully aligned with the Digital Rights Law, and their future status is not clear.

Sales regulation

The Digital Rights Law has amended the provisions of the Civil Code on objects of civil rights to list digital rights together with non-cash funds and book-entry securities. It means that from 1 October 2019 (the date of entry of this law into force), generally speaking, digital rights could be sold and bought and otherwise transacted with like non-cash funds on bank accounts or book-entry securities.

An important law to govern transactions with the digital assets would be the Digital Financial Assets Law if adopted. There were several drafts of this law already. Reportedly, the Digital Financial Assets Law is set to be adopted by the State Duma in 2019. The second reading has been postponed few times already: there are ongoing debates over the concept of cryptocurrencies and on whether they must be banned instead.[4] Notably, the most recent version of the draft Digital Financial Assets Law (the **Temporary Draft**) was publicly available at the State Duma website at http://sozd.parliament.gov.ru/ for a short period of time, and was removed from this website with no updated draft available yet.

The Temporary Draft suggests that digital financial assets are subject to strict regulation. For example, under the Temporary Draft, digital financial assets may be exchanged only for traditional currencies (*roubles* or foreign currency) through the so-called "operators of digital financial assets trade" (the digital asset trade operators). The Temporary Draft proposes that only special categories of Russian entities can be digital asset trade operators. These include Russian licensed credit organisations (e.g., banks) and organisers of trade (e.g., securities exchanges).

In addition to digital asset trade operators, the Digital Financial Assets Law also introduced the concept of operators of informational systems that will be used for issuing digital financial assets (the information system operators). The information system operators must be Russian legal entities and must be included in a register maintained by the Bank of Russia.

The Temporary Draft proposes to introduce rules for issuing and offering digital financial assets. Broadly speaking, these rules mimic the existing rules governing securities issuance and offering and require adopting and publicly disclosing a decision on issuance of digital financial assets.

It is proposed that a decision on issuance of digital financial assets must include (among others) information on the issuer of the digital financial assets including its ultimate beneficial owners, the type and scope of rights that the digital financial assets represent, an indication on whether smart contracts are used to sell and purchase the financial assets, and information on whether the issuer's liability is limited.

Taxation

Despite there being no special rules on the taxation of transactions with cryptocurrencies, the Tax Code of the Russian Federation applies to them.

Recently, the Ministry of Finance expressed a view that all profits from operations with cryptocurrencies should be subject to personal income tax, and issued two information letters in May[5] and July[6] 2018 (the **Letters**).

In these Letters, the Ministry of Finance specifically noted, among other things, that any economic benefit derived from transactions with cryptocurrencies is taxable and taxpayers must pay income tax (the tax imposed by the Tax Code); the tax base from cryptocurrency sale and purchase transactions should be determined in roubles as a surplus of income received by the taxpayer from the sale of cryptocurrencies over the total amount of expenditures for the purchase of cryptocurrencies; and the taxpayer must calculate the amount of tax to be paid and file the tax declaration himself.

Money transmission laws and anti-money laundering requirements

The key laws governing anti-money laundering (**AML**) rules in Russia are Federal Law No. 115-FZ "On Counteracting Legalization (Laundering) of Illegal Income and Terrorism Financing", dated 7 August 2001 (the **AML Law**) and a set of subordinate regulation adopted by the Government of the Russian Federation, the Federal Financial Monitoring Service, the Bank of Russia, the Federal Tax Service and other governmental bodies responsible for implementation of the AML legislation.

There is no express cryptocurrency-related AML legislation currently in force. The Temporary Draft proposed to amend the AML Law to include digital asset trade operators and informational system operators to the list of persons subject to the AML Law. For example, they would be required to:

- identify a client by obtaining, verifying and periodically updating and verifying certain information on the client, its directors and ultimate beneficial owners;
- check a client on involvement in extremist or terrorist activities;
- adopt internal controls including developing rules of internal controls and compliance programs; and
- report suspicious transactions to the AML enforcement authorities.

In September 2017, the Bank of Russia issued an information letter[7] warning about possible illegality and associated risks of transactions with cryptocurrencies. The Bank of Russia noted that cryptocurrencies were issued by anonymous and unidentifiable persons and, therefore, in transacting with cryptocurrencies, persons may become involved in illegal activities, including money laundering and terrorist financing. The Bank of Russia warned that cryptocurrencies entailed high-level risks, both when issuing cryptocurrency and tokens in initial token or coin offerings, as well as later, during exchange operations. The Bank of Russia further emphasised that it believed that "admission of cryptocurrencies and other

financial instruments nominated in or related to cryptocurrencies, to circulation and use in organised trading as well as in clearing and settlement infrastructure for servicing transactions with cryptocurrencies and related derivatives in Russia", is premature.

Promotion and testing

The Russian Government and the Bank of Russia have launched or announced several initiatives to support the development of blockchain technologies while keeping a watchful eye on the cryptocurrency market, including several working groups involving representatives of the Bank of Russia and business community.

In 2017, the Russian President issued an order[8] for the Russian Government and the Bank of Russia to create a regulatory sandbox for testing various innovative financial technologies. The Bank of Russia created the sandbox in April 2018.[9] It allows innovative start-ups to test their technologies without running a risk of violating current legislative restrictions.

To develop the regulatory sandbox concept, the Russian Ministry of Economic Development has presented a draft law under a working title "On Experimental Legal Regimes in the Sphere of Digital Innovations in the Russian Federation". This draft law aims at introducing relaxed AML rules, a fixed tax regime and carve-outs from certain existing regulations, to allow testing new technologies in projects which qualify for participation in the so-called digital innovations programmes. Reportedly, this draft law may be introduced to the State Duma in the autumn of 2019.

Russian organisations are also becoming increasingly active in the blockchain sphere. The National Settlement Depository, Russia's central securities depository, has initiated a pilot e-proxy shareholder voting[10] project using a blockchain solution, and has already serviced several blockchain-backed commercial bond offerings.[11]

Ownership and licensing requirements

The Digital Rights Law confirms that digital assets can be owned. It contains no specific restrictions and does not call for any licence. The Draft Laws have no provision to the contrary, save that certain entities through which financial digital assets are exchanged, such as digital asset trade operators and informational system operators, must be Russian entities, either licensed by or registered with the Bank of Russia (see section "*Sales regulation*" for further details).

Further, as regards investments, the Draft Investment Platforms Law proposes to introduce a concept of the "investment platform". An investment platform would be defined as an information system in the information-telecommunication network on the internet, that is used for concluding contracts with the use of information technologies and technical features of the investment platform by means of which investments are attracted, and which is also available as a mobile application. Only a Russian legal entity included by the Bank of Russia into a register of operators of investment platforms may be the operator of an investment platform.

Mining

Compared to the initial versions, the Draft Laws currently do not introduce the definitions of "mining" or any regulation for similar activities. There is certain existing legislation that may apply to mining activities. For example, certain hardware used in mining activities may be viewed as devices containing encryption and cryptographic tools. The use and distribution

of such devices may be subject to import restrictions as well as licensing by the Federal Security Service or the Ministry of Industries and Trade.

Border restrictions and declaration

At the moment, the existing laws and initiatives do not provide for any border restrictions or obligations to declare cryptocurrency holdings when entering or exiting Russia.

Reporting requirements

At present, there is no specific regulation with respect to cryptocurrency reporting requirements for individuals or legal entities. However, the issue of reporting has been discussed in the context of Russian anti-corruption laws, requiring public and governmental officials to report on their property and other holdings. These discussions are also associated with another important legal issue: whether cryptocurrency is property. Previously, the Ministry of Labour and Social Security of the Russian Federation issued the reporting guidelines[12] in which it specifically advised that public and government officials are not obliged to disclose ownership of "*virtual currencies*", in contrast to rather strict reporting obligations in relation to their assets and funds on bank accounts. In other words, these guidelines assumed that *virtual currencies* are not property.

The Digital Rights Law resolves this issue: from 1 October 2019, digital assets are property (and cryptocurrency will most likely be viewed as a type of digital assets).

Notably, even before the Digital Rights Law, cryptocurrency was viewed as property at least in the bankruptcy context. Russian courts were already facing questions regarding the nature of cryptocurrencies and their exposure against creditor claims. For example, the Moscow appellate court has ruled[13] that the concept of "*other property*" as set forth by the Civil Code of the Russian Federation could be interpreted to include cryptocurrency. Therefore, cryptocurrency should be included into the insolvency estate of the debtor along with other property. The court obliged the debtor to disclose his password to give the insolvency manager access to the debtor's cryptocurrency wallet.

Estate planning and testamentary succession

At present, there are no special rules on succession of cryptocurrency. Still, the rules on succession of the Civil Code generally apply, subject to the below considerations. Under the general rules of the Civil Code, cryptocurrency (digital assets) could be recognised as an estate property. However, given that access to cryptocurrency assets is restricted to persons having a code or specific "unique access", certain steps should be taken by a person to ensure that the cryptocurrency will be passed to heirs.

Cryptocurrency has two crucial features that prevent existing legal structures from being applicable to the succession of cryptocurrency: (1) that the identity of a cryptocurrency owner is not generally revealed to third parties; and (2) that the cryptocurrency owner is neither shown in any certificate or other document nor listed in any register.

Therefore, one needs to create an action plan to enable to include a person's cryptocurrency assets to the estate. In essence, a person needs to set up a structure allowing heirs to inherit, in addition to digital assets themselves, a tangible medium (a piece of property) containing the information allowing access to a cryptocurrency wallet and transaction with the cryptocurrencies stored in it. For example, the person can do as follows. First, determine what information is required to get access to the wallet and transactions with the

cryptocurrencies such as, for example, a login and password to a website, a secret question or a key (code). Secondly, fix such information on a physical storage device such as, for example, a USB flash drive, a compact disk, a paper note. A physical storage device would be a piece of property that could be inherited too, including by default. Under the Civil Code, estate includes assets and other property, including property rights and liabilities owned by the deceased as of the date of opening of the inheritance. These steps are relevant only if there are no laws addressing the issue. It is possible that once the cryptocurrency is expressly allowed in Russia, inheritance laws might be amended to deal with cryptocurrencies directly.

* * *

Endnotes

1. https://rns.online/finance/Minfin-isklyuchil-vozmozhnost-rascheta-kriptovalyutami-v-Rossii—2019-07-01/.
2. https://www.cbr.ru/press/PR/?file=27012014_1825052.htm.
3. https://www.rbc.ru/society/26/02/2019/5c74f3fa9a7947500e19cd24.
4. https://www.pnp.ru/economics/prinyatie-zakona-o-cifrovykh-finansovykh-aktivakh-mogut-perenesti-na-osen.html.
5. Letter of the Ministry of Finance No. 03-04-07/33234 of 17 May 2018, https://www.nalog.ru/html/sites/www.new.nalog.ru/docs/minfin/03040733234.pdf.
6. Letter of the Ministry of Finance No. 03-04-05/48714 of 12 July 2018, https://normativ.kontur.ru/document?moduleId=8&documentId=317281.
7. Information Letter of the Bank of Russia "On Using Private 'Virtual Currencies' (Cryptocurrency)" of 4 September 2017, https://www.cbr.ru/press/pr/?file=04092017_183512if2017-09-04T18_31_05.htm.
8. https://lenta.ru/news/2017/10/24/crypto/ and http://kremlin.ru/acts/assignments/orders/55899.
9. https://www.cbr.ru/fintech/regulatory_platform/.
10. https://www.nsd.ru/common/img/uploaded/files/gm_proxy_voting.pdf.
11. https://www.nsd.ru/en/press/ndcnews/index.php?id36=633749.
12. Methodical Recommendations on Issues of Reporting Information on Income, Expenditures, Property and Property Liabilities and on Filling out of the Respective Type of Certificate, of 16 May 2017.
13. Decision of the 9th Arbitrazh Appellate Court in Case No. A40-124668/2017, dated 15 May 2018.

Vasilisa Strizh, Partner
Tel: +7 495 212 2540 / Email: vasilisa.strizh@morganlewis.com

Vasilisa represents global and domestic strategic and financial investors across multiple industries, including financial services, mass media and telecommunications, energy, and pharmaceuticals and life sciences. Vasilisa's practice focuses on cross-border investment, joint venture, and merger and acquisition transactions. Vasilisa also counsels on corporate governance and compliance and advises on capital market transactions and related regulatory matters. She has served as lead lawyer on complex corporate projects, including acquisitions, divestitures and joint ventures, public and private equity offerings, financing, and structured settlements. She participated in a project for the Russian central securities depository on the Russian corporate reform to allow paperless shareholder meetings, electronic voting, settlements through the central securities depository and disclosures via the centre of corporate information.

Vasilisa serves as the Managing Partner of the Moscow office.

Dmitry Dmitriev, Associate
Tel: +7 495 212 2574 / Email: dmitry.dmitriev@morganlewis.com

Dmitry represents domestic and international companies across multiple industries, such as media, energy, retail, and financial services in mergers, acquisitions, and joint venture transactions as well as in general corporate matters and real estate transactions. On an ongoing basis, he also counsels clients on virtually all regulatory aspects of employment relations, including issues of personnel mobility, executive compensation, long-term incentive (LTI) programs and a variety of personnel issues arising in M&A transactions. He is also actively involved in the global Fintech industry working group at Morgan Lewis and regularly co-authors publications related to legal developments in the blockchain and cryptocurrency industries in Russia.

Anastasia Kiseleva, Associate
Tel: +7 495 212 2568 / Email: anastasia.kiseleva@morganlewis.com

With a focus on telecommunications, media, entertainment, and technology industries, Anastasia represents international and Russian companies in transactions relating to joint ventures, mergers and acquisitions, technology and IP licensing, distribution arrangements, as well as in general corporate and commercial matters. Anastasia also advises on: various regulatory aspects of mass media and IT businesses; use and protection of intellectual property; production and distribution of motion pictures in Russia; corporate governance and compliance matters; e-commerce; advertising; and outsourcing. Anastasia actively follows new initiatives in media and technology industries, including related to cryptocurrency and blockchain matters, and regularly participates in the firm's related activities, such as publications on the Morgan Lewis tech & sourcing blog.

Morgan, Lewis & Bockius LLP

Legend Business Center, Tsvetnoy Bulvar, 2, Moscow 127051, Russia
Tel: +7 495 212 2500 / Fax: +7 495 212 2400 / URL: www.morganlewis.com

Serbia

Bojan Rajić & Mina Mihaljčić
Moravčević Vojnović i Partneri AOD Beograd in cooperation with Schoenherr

Government attitude and definition

In March 2019, the Securities Commission of Serbia ("Commission") issued a Statement on regulation of crypto-assets in the Republic of Serbia ("Statement"), under which the Commission, in cooperation with the Office of Prime Minister, launched a public consultation process on the regulation of crypto-assets in Serbia. Here it should be noted, though the Statement is not considered an official opinion of the Commission, it reflects its current understanding and position on the matter.

Since there is a lack of clarity as to how the Serbian regulatory framework applies to crypto-assets, such instruments raise specific challenges for regulators and market participants. The Commission's current position is that the development of crypto-assets does not currently raise financial stability issues. Such opinion is in line with the paper issued by the European Securities and Market Authority ("ESMA") in its Advice Paper (*Initial Coins Offerings and Crypto-Assets*), issued on 9 January 2019. Also, the Commission has noted that the IT industry in Serbia is on the rise and in order to support the development of the industry, it is necessary to ensure legal certainty. The Commission believes that this could be achieved by establishment of the competent institutions regarding crypto-assets, but also by application of the existing regulations where appropriate. However, there is also a concern about the risks that could affect the Serbian market or prospective investors.

In its Statement, the Commission outlined its position on the gaps and issues that exist in the rules when crypto-assets qualify as financial instruments and the risks that can arise when crypto-assets do not qualify as financial instruments.

The Commission believes that crypto-assets that can be qualified as one of the financial instruments under Article 2 (1) of the Capital Markets Act (*Official Gazette of RS, nos 31/2011, 112/2015 and 108/2016*) ("CMA") are regulated by Serbian law and fall within the Commission's remit.

Accordingly, the Commission defines the criteria for determining whether a crypto-asset could be qualified as a financial instrument or not. Taking into account the definition of *transferable securities* as defined in the CMA, a crypto-asset would have the features of a transferable security if it: (i) were not used for purchasing goods and services; (ii) were negotiable on the capital market; and (iii) were to include at least one of the following: (A) right to a participation in the issuer's capital or voting rights; (B) right to register the rights defined under item (A) with the relevant public register; (C) right to receive remaining assets (liquidation proceedings); (D) right to a claim from the issuer determined as a fixed sum with a maturity of more than 397 days of the day of issue; (E) right to register the rights defined under item (D) with the relevant public register; (F) right to acquire securities; and/or

(G) right to a claim from the issuer determined by reference to transferable securities, currencies, interest rates, incomes, commodities, indices or other measures.

The Commission's preliminary view is that where crypto-assets qualify as financial instruments, the regulatory framework stipulated by the CMA should apply to them and to all transactions with respect to the crypto-assets. In such case, the provisions on prospectuses, reporting and rules on secondary trading have to be applied as well. So, IT companies dealing with such crypto-assets must satisfy all provided conditions and obligations required for issuers of financial instruments. This is particularly applicable to so-called "investment tokens"; i.e. digital tokens with an investment/speculative purpose, which are considered as already regulated financial instruments issued in the new form, through new blockchain technology.

On the other hand, in cases where crypto-assets do not qualify as financial instruments, the Commission took the position that the existing Serbian legislation cannot be applied directly. The legal framework proposed by the Commission for this type of crypto-assets is similar to the system for issuing and trading in financial instruments established by the CMA and European Union directives. In this regard, the Commission believes that Serbia has an opportunity to adopt a straightforward regulatory framework – which could have a positive impact on the development of IT sector.

In this regard, the Commission has proposed the following significant features of the prospective legal framework:

- the Commission would license agents providing professional services with respect to crypto-assets, and the issuers of crypto-assets would be required to conclude an agreement with such agent. Also, the agents would provide advice to issuers in relation to their obligations, represent them before the regulatory authority and file the required reports with the regulatory authority, etc. The agents would have an important role in the prevention of money laundering and terrorism financing;
- the issuer should publish a whitepaper at least 10 days before a crypto-asset has been issued. The whitepaper would be signed by management members of an issuer and would contain the prescribed information. These documents should be similar to a prospectus regulated under the CMA regarding securities, only simpler; and
- anyone who intends to provide services in relation to issuing/trading in crypto-assets will be required to hold a licence issued by the Commission. The services include organisation of trading, receipt and execution of orders, custody services, providing investment advice, portfolio management, etc.

The above overview of the prospective legal framework is not exhaustive but rather highlights some its key features.

In a separate instance, the Serbian central bank – the National Bank of Serbia ("NBS") – took a position on whether cryptocurrencies can be considered currencies. Namely, on 3 November 2017 NBS issued an official opinion on cryptocurrencies pursuant to which it confirmed that cryptocurrencies are not considered currencies under Serbian law. Accordingly, the trading of cryptocurrencies and platforms for internet trading of cryptocurrencies are not subject to NBS supervision. The exceptions to this are matters with regard to the anti-money laundering regulations, where NBS explicitly recognised its supervising authority (please see "Money transmission laws and anti-money laundering requirements" below).

NBS further emphasised its concern about the risks Bitcoin poses to cryptocurrencies users, and also issued a separate warning stating that anyone involved in virtual currency activities is doing so on its own responsibility, bearing its own financial risk.

Cryptocurrency regulation

While Serbian law does not prohibit cryptocurrencies, there is currently no specific legislation applicable to cryptocurrencies either. However, in the last two years, different proposals for governing cryptocurrencies and related matters have been published (please see "Government attitude and definition" above).

Sales regulation

In cases where cryptocurrencies can be qualified as financial instruments (for details, please see "Government attitude and definition" above), the provisions of the CMA must be applied on the sale process. On the other hand, in cases where cryptocurrencies do not qualify as financial instruments, the general civil law rules (particularly the Serbian Obligation Act) would apply.

However, it should be noted that, at this time, cryptocurrencies have not yet been explicitly qualified as securities, nor are they subject to the CMA.

Taxation

Serbia has not enacted any specific tax regulation concerning cryptocurrencies. Accordingly, Serbian tax rules do not include any special tax rules for income, profits or gains arising from transactions arising from transaction involving cryptocurrencies.

So far, the Serbian Ministry of Finance has issued only one opinion on cryptocurrencies, following the opinion of NBS, pursuant to which cryptocurrencies, and in particular Bitcoin, are not considered currencies under the Serbian law (referred to under "Government attitude and definition" above).

Following the opinion given by the Serbian central bank, on 26 November 2017 the Ministry of Finance of RS issued its opinion no. 413-00-168/2017-04, referring to Article 25(1)1) of the Value-Added Tax Act (*RS Official Gazette, 84/2004, 86/2004, 61/2005, 61/2007, 93/12, 108/13, 68/14, 142/14, 83/15, 108/16*), which prescribes a tax exemption without the right to deduct input VAT on transactions concerning legal means of payment (legal tender), which cannot be applied to the trade of Bitcoin, as Bitcoin does not represent a form of legal payment in Serbia. Hence, the sale of cryptocurrencies is not subject to VAT in Serbia.

When considering whether cryptocurrencies are subject to income tax, the situation is not clear-cut. Namely, the Individual Income Tax Act does not specify cryptocurrencies as a revenue source subject to income tax. However, the mentioned Act contains a general provision pursuant to which "other revenues" subject to income tax can be "all other revenues not subject to taxes on the basis of other laws or which are not freed from taxes or free from paying taxes on the basis of the Act". Consequently, it should be considered that income arising from the sale of cryptocurrencies, just as that arising from the sale of other assets, can be considered subject to personal income tax (which would in this case be 20%).

Money transmission laws and anti-money laundering requirements

Although crypto-assets are not regulated in the Serbian legal system, provisions of the Law

on Prevention of Money Laundering and Terrorism Financing (*RS Official Gazette, no. 113/2017*) ("AML Act") already cover crypto-assets to a significant extent; i.e. there are grounds for interpretation of the current rules to be applicable to crypto-assets.

Also, the Serbian Criminal Code (*RS Official Gazette, nos 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019*) ("Criminal Code") sanctions the crime of money laundering. Namely, under the Criminal Code:

> "*The one who converts or transfers assets while aware that such assets originate from a criminal activity, with intent to conceal or misrepresent the unlawful origin of the assets, or conceals and misrepresents facts on the assets while aware that such assets originate from a criminal activity, or obtains, keeps or uses assets with the intent, at the moment of receiving, that such assets originate from a criminal activity, shall be punished by imprisonment of six months to five years and a fine.*"

The Commission believes that the term "asset" can be interpreted to include crypto-assets, so the Criminal Code regulates laundering of crypto-assets as a criminal activity as described.

Additionally, the AML Act stipulates that NBS supervises legal persons and individuals that provide services in relation to virtual currencies. The AML Act does not define the term "virtual currency" and the word "currency" implies only cryptocurrencies and not other types of crypto-asset.

Promotion and testing

At the time of writing, we are not aware of any public "sandbox" or other programmes aimed at specifically promoting research or investment into cryptocurrencies in Serbia.

However, there are various initiatives in the private sector in Serbia which directly or indirectly promote blockchain technologies.

Ownership and licensing requirements

If the cryptocurrencies are used as financial instruments, they will be subject to stock market regulation.

At the time of writing, there are no specific licensing requirements imposed on an investment advisor or fund manager holding cryptocurrencies.

Mining

Mining of cryptocurrencies is not subject to regulation in Serbia. It is not prohibited as such; however, there are no rules which regulate under which conditions and how mining activities can be undertaken. It can hence be deduced that mining is currently permitted in Serbia. Also, no authority has yet assumed the mining of cryptocurrencies as falling under its (explicit) supervision.

Publicly available information and media reports suggest that mining activities are indeed undertaken in Serbia, although they do not appear to be wide-spread.

Border restrictions and declaration

There are currently no border restrictions or obligations to declare cryptocurrency holdings under Serbian law.

Reporting requirements

There are currently no specific reporting requirements aimed at cryptocurrency payments made in excess of a certain value under Serbian law.

However, it should be presumed that general AML rules may also be applicable to cryptocurrency and blockchain transactions, i.e. that certain AML requirements apply irrespective of the transaction being made in cryptocurrencies or via blockchain (e.g. identification and reporting of activities suspected of money laundering or terrorism financing).

Estate planning and testamentary succession

There are no specific rules as to how cryptocurrencies are treated for purposes of estate planning and testamentary succession.

Even though cryptocurrencies are not explicitly subject to civil law in Serbia, cryptocurrencies could be qualified as intangible assets from a Serbian civil law perspective. As such, they do not differ from ordinary assets and can be included in estate planning and testamentary succession.

Bojan Rajić
Tel: +381 11 3202 600 / Email: b.rajic@schoenherr.rs

Bojan Rajić is an attorney at law specialising in corporate/M&A. Bojan advises international clients on their market entry and is a member of the team that provides full-service transactional support in the implementation of their investments. Bojan is a specialist for contracts and investments incentives. Most recently, Bojan advised on the sale of an innovative technologies developer from Serbia to Epic Games. He also advised Telenor ASA on the largest telecoms M&A transaction ever in the CEE region, the sale of its subsidiaries in Serbia, Hungary, Bulgaria and Montenegro to PFF Group for EUR 2.8 billion. He is engaged in different sectors and industries, including IT, media, banking and finance, automotive, pharmaceuticals, energy and infrastructure. Bojan acted as a legal counsel and provided all M&A, regulatory and general corporate services to Solelos (formerly Gamecredits), an IT company operating various blockchain-based and cryptocurrency projects.

Mina Mihaljčić
Tel: +381 11 3202 600 / Email: m.mihaljcic@schoenherr.rs

Mina Mihaljčić has been an associate with the firm since 2017. She specialises in Corporate/M&A. She has advised clients in IT, telecommunications, banking and finance and packaging industries. Most recently she advised on the sale of an innovative technologies developer from Serbia to Epic Games, and the leading telecom operator on the acquisition of a major cable television, broadband internet and mobile service provider. Mina acted as legal counsel and provided all M&A, regulatory and general corporate services to Solelos (formerly Gamecredits), an IT company operating various blockchain-based and cryptocurrency projects.

Moravčević Vojnović i Partneri AOD Beograd in cooperation with Schoenherr

Dobračina 15, 11000 Belgrade, Serbia
Tel: +381 113 202 600 / URL: www.schoenherr.rs

Singapore

Franca Ciambella & En-Lai Chong
Consilium Law Corporation

Government attitude and definition

Singapore is commonly referred to as one of the world's "cryptohavens", not only because it is a world financial centre, but also as a result of its balanced legal and regulatory regime fostered by the Monetary Authority of Singapore ("MAS"). Acting as the central bank and as the financial regulating body, MAS' approach is to regulate the space to prevent stifling innovation, while simultaneously protecting investors and the public at large.

The government has not defined a virtual currency (used interchangeably with "cryptocurrency" or "token" or "coin" unless otherwise specified) to be one exclusive thing, but instead has stated the following: (a) they are not a currency or legal tender issued by any government; (b) they are to be encouraged as a means of paying for goods or services to someone who is willing to accept them as a mode of payment, and are a means of making payments; (c) they cannot be a store of value, as their prices fluctuate (in this regard, the government attitude is to not encourage people to use them as an investment tool as they are risky); and (d) they are recognised as assets and personal property, with more and more people trading in them.

Justice Simon Thorley, IJ, held that cryptocurrencies are assets in *B2C2 Ltd v. Quoine Pte Ltd* [2019] SGHC(I) 03, a matter heard in the Singapore International Commercial Court.

Regarding blockchain technology, the government encourages its development, but says that this positive attitude does not mean it is necessarily encouraging cryptocurrencies. Cryptocurrencies are not the only application of blockchain technology; it has many other uses. Government confidence in blockchain technology is shown through its development of "Project Ubin".

Backed by MAS, Project Ubin is aimed at creating a digital token for the Singapore dollar on the Ethereum blockchain. Each ledger is supported by the equivalent amount of Singapore dollars held by the government, which will ensure that the overall money supply is not impacted by the token and has full redemption possibilities. The project is intended to make financial transactions cheaper and more efficient. Although the project is still in its early stages, it is a prime example of one of the ways that Singapore is seeking to have digital tokens backed by the government and central banks.

Cryptocurrency regulation

A virtual currency itself is not regulated in Singapore; however, the activities surrounding it or its characterisation resulting from its activity are what determine whether it will be regulated under securities or other legislation. This leaves the door wide open for tokens, for example, of a payment nature only, to be unlicensed, non-security tokens that can be sold

to the public without any licensing or MAS oversight using a simple set of sale terms and conditions. Moreover, in the analysis of the characterisation of a token, a key difference with other major jurisdictions is that it will not be considered a security simply because there will be some sort of crowd-funding or capital-raising activity. Instead, an in-depth analysis of whether it falls within the scope of securities law is required to determine its characterisation as a security or not, and any ensuing or other licensing or regulatory requirements.

A "legal opinion" on the characterisation of the token as falling within securities legislation, and any other licences that may be required, should be a first step. One reason for this is that unlike some other jurisdictions, regulators such as MAS will not get involved in this exercise and do not provide opinions or specific guidance on a particular situation.

This section will deal with the regulations surrounding Initial Coin Offerings ("ICOs") and Exchanges.

ICOs – Are they securities?

An ICO refers to the fund-raising process whereby digital tokens (or coins) are offered for sale online to the public in return for payment in a specified cryptocurrency or fiat. The tokens may or may not have utility functions. Some tokens serve as both fund-raising tools and tools that enable access and usage of the issuer's platform or eco-system, while some other tokens are solely fund-raising tools.

As will be examined below, some tokens may resemble securities, which raises the issue of whether Singapore's securities laws apply to certain ICOs. The implications of this issue are significant, as there are extensive laws and regulations governing the issuing of securities to the public, such as the registration of a prospectus, making conducting an offering of security tokens an onerous and costly endeavour to embark on.

MAS announced on 1 August 2017 that the offer or issue of digital tokens in Singapore will be regulated by MAS if the digital tokens constitute products regulated under the Securities and Futures Act (Cap.289, Rev. Ed), (hereinafter "SFA") or other securities legislation.

Where digital tokens fall within the definition of securities in the SFA, the offeror of the tokens would be required to lodge and register a prospectus with MAS prior to offering such tokens, unless otherwise exempted from such requirement.

In the analysis, the first issue to look into is the definition of securities, which may be found in the SFA. The term "Securities" is defined in Section 2(1) of the SFA. As follows:

> Section 2(1)
>
> *"securities" means —*
>
> *(a) shares, units in a business trust or any instrument conferring or representing a legal or beneficial ownership interest in a corporation, partnership or limited liability partnership;*
>
> *(b) debentures; or*
>
> *(c) any other product or class of products as may be prescribed,*
>
> *But does not include —*
>
> *(i) any unit of a collective investment scheme;*
>
> *(ii) any bill of exchange;*
>
> *(iii) any certificate of deposit issued by a bank or finance company, whether situated in Singapore or elsewhere; or*
>
> *(iv) such other product or class of products as may be prescribed;"*

Section 240(1) SFA requires that any offer of securities or securities-based derivatives contract must be made in, or accompanied by, a prospectus that complies with the statutory requirements in Section 243 SFA, has been signed and lodged with MAS, has been registered by MAS and complies with any other regulatory requirements that MAS may prescribe.

There are some exemptions from the requirement in Section 240(1) SFA, and Section 272B(1) SFA provides an exemption for private placements, if certain requirements are met. Such exemptions can be one of the following:

(a) the offers are made to no more than 50 persons within any period of 12 months;

(b) none of the offers is accompanied by an advertisement making or calling attention to the offer or intended offer;

(c) no selling or promotion expenses are incurred in connection with each offer other than those incurred for administrative or professional services, or by way of commission or fee for services rendered thereby; and

(d) no prospectus in respect of any of the offers has been registered by the Authority or where a prospectus has been registered.

While ICOs are typically offerings to the public, some issuers limit the sale of their tokens to private or institutional investors. Some issuers carry out both the private and public sale, with the former at an earlier stage, before proceeding with the latter.

The Singapore Parliament has passed the Payment Services Act ("PSA"); however, the PSA is not yet in force. The PSA, when in force, will regulate the purchase and sale of virtual currencies. Under the PSA, entities that carry out any of the following activities need to hold a licence and are subject to regulation:

(a) account sale services;

(b) domestic money transfer services;

(c) cross-border money transfer services;

(d) merchant acquisition services;

(e) e-money sale;

(f) virtual currency services; and

(g) money-changing services.

It is possible that the activities of ICO companies may fall under the categories of "e-money sale" and/or "virtual currency services", and it would be important to look into the application of the PSA after it is in force.

Exchanges

Once a coin is offered, it is typically traded on the market via an exchange. Markets, as defined in the SFA, are regulated according to Section 7 of the SFA:

> "*7.—(1) A person must not establish or operate an organised market, or hold itself out as operating an organised market, unless the person is —*
>
> *(a) an approved exchange; or*
>
> *(b) a recognised market operator.*
>
> *(2) A person must not hold itself out —*
>
> *(a) as an approved exchange, unless the person is an approved exchange; or*
>
> *(b) as a recognised market operator, unless the person is a recognised market operator.*

(3) Except with the written approval of the Authority, a person, other than an approved exchange or a recognised market operator, must not take or use, or have attached to or exhibited at any place —

(a) the title or description "securities exchange", "stock exchange", "futures exchange" or "derivatives exchange" in any language; or

(b) any title or description that resembles a title or description referred to in paragraph (a)."

A party would have to obtain the requisite approvals or licences from MAS in order to set up and operate an exchange. However, this is a costly process with no guarantee that MAS would grant such an approval or licence.

Part I of the First Schedule of the SFA, defines an "organised market" as:

(a) a place at which, or a facility (whether electronic or otherwise) by means of which, offers or invitations to exchange, sell or purchase derivatives contracts, securities or units in collective investment schemes, are regularly made on a centralised basis, being offers or invitations that are intended or may reasonably be expected to result, whether directly or indirectly, in the acceptance or making, respectively, of offers to exchange, sell or purchase derivatives contracts, securities or units in collective investment schemes (whether through that place or facility or otherwise); or

(b) such other facility or class of facilities as the Authority may, by order, prescribe.

Further, futures contracts are defined in Section 2(1) of the SFA, which states that a contract that creates the effect where one party agrees to deliver a specific commodity by a specified future time at a specified price payable at that time. Alternatively, a futures contract may require that the parties to the contract agree to settle the difference in the value of the quantity of a commodity at the time of the making of the contract and that value at a specified future time.

Hence, the issue of whether or not a token is a futures contract could be affected by: whether it is paid for and delivered at or around the time of entering into the ICO contract instead of at a specified future time; whether there is any difference between the value of the token at different points of time that has to be settled between the issuer and the purchaser; whether the potential profits or losses that a purchaser may make on the token will be as against the issuer; and whether the tokens are interests in or contractual rights against the issuer that may be realised or enforced in the future.

Overall, it appears that as long as the virtual currency is not a "security" under the SFA, its virtual currency exchange would currently not be regulated and no licence is currently required; however, if even one token is a security, then the exchange would be regulated under the SFA.

On 24 May 2018, MAS issued a warning to eight cryptocurrency exchanges who were found to have permitted trading of coins that were securities in Singapore. It is clear that MAS is taking a firm stance on these exchanges. As set out above, cryptocurrencies that are securities may only be listed on approved exchanges or recognised market operators.

Besides regulating exchanges on which security tokens are listed, MAS will also regulate cryptocurrency exchanges in general through the PSA.

Sales regulation

Sales of virtual currencies can occur through: (a) private sale when created; (b) ICO; or (c) trading.

Private sale at creation

This could occur as part of a pre-ICO or sale and purchase in the context of a newly created token. Generally, these are by a private agreement. However, if a token is deemed a security under the SFA, then licences need to be applied for and obtained (as discussed above).

ICOs

Please refer to the above section on the rules pertaining to the sale of a token pursuant to an ICO.

Trading

There are no regulations for retail investors specifically governing their trading of cryptocurrencies. Nonetheless, MAS has issued a statement to advise the public to "act with extreme caution and understand the significant risks they take on if they choose to invest in cryptocurrencies".

However, there are regulations governing certain activities that are related to trading. There is a list of activities that are regulated and licensed under the SFA and some of them may be related to trading.

Sub-section 82(1) of the SFA states:

> *"Subject to subsection (2) and section 99, no person shall, whether as principal or agent, carry on business in any regulated activity or hold himself out as carrying on such business unless he is the holder of a capital markets services licence for that regulated activity."*

Section 2(1) and the Second Schedule of the SFA define the regulated activities as:

> *"(a) dealing in capital markets products;*
>
> *(b) advising on corporate finance;*
>
> *(c) fund management;*
>
> *(d) real estate investment trust management;*
>
> *(e) product financing;*
>
> *(f) providing credit rating services;*
>
> *(g) providing custodial services."*

Section 2(1) and Part II of the Second Schedule of the SFA states:

> *""dealing in securities" means (whether as principal or agent) making or offering to make with any person, or inducing or attempting to induce any person to enter into or to offer to enter into any agreement for or with a view to acquiring, disposing of, entering into, effecting, arranging, subscribing for, or underwriting any capital markets products."*

Hence, if a person is trading as part of their business, then they would be regulated under the SFA and require a Capital Markets Services licence.

Fund management is defined in the Second Schedule as:

> *""fund management" means managing the property of, or operating, a collective investment scheme, or undertaking on behalf of a customer (whether on a discretionary authority granted by the customer or otherwise) —*
>
> *(a) the management of a portfolio of capital markets products; or*
>
> *(b) the entry into spot foreign exchange contracts for the purpose of managing the customer's funds,*
>
> *but does not include real estate investment trust management;"*

Therefore, if a person trades on behalf of a customer, then he/she would be regulated under the SFA and require a Capital Markets Services licence.

Taxation

(a) Revenue for goods or services using virtual currencies: Businesses that choose to accept virtual currencies for consideration for goods or services are subject to normal income tax rules found in the Income Tax Act (Cap.1304), hereinafter, "ITA". For example, if a business accepts payment in Ether, then it will be considered as revenue just as it would be if paid in fiat. The value given would be the value of the services (or goods) on the date of the transaction, or the parties could choose a mutually acceptable date for valuation. Taxation would be based on the net profits (after deducting allowable expenses under the ITA). The general current tax rate for businesses is 17% of taxable income.

(b) Capital gains tax: Individuals or businesses that buy virtual currencies for long-term investment purposes may enjoy a capital gain from the disposal of these virtual currencies. However, there are no capital gains taxes in Singapore, and as a result, these gains are not subject to tax. However, individuals or businesses that buy and sell virtual currencies in the ordinary course of their business will be **taxed on the profit derived from trading in the virtual currency**. Profits derived by businesses which mine and trade virtual currencies in exchange for money are also subject to tax, as these would be considered "revenue". Whether gains from disposal of virtual currencies are subject to capital gains tax depends on the facts and circumstances of each case. Factors such as purpose, frequency of transactions, and holding periods are considered when determining if such gains are taxable.

(c) Tax on proceeds from an ICO: The issue is whether the proceeds from an ICO are recorded as revenue and taxable in Singapore. As time evolves, more guidance is being given by the Inland Revenue Authority of Singapore (hereinafter "IRAS"); however, the position is not yet definitive. According to the ITA, revenue is taxable in Singapore if: (i) it is accrued or derived from Singapore; or (ii) if it is foreign-derived income, it is received in Singapore. The situation in (i), following Par.10(1)(a) of the ITA which states that revenue by a trade or business carried on by a taxpayer (as the entity usually used for an ICO is registered in Singapore, it would qualify as a taxpayer), is taxable. As it is still not clear, some taxpayers have therefore deemed income derived outside of Singapore (i.e. in the case where a token purchaser is outside of Singapore) as not subject to tax. It is for this reason that some ICO terms and conditions stipulate that Singaporeans may not purchase tokens. In scenario (ii), proceeds would not be taxable if not received in Singapore. This territorial criterion is based on an analysis of the facts, such as where the founders of the ICO are based, if the ICO is marketed outside of Singapore through promotional "hypathons" or via the cloud, and if the participants are based outside of Singapore. Even for those ICO proceeds that fall within (i) or (ii), tax planning such as imputing proceeds over a period of time and offsetting qualifying expenses can serve to minimise taxes payable. In addition, it should be remembered that only the income that falls within (i) or (ii) is taxable, and not the totality of the proceeds. It is advisable to seek tax advice prior to embarking on an ICO.

(d) Goods and Services Tax ("GST") on sale of virtual currencies: IRAS has confirmed the sale of tokens as a sale of a "supply of services". Under the Goods and Services Act ("GSTA"), GST is imposed on the supply of services. However, if the sale of a token

is to purchasers who do not have any connection to Singapore, then this could be viewed as an international supply of services, which has a zero rate of tax under the GSTA. The current rate of tax under the GSTA is 7%; however, this is expected to increase to 9% at some point between 2021 and 2025.

Money transmission laws, Know Your Client and Anti-Money Laundering requirements

With respect to money transmission laws, please refer to the above discussion on PSA.

In this section, the following will be examined:

- Know Your Client "KYC" requirements (including source of income requirements).
- Anti-Money Laundering ("AML") requirements.
- Combating of Financing of Terrorism ("CFT") requirements.

The standards an issuer of a cryptocurrency token must comply with depend on whether or not the token is a security. If the token is a security as defined in the SFA, the MAS guidelines on KYC, AML and CFT will apply.

MAS requires that financial institutions must:

- verify the customer's identity including name, unique identification number, date of birth, nationality and residential address;
- if the customer is not a natural person, verify the identities of the natural persons who have the authority to act for the customer;
- ascertain whether there are any beneficial persons and, if so, the identities of those beneficial persons;
- determine the nature and purpose of the business relations with the customer;
- visit the place of business if it is considered necessary;
- obtain information about the source of the funds;
- after business relations are established, conduct ongoing monitoring of the business relations; and
- conduct periodic reviewing of the adequacy of the customer information.

When the business is not done on a face-to-face basis, MAS suggests the following measures:

- holding real-time video conferencing that is comparable to face-to-face communication in addition to obtaining electronic copies of identification documents;
- verifying the identity of a customer through a document the customer has signed with a secure digital signature using a set of Public Key Infrastructure-based credentials issued by a certified Certificate Authority; and
- using biometric data such as fingerprints, iris scans or facial recognition.

Regarding the KYC process, in order to determine if someone is a Politically Exposed Person ("PEP"), it is possible to refer to databases compiled commercially or by the authorities. It is also beneficial to look at the customer themselves including details of their occupation, name of their employer, and non-public information.

MAS publishes lists of entities who are suspected of terrorist activities and all potential token purchasers must be screened to ensure they are not dealing with suspected terrorists (part of CFT requirements). Additionally, MAS maintains a list of countries which are subject to sanctions and customers must also not be from these countries. These should also be consulted.

In the event of a suspicious transaction, the Suspicious Transaction Reporting Office should be notified within 15 days.

Examples of suspicious transactions include:

- transactions which do not make economic sense;
- transactions involving large amounts of cash;
- transactions involving a high velocity of transactions through a bank account;
- transactions involving transfers abroad;
- investment-related transactions that are suspicious;
- merchants acquired for the purpose of credit or charge card transactions;
- transactions involving unidentified parties;
- transactions related to tax crimes; and
- trade-related transactions with significant discrepancies.

For tokens that do not fall within the definition of securities set out in the SFA, the MAS Guidelines on KYC, AML and CFT do not, strictly speaking, apply. However, it is good business practice to follow these Guidelines nevertheless.

Personal data protection laws

The Singapore Personal Data Protection Act ("PDPA") and the European Union's General Data Protection Regulations ("GDPR") are discussed in this section.

The protection of a customer's personal data is governed by the PDPA. When an individual's personal data is collected, consent must be obtained and the individual must be informed of the purpose for which it is collected. Consent is deemed to have been given in circumstances where the individual volunteers the personal data and it is reasonable that the personal data would be provided. An individual may withdraw consent to the collection of personal data at any time.

An organisation must ensure that personal data cannot be accessed by implementing reasonable security arrangements. Security would include measures such as encryption and requiring that personal data can only be accessed with passwords of a sufficient length. When personal data is transferred out of Singapore, the organisation must ensure that it is afforded the same level of protection as required by the PDPA.

Under the PDPA, an individual may request access to and the correction of personal data. While an organisation may charge a reasonable fee to comply with such requests, it must provide a written estimate of the fee before complying with a request for access.

Singapore's PDPA is well aligned with the European Union's GDPR. However, the GDPR further provides that, in relation to citizens or residents of the European Union, the owner of personal data may request that his or her personal data be erased. The GDPR also requires that an organisation's privacy policy must be readily understood by a layperson.

The Personal Data Protection Commission ("Commission") has jurisdiction over complaints made by individuals in respect of breaches of the PDPA. The Commission has the power to order that an organisation cease collecting or destroy personal data, and also to impose a fine of up to S$1 million.

Ownership and licensing requirements

In this section, ownership and investment licences under MAS, as well as licensing, are discussed by asking the following questions:

- Can investment managers use virtual currencies for investment purposes? Are they required to have the same licences as if they were using fiat? What could these licences be?
- What are the types of licences needed by someone who uses virtual currencies as an investment advisor or fund manager or capital markets advisor? What is the process for obtaining these?

MAS has not provided any guidance on whether virtual currencies may be used for investment purposes. Therefore, it would be advisable for investment managers to enquire with MAS before using virtual currencies.

Under the Second Schedule of the SFA, MAS requires companies engaged in fund management or advising on corporate finance to hold a Capital Markets Services Licence. If the assets under management are less than S$250 million and the number of qualified investors is 30 or less, the company would need to be a Registered Fund Management Company.

MAS estimates that applications for a licence or registration will take approximately two to four months to process.

The General Criteria for the grant of a CMS licence are set out in the MAS Guidelines on Criteria for the Grant of a Capital Markets Services Licence:

- must be a corporation;
- must be a reputable entity with an established track record in the proposed activity to be conducted in Singapore or in a related field for at least the past five years;
- the applicant and its holding company or related corporation must have a good ranking in their home country;
- must be subject to proper regulation by the authority in its home country, if applicable;
- must satisfy MAS that it will discharge its duties efficiently, honestly and fairly;
- must establish and operate out of a physical office situated in Singapore;
- must be primarily engaged in conducting one of the regulated activities under the SFA; and
- its officers, employees, representatives and substantial shareholders are fit and proper, in accordance with the criteria set out by MAS.

In order for the Board of Directors, Chief Executive Officer and Representatives to hold a CMS licence, they are required to comply with additional criteria.

Investment advisors would be required to have a financial advisor's licence pursuant to the Second Schedule of the Financial Advisors Act.

The MAS Guidelines on Criteria for the Grant of a Financial Advisor's Licence specify a minimum paid-up capital of S$150,000 or the equivalent in a foreign currency. Other relevant criteria include:

- whether at least two individuals are employed or appointed for financial advisory services;
- whether the Chief Executive Officer and all Executive Directors have at least five years of relevant working experience in financial advisory services, with a minimum of three years in management, as well as acceptable academic and professional qualifications;
- whether the Board of Directors has at least two members one of whom is resident in Singapore;

- whether the Chief Executive Officer is resident in Singapore; and
- whether the Chief Executive Officer or Executive Directors are placed in a position of conflict of interest.

Mining

Cryptocurrency mining is the process of using computers to verify transactions on the blockchain and add a new block to the blockchain, in return for an amount of cryptocurrency. Cryptocurrency miners need to compete against each other in order to be the first to verify the transaction and earn the amount of cryptocurrency, using the Proof-of-Work ("PoW") method. In order to sustain a mining business, large amounts of computational power and electricity are required. This is the same process as is used in most other jurisdictions.

Currently, there are no regulations specifically governing the mining of cryptocurrency in Singapore. A miner would require specialised hardware with adequate cooling systems and large amounts of electricity. Hence, the miner should ensure that he is allowed to carry out mining at his chosen venue following local regulations on emissions and noise.

A miner should also be conscious of his tax liabilities arising from his income from mining. IRAS states on its website that: "Profits derived by businesses which mine and trade virtual currencies in exchange for money are also subject to tax." The current business tax rate is 17% on net profits pursuant to the ITA.

As mining is considered work, a foreigner would be required to have the requisite work permit to be able to work in Singapore. In addition, businesses who employ miners need to respect Singapore employment law.

In any case, mining is likely to become less prevalent in the future in Singapore given the high electricity costs, tropical temperatures, and premium on space. Blockchain projects initially relied on PoW to validate transactions. However, in Singapore, there are now more blockchain projects using the Proof-of-Stake ("PoS") method of validating transactions on the blockchain. The PoS method does not require mining in the way that the PoW method does, because, under the PoS method, whether a transaction on the blockchain may be verified by a person depends on the number of coins that he/she holds. The said person would earn an amount of cryptocurrency by verifying the transaction on the blockchain, but there is no competition in doing so, and minimal computational power is required, thereby saving on electricity.

Border restrictions and declaration

There are currently no border restrictions or declarations required with respect to virtual currencies, other than complying with the regulatory regime as described above. Virtual currencies are borderless.

The IRAS treats virtual currencies as the supply of services. While this usually means virtual currencies are a service provided to the purchaser when the currency is first issued, there is some uncertainty as to whether a virtual currency must be declared when it is imported into Singapore.

Arguably, importing cryptocurrencies stored on USB flash drives or similar hardware wallets into Singapore need not be declared to the customs authorities as only the private keys are being transported, while the blockchain remains decentralised and not situated in any particular location. Further, cryptocurrencies are not one of the categories of goods subject to import duty under the Customs Act (Chapter 70). That said, to err on the side of caution,

it would be advisable to declare the value of goods or services which exceed S$600 when entering Singapore. The Goods and Services Tax (Imports Relief) Order provides that a *bona fide* traveller may import goods worth up to S$600 if the traveller has been outside Singapore for at least 48 hours, or up to S$150 if the traveller has been outside Singapore for less than 48 hours.

Reporting requirements

Virtual currencies are meant to be decentralised and anonymous. There are currently no reporting requirements for the ownership, use or sale of virtual currencies other than for tax purposes as described above.

Everyone is required under the law to report suspicious transactions, which they come across in the course of their trade, profession, business or employment, to the Suspicious Transaction Reporting Office ("STRO") in the Commercial Affairs Department of the police. All suspicious transaction reports, including those involving cryptocurrencies and digital tokens, are analysed by STRO. Where there are indications of an offence, STRO will refer the matter to the enforcement agencies, such as IRAS for possible tax crimes, and the Capital Adequacy Directive ("CAD") for possible money laundering.

Estate planning and testamentary succession

This section will discuss how virtual currencies can be included as an asset in estate planning and succession, including issues of confidentiality or security and valuation.

The main pieces of legislation, the Intestate Succession Act (Cap.146), the Wills Act (Cap.352), and the Probate and Administration Act (Cap.251) have no specific laws dealing with estate planning and succession relating to virtual currencies. Wallets containing virtual currencies, and even value-stored cards, can be transferred in much the same way as other personal property is transferred.

The security of a cryptocurrency is a major concern. Virtual currencies are typically stored in wallets where their ownership is anonymous, and where there are no designated beneficiaries. If no-one has details of a wallet, it will not generally be possible to have access to its contents. For estate planning or testamentary purposes, methods are being devised to make the wallet accessible through an executor or trustee by providing details of the service provider, the user details and the private key. As wills have to be in writing in Singapore, and witnessed by two persons, and often sent to a central registry, it is not recommended that these details be written in a will or trust or other estate document, as whoever has access to these details will be able to access the wallet.

With respect to valuation, since there is no capital gains tax in Singapore, the differences in valuations from the time a cryptocurrency is acquired by a testator, bequeathed, inherited and converted to fiat are not relevant. Valuations may, however, be relevant for practical purposes when trying to bequeath specific sums to heirs or beneficiaries, as their value changes over time.

Franca Ciambella
Tel: +65 6235 2700 / Email: fciambella@consiliumlaw.com.sg

Trained in law and business in Canada, New York and Singapore, Franca was one of the first foreign lawyers to gain admission to the Singapore Bar. Her legal career of 29 years encompasses being a partner at a major Canadian law firm, General Counsel for Asia for a US-based Fortune 500 corporation, and since 2010, being Managing Director of Consilium Law Corporation. Consilium represents clients doing business in ASEAN and Canada, in diverse sectors.

Franca's expertise lies in corporate and commercial law, contracts, technology law, fintech, cross-border M&A, and foreign investment law. Her focus is on technology projects and has a cutting edge multi-jurisdictional practice in the area of cryptocurrency. She also works extensively in foreign direct investment in ASEAN and Canada.

Franca is on the Board of the Canadian Chamber of Commerce in Singapore and sits on various other professional and charitable board and advisory committees.

En-Lai Chong
Tel: +65 6235 2700 / Email: enlai@consiliumlaw.com.sg

Having graduated from the National University of Singapore in 2005, En-Lai Chong has a broad range of experience from civil litigation to corporate & commercial law. From working with a multinational corporation as a legal counsel, he also gained practical commercial experience. He has a keen interest in blockchain technology and cryptocurrencies.

Consilium Law Corporation

1 Scotts Road, #16-02, Shaw Centre, Singapore 228208
Tel: +65 6235 2700 / URL: www.consiliumlaw.com.sg

South Africa

Angela Itzikowitz & Ina Meiring
ENSafrica

Government attitude and definition

As a result of the growing interest and rapid innovation in the financial technology ("**fintech**") and crypto assets domain, the Intergovernmental Fintech Working Group ("**IFWG**") was established in 2016. The IFWG is comprised of members from the National Treasury, the South African Reserve Bank (the "**SARB**") (Prudential Authority), the Financial Sector Conduct Authority (the "**FSCA**") (the Market Conduct Authority), the South African Revenue Service ("**SARS**") and the Financial Intelligence Centre (the "**FIC**"). The overarching objective of the IFWG has been to develop a common understanding among regulators and policymakers of fintech developments, as well as the policy and regulatory implications (of fintech) for the financial sector and the economy as a whole.

In early 2018, a joint working group, the Crypto Assets Regulatory Working Group (the "**CARWG**") was established under the aegis of the IFWG and is represented by members of the IFWG and SARS. The mandate of the CARWG was to review the position on crypto assets and to consider the public policy concerns raised by these assets, which should inform the regulation of these assets going forward.

The need to develop a policy and regulatory response to crypto asset activities in South Africa was driven by the impact of crypto assets on the financial sector, the potential for regulatory arbitrage and the like.

In developing its policy and regulatory responses to the emergence of crypto assets in South Africa, the CARWG adopted a functional approach (rather than focusing on the specific technology applied or the entity involved) and the following use cases (and risks inherent in these cases) were identified: (i) purchasing and/or selling; (ii) payments; (iii) capital raising through initial coin offerings; (iv) crypto derivatives and funds; and (v) market provisioning. The CARWG accepts that these use cases are not watertight and that the market, as a rapidly evolving one, requires continuous assessment.

In formulating its policy, guidance from international standard-setting bodies was considered, as well as the approaches taken by numerous other jurisdictions.

From a regulatory perspective, having definitional clarity on crypto assets is crucial, as it directly influences its classification and concomitant regulatory treatment. Despite the various nomenclature used, namely "crypto tokens", "crypto assets", "digital tokens" and the like, the crypto-phenomenon is commonly based on decentralised technology such as blockchain and other distributed ledger technology.

In January 2019, the IFWG and the CARWG released a joint consultation paper entitled the "*Consultation Paper on Policy Proposals for Crypto Assets*" (the "**Consultation Paper**")

for public comment. The Consultation Paper provides a background and context for the review of the position on crypto assets in South Africa, and provides a scope of the crypto activities assessed. While the Consultation Paper identified the following crypto asset specific use cases:

(i) the purchase and sale of crypto assets;

(ii) payments using crypto assets;

(iii) capital raising through initial coin offerings;

(iv) crypto derivatives and funds; and

(v) market provisioning,

it currently focuses only on the purchase and sale of crypto assets and payment using crypto assets.

The regulatory authorities in South Africa are of the view that crypto assets do not constitute "money" as per the traditional definition of the word, but acknowledge that crypto assets may perform certain functions similar to those of currencies, securities and commodities. To this end, the following definition of "crypto assets" is proposed:

> "*Crypto assets are digital representations or tokens that are accessed, verified, transacted, and traded electronically by a community of users. Crypto assets are issued electronically by decentralised entities and have no legal tender status, and consequently are not considered as electronic money either. It therefore does not have statutory compensation arrangements. Crypto assets have the ability to be used for payments (exchange of such value) and for investment purposes by crypto asset users. Crypto assets have the ability to function as a medium of exchange, and/or unit of account and/or store of value within a community of crypto asset users.*"

In defining the most appropriate regulatory approach, the South African regulatory authorities have considered whether crypto assets require completely new regulation, or whether they can be accommodated and regulated in line with existing regulation.

The attitude of the CARWG is that regulatory action should not be delayed until the most appropriate regulatory approach has become clear, and that to the extent possible, existing regulation with the relevant amendments should be adopted to accommodate this new asset class. The South African regulatory authorities have an open door policy in considering and discussing innovation and concomitant regulation with fintech players.

Cryptocurrency regulation

There is currently no fintech specific regulation for crypto assets, but crypto assets are also not prohibited.

Sales regulation

The issuing of financial products, and related services such as the purchase and sale of financial products, is regulated in terms of the various "financial sector laws", as that term is defined in the Financial Sector Regulation Act 9 of 2017 ("**FSRA**").

Some of the financial sector laws which apply to the issuing and sale of financial products and which are, or may be relevant to crypto assets are the following:

(1) Banks Act 94 of 1990 ("**Banks Act**");

(2) Financial Advisory and Intermediary Services Act 37 of 2002 ("**FAIS**");

(3) Companies Act 71 of 2008 (the "**Companies Act**").

(4) Financial Markets Act 19 of 2012 ("**FMA**"); and

(5) Collective Investment Schemes Control Act 45 of 2002 ("**CISCA**").

Most of the financial sector legislation which applies to financial products and financial services pre-dates crypto assets and other digital assets and it is therefore not surprising that none of the financial sector laws (as set out above) dealing with the issue and sale of financial products apply (at least not expressly) to crypto assets.

For example:

(1) the marketing of crypto assets, including the giving of any advice or making a recommendation as to which assets to purchase, would not currently require authorisation in terms of FAIS as these assets are not financial products within the remit of that Act ("**FAIS**"). Importantly, however, if a person gives advice regarding a financial product (as defined in FAIS) that referenced a crypto asset or in which a crypto asset was the underlying asset, then that person would possibly be required to be registered as a financial services providers in terms of FAIS; and

(2) the FMA, which regulates the provision of securities services in South Africa, does not contain any reference to crypto assets in the definition of "securities" and the Registrar of Securities Services has not prescribed crypto assets to be instruments similar to any of the securities listed in the FMA. Furthermore, the type of securities listed in the FMA all have one common feature: there is a "central issuer" against whom the holder of the securities will have a claim. A crypto asset lacks this feature, as it is not issued by any central authority or person.

Taxation

A draft Taxation Laws Amendment Bill ("**TLAB**") has been published and proposes various amendments to the Income Tax Act 58 of 1962 ("**Income Tax Act**") and the Value Added Tax Act 89 of 1991 ("**VAT Act**"), which (amongst others) seeks to clarify the existing provisions dealing with crypto assets in the South African tax law.

Under the VAT Act, it is proposed to amend section 2 to include in the description of "financial services", the issue, acquisition, collection, buying or selling or transfer of ownership of any crypto assets. As a result, if the proposal in respect of the VAT Act is accepted, all dealings in crypto assets will be exempt from VAT in terms of section 12 of the VAT Act.

Under the Income Tax Act, it is proposed that crypto assets be included in the definition of "financial instrument". Moreover, it is also proposed to amend section 20A of the Income Tax Act, to include the acquisition or disposal of any crypto assets under the ring-fencing of assessed loss provisions. If this proposal is accepted, crypto asset dealers will not be able to offset the losses incurred from dealing in crypto assets from any other trade. These losses are therefore ring-fenced to be used only against income earned from crypto asset trade.

The purpose of these proposed amendments to the tax legislation is to clarify the tax treatment of crypto assets under the tax laws. From an income tax perspective, crypto assets are to be treated as financial instruments for income tax purposes, and from a VAT perspective, the issue, acquisition, collection, buying or selling or transfer of ownership of any crypto asset is to be treated as a financial service. Until such time as these amendments take effect, there remains a gap in the tax treatment of crypto assets.

Money transmission laws and anti-money laundering requirements

The Financial Intelligence Centre Act 38 of 2001 ("**FICA**"), one of South Africa's anti-money laundering statutes, imposes various duties on "accountable institutions". These include the duty to: identify and verify clients; keep records; and report certain transactions to the Financial Intelligence Centre ("**FIC**").

"Accountable institutions" are listed in schedule 1 to FICA and include banks and money remitters. Importantly, the duty to report suspicious or unusual transactions is more widely cast and applies not only to accountable institutions but to all persons who carry on business in South Africa.

Going forward, crypto asset service providers (including crypto asset exchanges and entities that provide custodial services) will be obliged to register as accountable institutions in terms of FICA, and as such will be obliged to comply with anti-money laundering and counter financing of terrorism requirements in the FIC Act.

In terms of section 29 of FICA, any person (including an accountable institution) who carries on a business, or is in charge of, or manages a business, or who is employed by a business, who knows or suspects that:

(a) the business has received or is about to receive the proceeds of unlawful activities or property connected to an offence relating to the financing of terrorism;

(b) a transaction or series of transactions to which the business is a party, facilitated or is likely to facilitate the transfer of the proceeds of unlawful activity or property relating to the financing of terrorist activities; has no apparent business or lawful business; may be relevant to the investigation of tax evasion or relates generally to the financing of terrorism; or

(c) the business has been used, or is about to be used for money-laundering purposes, or the financing of terrorism,

must report within a prescribed period to the FIC.

These reporting provisions would apply to any entities doing business involving crypto assets.

The remittance of crypto assets would not currently constitute money remittance within the purview of FICA as crypto assets are not considered money.

Promotion and testing

As discussed under "*Government attitude and definition*", the IFWG and the CARWG have been tasked with engaging with regulators and policymakers, and developing key considerations and a more harmonised approach to fintech-driven innovations. The purpose of this engagement is to identify the risks and benefits of financial innovation driven by fintech, so that regulators and policymakers can develop appropriate policies and implement effective frameworks that allow for responsible innovation.

Ownership and licensing requirements

As crypto assets are decentralised, there is no central government controlling authority that claims ownership of crypto assets. Further, there are currently no restrictions on investment managers owning crypto assets for investment purposes. As a result, there are also no licensing requirements imposed on anyone holding crypto assets as an investment advisor.

The Financial Institutions (Protection of Funds) Act 28 of 2001 ("**FI Act**") imposes certain duties on persons dealing with funds of clients, and with trust property controlled by financial institutions and nominee companies. "Trust property" is defined in the FI Act to mean:

> "*[A]ny corporeal or incorporeal, movable or immovable asset invested, held, kept in safe custody, controlled, administered or alienated by any person, partnership, company or trust for, or on behalf of, another person, partnership, company or trust, and such other person, partnership, company or trust is hereinafter referred to as the principal*."

This definition is sufficiently wide to encompass money – and arguably also a crypto asset – as an incorporeal asset. If an asset manager as a financial institution holds crypto assets on behalf of clients, this may amount to holding trust property for purposes of the FI Act. The FI Act imposes duties on financial institutions which deal with trust property.

Section 2 of the FI Act provides that a financial institution which invests, holds, keeps in safe custody, controls, administers or alienates any funds of the financial institution or any trust property:

- must, with regard to such funds, observe the utmost good faith and exercise proper care and diligence;
- must, with regard to the trust property and the terms of the instrument or agreement by which the trust or agency in question has been created, observe the utmost good faith and exercise the care and diligence required of a trustee in the exercise or discharge of his or her powers and duties; and
- may not alienate, invest, pledge, hypothecate or otherwise encumber or make use of the funds or trust property, or furnish any guarantee in a manner calculated to gain, directly or indirectly, any improper advantage for any person to the prejudice of the financial institution or principal concerned.

Other duties imposed by the FI Act on financial institutions (or the directors, members, partners, officials, employees or agents of the financial institution) include:

- a requirement for all parties who take part in investment decisions to declare any direct financial interest in a company in which trust property will be invested to the board of management of the company prior to the investment being made (section 3);
- investing the trust property only in such manner as directed by agreement (with the client) or, in the absence of such an agreement, as directed by the FI Act; and
- keeping its assets separate from the trust property (which separation must be visible in its books of accounts).

The FI Act, however, does not impose a regulatory approval or registration requirement on financial institutions.

Mining

Crypto asset "mining" is not regulated in South Africa and is therefore permissible. As far as we are aware, the South African regulatory authorities are not planning to regulate mining.

Border restrictions and declaration

Exchange Control in South Africa is mainly governed by the Currency and Exchanges Act 9 of 1933 (as amended) and the Exchange Control Regulations issued under this Act. The SARB also publishes Exchange Manuals and guidelines ("**Manuals**").

Any person wishing to move funds offshore for the purposes of buying crypto assets has to make an application for exchange approval through authorised dealers in foreign exchange. "Authorised Dealers" are South African commercial and merchant banks, appointed by the Minister of Finance, to buy and sell foreign exchange, within the limits and subject to conditions prescribed by the National Treasury and the SARB. Authorised dealers act on behalf of their customers and they are not agents of the SARB.

The basic principle underlying the Exchange Control Regulations is that no exchange commitment may, in terms of the Exchange Control Regulations, be entered into by South Africans without prior approval. In certain instances, Authorised Dealers are empowered to approve applications themselves (i.e. without reference to the SARB). The Manuals contain the conditions and limits applicable to transactions in foreign exchange which may be undertaken by Authorised Dealers. For all other applications involving foreign exchange that fall outside the scope of the Manuals, the Authorised Dealer must forward such application to the Financial Surveillance Department of the SARB.

The issue of crypto asset cross-border remittance is currently being considered by the Financial Surveillance Department (which monitors exchange control) within the SARB.

Reporting requirements

The reporting requirements under FICA require certain cash transactions to be reported. However, FICA defines cash as: (a) coin and paper money of South Africa or of another country that is designated as legal tender and that circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue; and (b) travellers' cheques. This definition clearly does not include crypto assets and such reporting obligations will therefore not be imposed under FICA. Other reporting obligations under FICA relate to electronic transfers of money to and from South Africa. Since it is not possible to transfer crypto assets via an electronic funds transfer, these reporting obligations will also not apply.

Estate planning and testamentary succession

Crypto assets are not regulated for purposes of estate planning and succession.

* * *

Acknowledgment

The authors wish to acknowledge and thank Byron Bromham, a trainee at ENSafrica, for his assistance in compiling this chapter.

Angela Itzikowitz
Tel: +27 11 269 7600 / Email: aitzikowitz@ensafrica.com

Professor Angela Itzikowitz is a director in ENSafrica's Banking and Finance Department and co-heads the newly established Fintech department. She specialises in banking and financial market regulation, including finance and regulatory reform, card and related electronic payment instruments, derivatives, loan agreements, collective investment schemes, insurance and Fintech. She has been recognised as a leading Fintech lawyer in a number of international publications including *Chambers* and advises banks, insurers and start-ups on the regulation of Fintech. She was recently appointed external counsel to the South African Reserve Bank's (**SARB**) Intergovernmental Fintech Working Group (**IFWG**) and the Crypto Assets Regulatory Working Group (**CAR**). In her capacity as external counsel, she is assisting with the drafting of the policy paper soon to be issued by the SARB and advising on the regulation of crypto assets. She also teaches short courses on Fintech and Blockchain at the University of Cape Town. She is the author of the *Law of South Africa Banking and Financial Markets* (**LAWSA**), has co-authored a number of books and has published numerous articles in local and foreign journals.

Angela has been recognised as a leading lawyer for a number of consecutive years by:

- *Chambers Global Guide* (Banking and Finance: Regulatory). Angela is the only South African Lawyer to be ranked Band 1 for both 2018 and 2019.
- *Who's Who Banking and FinTech* (South Africa).
- *Best Lawyers* – Banking and Finance (South Africa).

Angela is fluent in English, Afrikaans and German and speaks South Sotho and Mandarin.

Ina Meiring
Tel: +27 11 269 7600 / Email: imeiring@ensafrica.com

Ina Meiring is an executive in ENSafrica's banking and finance department. Ina is regarded as one of the top finance regulatory experts in South Africa and her clients include leading local and international financial institutions. Her experience includes advising on banking and financial services regulation and consumer law matters, including: the South African Consumer Protection Act, 2008; the National Credit Act, 2005; and the Protection of Personal Information Act, 2013. Her expertise further includes advising on corporate governance, exchange control, securitisations, payment instruments and payment methods. Ina is a member of the expert group appointed by the South African Reserve Bank for the review of the National Payment System Act, 1998. She has authored chapters on South African banking regulation for a number of legal publications, and has lectured at the University of Johannesburg and the University of South Africa.

ENSafrica

The MARC | Tower 1, 129 Rivonia Road, Sandton, Johannesburg 2196, South Africa
Tel: +27 11 269 7600 / URL: www.ENSafrica.com

Spain

Alfonso López-Ibor, Pablo Stöger & Olivia López-Ibor
Ventura Garcés López-Ibor

Government attitude and definition

The Spanish government has been very cautious and conservative with regard to cryptocurrencies, since Spanish law is highly protective of the rights of investors and consumers, and because during the recession there has been a large number of cases of financial and securities fraud.

Cryptocurrency cannot be legally treated as money for legal tender. Law 46/1998 of 17th December, on the introduction of the euro as the national currency, provides that from 1st January 1999 the national currency of Spain shall be the euro. This law cross-refers to Council Regulation (EC) Nº 974/98 of 3rd May 1998. Under article 10 of this Regulation, only banknotes and coins denominated in euros and valid in other Eurozone countries shall have the status of legal tender in Spain and, more generally, the euro shall be the sole unit of account in legal instruments, whether under private or public law.

On 8th February 2018, the Bank of Spain and the Spanish Stock Market Regulator (CNMV) issued a joint communiqué about the perils of investing and dealing in cryptocurrencies and emphasised that small investors should avoid these investments. The communiqué does not contain a normative definition of cryptocurrencies, although it describes accurately concepts such as an "initial coin offering" (ICO) and "tokens" by differentiating between "security tokens" and "utility tokens", using terms in Spanish which can be easily understood and are accessible to the layman. The communiqué is not part of Spanish true legal order as such, but certain parts could be considered as "soft law" in as much as they signal the Spanish government's attitude.

Regarding blockchain technology, it is fair to say that a technology which allows digital information to be distributed but not to be copied, will have many uses in the Spanish legal environment. In Spain, notaries have a monopoly on certifying the authenticity of legal documents, so that blockchain platforms could be an alternative to notaries for the documentation of certain legal documents. A recent example has been a syndicated financing carried out by a major bank (BBVA) based on a blockchain platform.

Cryptocurrency regulation

There is no specific regulation on cryptocurrencies in Spain, except that they cannot be treated as legal tender, which is exclusively reserved for the euro as the national currency. The abovementioned joint communiqué also points out that there are no issues for cryptocurrencies or ICOs which have been approved or verified by any regulatory authority such as the Bank of Spain or the CNMV. In Spanish law, cryptocurrency cannot be considered as a financial instrument (promissory note, derivative, etc.) either, nor a currency (domestic or foreign), but we consider that they could be assimilated to securities in the case of public offerings, or to chattels or commodities when they are traded individually.

To the extent that they can be considered as securities, ICOs may fall within the prospectus-filing requirements of the Spanish stock market law (LMV), as the definition of financial instruments and negotiable securities is very wide (article 2 LMV), and the Spanish government can add new types of securities by its own fiat without an amendment of the law being necessary, provided this has been agreed under EU regulations. A communiqué of the CNMV dated 8th February 2018 has also confirmed this view and therefore ratified it by a notice, dated 6th July 2018. Under article 38 of Royal Decree 1310/2005, as amended from time to time, offerings addressed exclusively to professional investors or to fewer than 150 persons, or with a minimum investment of at least €100,000 per investor, or in the case of securities having a face value of at least €100,000, would not be subject to the prospectus-filing requirements (CNMV).

As discussed, the Spanish regulator (CNMV) is highly protective of small investors' rights. This may have had an impact on the non-advertisement of ICOs in the Spanish market so far. On the other hand, the CNMV is also sensitive to the benefits of ICOs, to the extent that they bring technological innovation and may promote entrepreneurial business.

The current position of CNMV and Bank of Spain is that specific regulation of cryptocurrency and ICOs is necessary, but such regulation can only be made at European Union level and after consultation with certain third countries such as the U.S., which play a major role in world financial markets (see statement to the press by Sebastian Albella, Chairman of the CNMV, *El Economista*, dated 9th June 2018).

Sales regulation

To the extent that cryptocurrencies are considered commodities, they will be traded under the general rules of the Civil Code and the Code of Commerce, and in particular, those applicable to the contract of barter (*permute*). Aside from Spanish law that would allow the parties freedom of choice of the governing law, applicable to the transaction (article 3 of Regulation Rome I, Regulation (EC) 593/2008 on the law applicable to contractual obligations), small investors qualify for treatment as consumers and therefore even if a law other than Spain's has been chosen, mandatory Spanish law on consumer or investment protection will apply to the trade in order to benefit the Spanish party (article 6.2 of Regulation Rome I), which expressly refers to the "protection afforded by legal provisions that cannot be derogated from by agreement (…)".

Depending on the type of tokens (security or utility), the Spanish rules on title transfer may be more easy or difficult to apply. Broadly speaking, Spanish law requires a contractual agreement plus the delivery of the object, so that title is passed from the seller to the purchaser. This would be non-controversial if the security token comprised only membership rights within the meaning of corporate law but would be different and more complicated in the case of dematerialised claims such as payment claims via the internet.

Thus, much depends on how Spanish law would characterise cryptocurrencies. The Bank of Spain and the CNMV seem to consider them as "securities" based on the position adopted by the SEC (see the SEC Chairman's communiqué dated 11th December 2017, which has been extensively quoted by Spanish regulators). This view is based on the fact of the purchase of a financial instrument, there being a profit expectation, and also the confidence in other people's efforts to generate an economic revenue. However, in Spanish law, in certain cases, cryptocurrency has been simply categorised as an electronic product, which is intangible, and which is certainly similar to the information stored in computer hardware. The Spanish Mercantile Register already followed this approach in late 2017 when it accepted that the corporate capital of a limited company could be contributed in bitcoins (although the capital was denominated in its euro counter value).

Aside from the foregoing, the judgment of the European Court of Justice (ECJ) of 22nd October 2015, which treated bitcoins as foreign exchange, could also have a future bearing in Spain, even though there is the serious objection that there is no state authority or central bank supporting bitcoins and they cannot be legal tender, which creates legal uncertainty. Finally, utility tokens which can be assimilated to vouchers entitling the selling entities to discounts would not be treated as securities or commodities and would only be subject to consumer protection legislation.

Aside from the foregoing, token sales of bitcoins against euros could lead to a risk of criminal prosecution to the extent that the bitcoins' seller purports to the buyer to be selling or exchanging "money", hiding the risk of bitcoins' depreciation, as under Spanish law the payment of debts must be done in the agreed currency or in euros as the currency of legal tender in Spain (article 248 CP in relation with section 1170 CC).

Taxation

Capital gains from the sale of cryptocurrencies by a person resident in Spain will be taxed according to a rate of 23%. If they have been acquired and sold within 12 months, the tax rate may vary from 24.75% to 52%. If the capital gains have been obtained by a company, there is a flat tax rate of 25%.

VAT treatment

The exchange of cryptocurrencies into euros or *vice versa* is VAT-exempt (ECJ, 22nd October 2015-C-264/14, Hedqvist). This judgment establishes that such exchange is a provision of a service and not the delivery of a good, and that bitcoins can be assimilated as to a type of foreign exchange, which has been voluntarily accepted by the parties to the relevant transaction, and therefore enjoys the VAT exemption provided under article 135, 1 point e) of Directive 2006/112/CE on VAT.

Money transmission laws and anti-money laundering requirements

Law 10/2010 dated 28th April, on the prevention of money laundering, is widely drafted with regard to the parties which are subject to it. Article 2 expressly mentions entities of electronic money, foreign exchange or money transfer companies, depositors or custodians or funds or payment means, all of which may trade or deal in one way or another in cryptocurrencies, and therefore become subject to money laundering supervision. On top of this, the new EU Directive (2015/849/EU) will also extend the requirements to entities providing services to safeguard private cryptographic keys to hold, stake or transfer virtual currencies. In addition to this, it is clear that purchase, conversion or transfer of cryptocurrencies that have originated in a crime will fall within the scope of the Spanish Criminal Code (article 301 *et seq.*), which imposes very serious penalties on this activity.

Promotion and testing

There is new draft legislation currently before Parliament which will allow the introduction of new technologies to the Spanish market through a "controlled testing environment". In this, Spanish law seems to be drawing its inspiration from the UK Financial Authority (FA) which grants licences for sandboxes, but it is still at a very incipient stage and the Ministry of Economy has drafted preliminary legislation that will be subject to open consultation.

Ownership and licensing requirements

To the extent that cryptocurrencies are considered to be technological products, there are no licence requirements. If they are used as financial instruments, they will be subject to stock

market regulation with regard to the issue and the ICO of cryptocurrencies. There is no published guidance about investments in cryptocurrencies by funds except that alternative investment funds may invest in cryptocurrencies when dealing with the money of qualified investors.

Mining

Bitcoin and many other cryptocurrencies are not yet regulated, and this is permitted except as discussed in 'Cryptocurrency regulation', above.

Border restrictions and declaration

There are no frontier restrictions or obligations to report cryptocurrency holdings at the border which are only applicable to "cash" as defined by article 2 of regulation (EU) 1889/2005, which does not include electronic means of payment.

Reporting requirements

Under article 34.2 of Law 10/2010 dated 28th April, on the prevention of money laundering, electronic payments which can be used to make payments to an unidentified beneficiary (payments to the bearer) are treated as physical money (banknotes, cheques, etc.) and are therefore subject to a limit of €2,500 per payment, or €15,000 per payment if the party making the payment is not resident in Spain. This limitation is not applicable if the payment is made through banks.

Estate planning and testamentary succession

Cryptocurrency for the purposes of wills and intestate succession will be treated as any other ordinary assets of the deceased person.

Alfonso López-Ibor
Tel: +34 91 521 78 18 / Email: alfonso.lopezibor@vg-li.com

Alfonso López-Ibor is the Managing Partner of the Madrid office. He had previously been the Managing Partner of the Madrid office of Allen & Overy for 10 years. He has extensive experience of corporate law, finance and banking. Alfonso López-Ibor is also widely known for his expertise in litigation, arbitration and air transport.

In the corporate field, he regularly advises clients on the acquisition and sale of Spanish and foreign companies, venture capital and private equity transactions, management buy-outs and corporate restructuring processes. He has extensive experience advising multinationals setting up in Spain, whether through subsidiaries, branches or the acquisition of existing companies. In banking and finance, he has developed extensive experience of syndicated loan operations, guarantees and asset finance and dealing with the Spanish stock market regulator (CNMV).

He leads a department that has gained wide recognition for its expertise in providing legal advice to the air transport industry in areas such as domestic and international commercial agreements, handling agreements and financing structures, including operational leasing arrangements, guarantees, acquisition finance, licences, authorisation and registration.

He is one of Spain's foremost legal experts on the aviation sector. His litigation work includes advising on international disputes and arbitration processes, with a focus on highly complex issues.

Pablo Stöger
Tel: +34 91 521 78 18 / Email: pablo.stoger@vg-li.com

Pablo Stöger Pérez is a partner of the firm who has spent most of his legal career with Ventura Garcés López-Ibor.

Pablo is a specialist in Corporate Law and Litigation (contracts, company agreements, mergers & acquisitions and bankruptcy law, among other areas). He has extensive experience of forming subsidiaries, branches and representative offices for foreign companies in Spain, and has advised clients in sectors such as banking and financing, private equity, air transport, real estate and construction, insurance, automation and control, high-tech and food and agriculture.

Olivia López-Ibor
Tel: +34 91 521 78 18 / Email: olivia.lopezibor@vg-li.com

Olivia López-Ibor advises Spanish and foreign companies on general corporate, commercial and tax matters in national and international operations. Her experience in the aviation industry includes advising clients in the purchase, sale and financing of aircraft, aircraft leasing and maintenance contracts, mortgages and other charges and guarantees on aircraft and engines and aircraft registration.

Ventura Garcés López-Ibor

López de Hoyos, 35, 3º A 28002 Madrid / Freixa, 26-28, Baixos 08021 Barcelona, Spain
Tel: +34 91 521 78 18 (Madrid) / +34 93 241 97 40 (Barcelona) / URL: www.venturagarceslopezibor.com

Switzerland

Daniel Haeberli, Stefan Oesterhelt & Alexander Wherlock
Homburger AG

Government attitude and definition

Introduction

In Switzerland, the government's general attitude towards cryptocurrencies, and in particular towards the technology underlying cryptocurrencies, is very positive.

Both the Swiss federal government as well as the Swiss Financial Market Supervisory Authority FINMA ("**FINMA**") recognise the potential that blockchain and the distributed ledger technology ("**DLT**") offers to the financial services industry as well as various other areas of the economy. Switzerland sees an opportunity to take a global lead in this sector, and officials and authorities are generally open *vis-à-vis* new developments. This is particularly true for cantonal, *i.e.* state authorities, namely in the Canton of Zug.

In December 2018, the Swiss Federal Council published a comprehensive report covering the legal framework for DLT and blockchain in Switzerland.[1] The report generally concluded that Switzerland's current legal framework, in principle, already provides for adequate regulations, covering the questions arising in connection with the development of new technologies, such as DLT. However, a need for selective action and improvements in certain areas of private, financial market and insolvency law was identified. In light of these findings, the Swiss Federal Council published a draft law relating to blockchain and DLT ("**DLT-Draft Law**") on March 22, 2019.[2]

Definition

Swiss law does not define the term cryptocurrency or virtual currency. However, the Swiss federal government had to address the topic of virtual currencies in a special report dated June 25, 2014.[3] In this report, the following definition was used:

> "*A virtual currency is a digital representation of a value which can be traded on the Internet and although it takes on the role of money – it can be used as means of payment for real goods and services – it is not accepted as legal tender anywhere. (…) Virtual currencies exist only as a digital code and therefore do not have a physical counterpart for example in the form of coins or notes. Given their tradability, virtual currencies should be classified as an asset.*"

The same definition was later used by FINMA, when anti-money laundering regulations were being amended,[4] and the term virtual currency is also mentioned in the Swiss anti-money laundering ordinance ("**AMLO**") since January 1, 2016.[5]

However, given that there is no statutory definition and no case law, currently the best approach is to rely on the token categories introduced by FINMA in its "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (**ICO's**)" ("**FINMA**

ICO Guidelines") of February 2018.[6] Based on this classification, which is also referenced by the Swiss Federal Council in its explanatory report to the DLT Draft Law,[7] the following three categories of tokens can be distinguished:

- Payment tokens (according to FINMA, synonymous with "pure cryptocurrencies"; referred to herein as "cryptocurrencies"), are tokens which are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Pure "cryptocurrencies" do not give rise to any claims towards an issuer or a third party. Consequently, according to the prevailing view, these tokens are "purely factual intangible assets".[8] Examples of such cryptocurrencies are Bitcoin (including numerous cryptocurrencies resulting from forks or variations of Bitcoin, such as Bitcoin Cash, Bitcoin Gold and Litecoin) or Ether.
- Utility tokens are tokens that are intended to provide access digitally to an application or service by means of a DLT-based infrastructure.
- Asset tokens represent assets such as a debt or an equity claim against the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, such tokens are analogous to equities, bonds or derivatives. Tokens, which enable physical assets to be traded on a blockchain-infrastructure, according to FINMA, also fall into this category.

FINMA points out that tokens may also fall into more than one of these three basic categories. Such *hybrid tokens* are, for example, asset tokens or utility tokens, which at the same time also qualify as payment tokens.

Cryptocurrencies are not legal tender

In Switzerland, cryptocurrencies are not legal tender.[9] Consequently, cryptocurrencies do not qualify as "money" in a narrow sense. However, some legal scholars argue that cryptocurrencies, provided they are widely used, accepted by the public and have adopted the typical functions of money, qualify as "money" in a broader sense.[10] The Swiss Federal Council does, however, not seem to follow this view.[11]

Also, there is currently no form of "state-backed" cryptocurrency available in Switzerland. In particular, the Swiss National Bank, Switzerland's central bank, has not issued any cryptocurrencies, nor are there any indications that it intends to do so in the near future.[12]

The Swiss Federal Council's recent legislative initiative

The DLT-Draft Law suggests the introduction of a new concept of so-called "DLT-Rights", allowing for the tokenisation of rights, claims and financial instruments, such as bonds, shares or derivatives. The concept of DLT-Rights aims to ensure the tokenisation of rights by providing the legal framework for an electronic registration of rights that entails the same protection as a negotiable security.

Contractual claims (namely under a bond or other debt instruments) or membership rights (*e.g.*, shares in a corporation) both qualify as an admissible underlying of a DLT-Right.[13] Therefore, in particular, asset tokens could be issued as DLT-Rights under the DLT-Draft Law. On the other hand, cryptocurrencies (such as, for example, Bitcoin) that do not give rise to a claim against an issuer and therefore do not have an admissible underlying within the meaning of the DLT-Draft Law, cannot be issued in the form of DLT-Rights.[14]

The public consultation on the DLT-Draft Law ended in late June 2019 and the law will still have to be adopted by the Swiss Parliament. It is therefore still unclear whether any additional amendments will be made to the draft and when the DLT-Draft Law will enter into force.

Cryptocurrency legislation

In Switzerland, cryptocurrency-related activities are not prohibited. Further, subject to the enactment of the DLT-Draft Law, there are currently (apart from the provision in the anti-money laundering ordinance mentioned under "Government attitude and definition", above) no Swiss statutes or regulations which are tailor-made for cryptocurrencies.

Sales regulation

While offering and selling cryptocurrencies is not subject to specific Swiss sales regulations, an offer and sale of utility tokens and asset tokens may become subject to offer/sales regulations if the tokens in question constitute securities.

Under Swiss law, securities (*Effekten*) are financial instruments, which are: (i) standardised; (ii) suitable for mass trading; and (iii) either certificated securities (*Wertpapiere*), uncertificated securities (*Wertrechte*), derivatives or intermediated securities (*Bucheffekten*). Whether, or which, tokens are securities is currently not absolutely clear, *i.e.*, there is neither any statutory guidance nor any case law regarding this question. Therefore, each token will have to be subject to a specific determination on a case-by-case basis in consideration of the principles outlined by FINMA.

However, in its ICO Guidelines (see above under "Definition"), FINMA indicated that, generally speaking, it does not intend to qualify cryptocurrencies as securities. According to FINMA, utility tokens are not treated as securities if their sole purpose is to confer digital access rights to an application or service, and if the utility tokens can already be used in this way at the point of issue.

Currently,[15] FINMA has the following view on whether tokens qualify as securities or not:[16]

- Cryptocurrencies to date are not treated as securities by FINMA. In our opinion, this assessment is correct. Cryptocurrencies do not grant their holders or users any relative or absolute rights *vis-à-vis* an issuer or a third party. They serve as mediums of exchange and (arguably) also as units of account and storage of value. Whether cryptocurrencies are "financial instruments" as defined in the recently adopted Swiss Financial Services Act ("**FinSA**"), which will enter into force on January 1, 2020, remains unclear. Given the wording of the FinSA, we are of the opinion that cryptocurrencies are not "financial instruments" within the meaning of the cited Act (see also "Securities dealer licence", below).
- Utility tokens are currently not treated as securities by FINMA, provided: (i) their sole purpose is to confer digital access rights to an application or service; and (ii) the tokens can actually already be used in this manner when they are issued. If these two conditions are met, the typical "connection with capital markets" inherent to securities, according to FINMA, does not exist. FINMA points out that it will qualify utility tokens as securities if they fully or partially "have the economic function of an investment".
- Asset tokens shall, according to FINMA, generally be treated as securities; for example, if they represent uncertified securities or derivatives and are standardised as well as suitable for mass trading. As FINMA points out, uncertificated securities may also be created in so-called pre-financing and pre-sale scenarios, if claims to purchase tokens in the future are granted in the course of such processes. Such uncertified securities will also be treated as securities provided they are standardised and suitable for mass trading.

Securities dealer licence

Sales activities relating to tokens, which qualify as securities, may in particular trigger: (i) Swiss securities dealer licence requirements under the Swiss Stock Exchange and Securities Trading Act ("**SESTA**");[17] (ii) Swiss trading platform regulations under the Financial Markets Infrastructure Act ("**FMIA**");[18] and/or (iii) Swiss prospectus requirements.

- Persons creating securities tokens and/or trading in such securities on behalf of his/her clients in a professional capacity may qualify as a securities dealer under Swiss law and therefore require a securities dealer licence. For example, issuing asset tokens, which are linked to the performance of a share or a project may, under certain circumstances, qualify as regulated securities dealer activity. Such licensing requirements do, however, not apply as long as the person engaging in such activities has no physical presence (*i.e.*, no personnel and no branch) in Switzerland. Acting on a mere cross-border basis does not trigger any duty to obtain a securities dealer licence. Whilst the term securities dealer will be replaced by the term securities firm under the Financial Institutions Act ("**FinIA**"), which will enter into force on January 1, 2020, the licensing requirements for securities firms will remain substantially the same.
- Operating a platform in Switzerland which enables trading of tokens may trigger licensing requirements under the FMIA. For example, so-called "organised trading facilities" may only be operated by licensed banks, licensed securities dealers or recognised (foreign) trading venues. Organised trading facilities are establishments for: (i) multilateral trading in securities or other financial instruments whose purpose is the exchange of bids and the conclusion of contracts based on discretionary rules; (ii) multilateral trading in financial instruments other than securities whose purpose is the exchange of bids and the conclusion of contracts based on non-discretionary rules; and (iii) bilateral trading in securities or other financial instruments whose purpose is the exchange of bids. Even if the types of tokens traded are limited to such that do not qualify as securities under Swiss law, a platform may still be regulated as an "organised trading facility" if the tokens traded are qualified as "other financial instruments". Unlike for "securities", FINMA to date has not yet offered any public guidance on whether they consider cryptocurrencies to be such "other financial instruments".

  As mentioned, the FinSA will provide for a definition of the term "financial instrument" (see above, "Sales regulation"), which is commonly held to also be relevant for "organised trading facilities". This definition of "financial instrument" is wider than the definition of securities. However, in our view, the wording of the legal definition suggests that cryptocurrencies do not qualify as financial instruments within the meaning of FinSA. This view seems to be shared by the Swiss Federal Council.[19] Should this view be followed, a platform allowing for the trading of cryptocurrencies such as Bitcoin or Ether would not be considered an "organised trading facility" and would therefore fall outside the scope of the Swiss financial regulations.
- The DLT-Draft Law also provides for the introduction of a new licensing category as a DLT-Trading Venue under the FMIA. Licensed DLT-Trading Venues will be authorised to provide services in the areas of trading, clearing, settlement and custody of DLT-Securities to both regulated and unregulated financial market participants, including potentially retail investors. Under certain conditions, the trading of cryptocurrencies may also be permitted at a DLT-Trading Venue.[20] The licensing requirements for DLT-Trading Venues are mainly based on the existing requirements for trading venues (such as stock exchanges and multilateral trading facilities).

However, the FMIA will provide for specific rules for DLT-Trading Venues governing, namely, the admission of participants and the respective DLT-Securities.

Taxation

Cryptocurrencies held by individuals

- *Wealth tax*

  For the purpose of tax assessment, cryptocurrencies must be converted into Swiss francs.[21] The Federal Tax Administration ("**FTA**") provides year-end conversion rates for certain cryptocurrencies such as Bitcoin, Ethereum, Ripple, Bitcoin Cash or Litecoin. According to the understanding of different cantonal tax authorities, cryptocurrencies are considered to be assets, comparable with bank deposits, and are therefore subject to wealth taxes. If the FTA does not determine a year-end market value, the cryptocurrencies must be declared at the year-end price of the trading platform via which the buying and selling transactions are executed. If no current valuation rate can be determined, the cryptocurrency must be declared at the original purchase price in Swiss francs (cost of acquisition). Because the rules for declaring the cryptocurrencies can vary, the rules must first be checked in the canton of residence.

- *Income tax*

  In general, capital gains on assets of individuals such as cryptocurrencies are exempt from income tax.

  However, if cryptocurrencies are held as part of the business assets of an individual (e.g. because the individual is classified as a professional securities dealer based on the principles laid out in circular no. 36 of the Swiss Federal Tax Administration), capital gains of cryptocurrencies are subject to income tax.

Cryptocurrencies held by legal entities

- *Capital tax*

  Legal entities are subject to annual capital tax. Therefore, legal entities have to declare cryptocurrencies in their tax assessment at cost of acquisition or, if this value is lower, converted at the year-end exchange rate provided by the FTA. Therefore, cryptocurrencies with no market value provided by the FTA are to be declared at acquisition costs.

- *Corporate income tax*

  Corporations are subject to Swiss corporate income tax on any net taxable earnings from the sale of cryptocurrencies. Non-realised gains on cryptocurrencies are only subject to Swiss corporate income tax in case of a mark-to-market accounting in the Swiss GAAP accounts of the corporate investor.

- *VAT*

  For the purpose of VAT, cryptocurrencies are treated the same way as legal tender, meaning that the trading or exchange activities of cryptocurrencies and additional services related to such trading or exchange activities are exempt from VAT.[22]

Money transmission laws and anti-money laundering requirements

Under Swiss law, both issuing cryptocurrencies as well as the subsequent trading of such tokens may be subject to anti-money laundering requirements.

The relevant starting point is to ask whether a person/company engages in any activities, which constitute so-called financial intermediation and hence is considered a financial intermediary under the Swiss Anti-Money Laundering Act ("**AMLA**").[23]

There are two main groups of financial intermediaries. First, regulated financial intermediaries belonging to the "banking sector", and second, other financial intermediaries belonging to the "non-banking sector":

- Financial intermediaries belonging to the "banking sector" are companies that are subject to comprehensive, prudential regulation under special legislation, covering the whole range of their activities. Such financial intermediaries are, for example, banks or securities dealers.
- Financial intermediaries belonging to the "nonbanking sector" are any persons/companies, which on a professional basis: (i) accept or hold deposit assets belonging to third parties; (ii) assist in the investment of such assets; or (iii) assist in the transfer of such assets. This general definition covers, for example, persons/companies that provide services related to payment transactions, hold securities as deposits or manage securities. Whether such activity is carried out in a professional capacity or not must be assessed based on quantitative benchmarks (*e.g.,* gross margin of CHF 50,000 p.a., business relationships with more than 20 parties p.a., unlimited control over third-party assets exceeding CHF 5m at any time, or transaction volume exceeding CHF 2m per calendar year). Prior to engaging in financial intermediation, such persons/companies must either join a Swiss self-regulatory organisation ("**SRO**") or request a licence from FINMA in order to become a so-called directly supervised financial intermediary ("**DSFI**").

The AMLA and implementing regulations provide for a series of obligations that financial intermediaries must adhere to, *e.g.*, regarding the verification of the identity of customers/contracting parties as well as the beneficial owners of funds held.

With regard to cryptocurrencies, the following is important with regard to anti-money laundering regulations:

- *Primary market/ICOs*: According to FINMA, issuing cryptocurrencies constitutes financial intermediation (issuance of a means of payment).[24]
- *Secondary market/sales and trading*: Merely selling cryptocurrencies to another party, or using such cryptocurrencies as means of payment for the sale or purchase of goods and services, does not constitute financial intermediation. However, specific rules would apply if cryptocurrencies would be qualified as securities (see "Sales regulation", above). Also, depending on the services offered by the relevant person/company, activities relating to sales and trading may constitute financial intermediation, whenever a person/company on a professional basis: (i) accepts or holds cryptocurrencies belonging to third parties as a deposit; (ii) assists in the investment of cryptocurrencies; or (iii) assists in the transfer of cryptocurrencies.

Promotion and testing

Switzerland has not established any "sandbox" exemptions or similar arrangements, which specifically focus on DLT or cryptocurrencies.

However, there are specific rules in place, which aim at generally promoting fintech developments in Switzerland.

In 2016, the Swiss Government announced that it plans on reducing barriers to market entry for fintech businesses.[25] This legislative initiative has been implemented and consists of three pillars.

- The first pillar, in force since August 1, 2017, the Swiss "sandbox" exemption, allows companies to engage in activities which would usually trigger bank licensing requirements. According to the Swiss Banking Act ("**BA**"),[26] only licensed banks are allowed to accept deposits from the public in a professional capacity. Any person or entity continuously accepting more than 20 deposits from the public or publicly advertising to accept deposits is deemed to be acting in a professional capacity.[27] Under the sandbox exemption, companies accepting deposits are not considered to be acting in a professional capacity, if: (i) the deposits accepted do not exceed the threshold of CHF 1m; (ii) the deposits accepted are neither invested nor interest-bearing; and (iii) the investors are informed in advanced, in writing or in another form that provides for a record in text form, that the company is not supervised by FINMA and that the deposits are not protected by the Swiss deposit insurance regime. If the threshold of CHF 1m is exceeded, the company must notify FINMA within 10 days and file for a banking licence.
- The second pillar, in force since August 1, 2017, provides that funds held in customer accounts of asset managers, securities dealers, dealers of precious metals or similar companies, which exclusively serve the purpose of settling customer transactions, do not qualify as deposits and therefore do not trigger bank licensing requirements, provided the funds are not interest-bearing and provided that they are forwarded within up to 60 days. However, FINMA clarified that this "settlement accounts exemption" will not apply to cryptocurrency-traders which execute a similar activity as foreign exchange traders by maintaining accounts for their clients for investments in different currencies. Under what circumstances a particular activity is considered to be similar to the activities of "foreign exchange traders" is currently not clear.
- The third pillar, in force since January 1, 2019, provides for a so-called "simplified" "FinTech licence", which allows the respective licence holder to accept deposits up to the threshold of CHF 100m, provided that the deposits are neither invested nor interest-bearing. The "FinTech licence" does, however, not allow the offering and provisions of loans and mortgages. Therefore, it will be predominately crowd-funding platforms that will benefit from the simplified licence. The implementing Ordinance provides for a number of simplified requirements, relating to the required minimum capital, organisation and risk management which must be satisfied in order to obtain a Fintech licence.

Ownership and licensing requirements

Ownership

Whether tokens can actually be "owned" within the meaning of Swiss ownership laws depends, in particular, on the question of whether they qualify as securities or not. Under Swiss law, it is undisputed that securities may be legally owned. With regard to tokens, which do not qualify as securities, *i.e.*, cryptocurrencies such as Bitcoin, the ownership question is currently unresolved. The majority of Swiss scholars currently are of the view that, due to their lack of tangibility and for other reasons, cryptocurrencies are not a "thing" (*Sache*) in the sense of Swiss civil law.[28]

Licensing requirements

There are no licences/authorisations specifically relating to cryptocurrencies in Switzerland and, therefore, a variety of regulatory licences may be relevant in the area of

cryptocurrencies, in particular (but not limited to) the banking licence and the securities dealer licence (see above, "Sales regulation").

Under Swiss law, only banks are allowed to accept deposits from the public on a professional basis (see above, "Promotion and testing"). Regulated deposit-taking may become an issue for service providers offering to store customers' cryptocurrencies, in particular. It is currently not clear under which circumstances such service providers qualify as banks. This depends, in particular, on how the cryptocurrencies are being stored, and the technical details of how such storage occurs. FINMA's current position is that no banking licence is required if (i) cryptocurrencies "are transferred for safekeeping only", if these transferred cryptocurrencies are (ii) "stored separately on the blockchain for each customer", and if (iii) "each deposit can be attributed to an individual customer at all times".[29]

With regard to licensing requirements, it must further be kept in mind that Switzerland will implement the new FinIA along with the FinSA in 2020. These new acts will set forth a new licensing requirement for individual asset managers, and a registration requirement for client advisors. Such registration will be subject to certain requirements such as proof of a sufficient education, training and professional experience in the respective area of practice.

Insolvency

Under the current Swiss insolvency regime, it is not sufficiently clear whether cryptocurrencies could be segregated in favour of the entitled creditors, if a third-party custodian, such as a wallet provider, were to enter into bankruptcy proceedings. In view of these uncertainties, the DLT-Draft Law suggests certain amendments to the Swiss Debt Enforcement and Bankruptcy Act, in order to allow the segregation of cryptocurrencies frothe bankruptcy estate of an insolvent third party custodian.

The segregation in favour of the creditor will, however, require that the crypto assets in question can unambiguously be allocated to the respective creditor.[30] Therefore, the custody set-up under which the cryptocurrencies are stored is decisive for the question whether the cryptocurrencies can be segregated in insolvency. Pursuant to the Explanatory Report to the DLT-Draft Law, cryptocurrencies stored by a third party can be allocated to a specific client and can therefore be segregated in insolvency, if the custody set-up ensures that a client's balance can be tracked to a specific blockchain address and that said address is stored directly on the blockchain.[31]

Mining

Switzerland has no laws or regulations which are tailor-made to the phenomenon of cryptocurrencies or mining of cryptocurrencies. Hence, mining of cryptocurrencies is permitted and the activity is not subject to particular laws and regulations.

Since the mere use of cryptocurrencies is not considered as financial intermediation (see above, "Money transmission laws and anti-money laundering requirements"), mining does not constitute financial intermediation, as far as it is for personal use.[32] Further, mining does not qualify as a financial service within the meaning of FinSA.[33]

Border restrictions and declaration

In Switzerland, there are no particular border restrictions or declaration requirements that would apply to cryptocurrencies.

Reporting requirements

In Switzerland, making payments with cryptocurrencies is not a regulated activity and there are no reporting requirements to be met when such payments are made.

Estate planning and testamentary succession

In Switzerland, there are no particular estate planning or testamentary succession aspects concerning cryptocurrencies.

Under Swiss law, heirs acquire the inheritance as a whole upon death of the testator by operation of law. Therefore, all possessions with an inheritable value are transferred to the heirs by universal succession.

Cryptocurrencies such as Bitcoin are considered as having an inheritable value.[34] They are part of the inheritance and are therefore transferable. Bitcoins that are recorded on a blockchain are attached to the latter. It is recommended to determine the heir of the cryptocurrency assets, thereby taking into account the value of these assets for calculating the recipient's share. Problems arise when the heir does not possess the necessary means (usually the private keys) to dispose of the inherited cryptocurrencies.

* * *

Acknowledgment

The authors acknowledge with thanks the contributions of Manuel Dubach and Urs Meier to this chapter.

* * *

Endnotes

1. Federal Council Report – Legal framework for distributed ledger technology and blockchain in Switzerland, dated December 14, 2018 (https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf).
2. *Cf.* https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-74420.html.
3. *Cf.* https://www.newsd.admin.ch/newsd/message/attachments/35355.pdf.
4. *Cf.* https://www.finma.ch/en/news/2015/06/mm-gwv-finma-20150623/.
5. *Cf.* article 4 paragraph 2 of the Swiss Anti-Money Laundering Ordinance: "Money or asset transfer transactions are deemed to be the transfer of assets through the acceptance of cash, precious metals, virtual currencies (…)."
6. *Cf.* FINMA ICO Guidelines, p. 2 *et seq*. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.
7. Federal Council Explanatory Report – DLT-Draft Law, p. 83 *et seq.* (https://www.newsd.admin.ch/newsd/message/attachments/56192.pdf).
8. Federal Council Explanatory Report – DLT-Draft Law, p. 8; Zogg, Bitcoin als Rechtsobjekt – eine zivilrechtliche Einordnung, in: recht 2019, p. 95 *et seq*.
9. The Swiss Federal Act on Currency and Payment Instruments determines Switzerland's legal tender. To date, only (i) coins issued by the Federal Government,

(ii) banknotes issued by the Swiss National Bank, and (iii) Swiss franc sight deposits at the Swiss National Bank qualify as legal tender. Legal tender is considered as "money" in the narrow sense and as legal tender are an official means of payment.

10. *Cf.* Hauser-Spuehler/Meisser, Eingenschaften der Kryptowährung Bitcoin, in: digma 2018, p. 7; Müller/Reutlinger/Kaiser, Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und in der Europäischen Union, in EuZ 2018, p. 80.
11. Federal Council Explanatory Report – DLT-Draft Law, p. 52.
12. https://www.snb.ch/en/mmr/speeches/id/ref_20180405_amr.
13. *Cf.* Kramer/Oser/Meier, Tokenisierung von Finanzinstrumenten de lege ferenda, in: Jusletter May 6, 2019, N 22.
14. Federal Council Explanatory Report – DLT-Draft Law, p. 29.
15. It must be noted that this is a novel and rapidly developing field of law and different views can be taken as to the classification of crypto assets as securities under Swiss law. In light of this, it cannot be excluded that FINMA will come to a different conclusion in the future, in particular with regard to cryptocurrencies. FINMA noted that they would reconsider their conclusion in light of the views taken in any future case law or any new legislation in this area.
16. *Cf.* FINMA ICO Guidelines, p. 4.
17. Federal Act on Stock Exchanges and Securities Trading of March 24, 1995, SR 954.1.
18. Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading of June 19, 2015, SR 958.1.
19. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 122.
20. *Cf.* Federal Council Explanatory Report – DLT-Draft Law, p. 50.
21. *Cf.* Swiss Legal Tech Association (SLTA), *Regulatory Task Force Report*, p. 33; the Federal Tax Administration publishes every year end an exchange list (official exchange rate) for Bitcoin, Ethereum, Ripple, Bitcoin Cash, Litecoin, Cardano, NEM, Stellar, IOTA and Tron.
22. *Cf.* Swiss Legal Tech Association (SLTA), Regulatory Task Force Report, p. 33.
23. Federal Act on Anti-Money Laundering of October 10, 1997, SR 955.0.
24. *Cf.* FINMA ICO Guidelines, p. 6.
25. *Cf.* https://www.sif.admin.ch/sif/en/home/dokumentation/medienmitteilungen/medienmitteilung.msg-id-61427.html.
26. Federal Act on Banks of November 8, 1934, SR 952.0.
27. *Cf.* articles 2 and 6 of the Swiss Banking Ordinance of April 30, 2014, SR 952.02.
28. *Cf.* Mueller/Reutlinger/Kaiser, p. 86 *et seq.*; Maurenbrecher/Meier, Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen; Eggen, Chain of Contracts – Eine privatrechtliche Auseinandersetzung mit Distributed Ledgers, AJP 2017, p. 14; Bärtschi/Meisser, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Weber/Thouvenin (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zurich 2015, p. 141.
29. *Cf.* FINMA fact sheet on "virtual currencies" dated January 1, 2019, p. 2.

30. *Cf.* Federal Council Explanatory Report – DLT-Draft Law, p. 39.
31. *Cf*. Kramer/Meier, Crypto assets and data in insolvency: Switzerland's proposed new rules, in: International Insolvency & Restructuring Report 2019/20, p. 51.
32. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 148.
33. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 124.
34. *Cf*. Eigenmann/Fanti, Successions, Données Personnelles, Numériques et Renseignements, in: SJ 2017 II, p. 198.

Daniel Haeberli
Tel: +41 43 222 16 33 / Email: daniel.haeberli@homburger.ch
Daniel Haeberli is a banking and finance as well as a capital markets transactions and financial market regulations specialist. He is particularly focused on secured lending, syndicated debt and structured financing as well as derivatives, securitised structured products, investment funds and bond offerings. Daniel regularly advises clients on initial coin offerings (ICOs) and on cryptocurrency matters.
Daniel Haeberli heads the working group "Legal & Regulation" of the Swiss Structured Products Association SSPA.

Stefan Oesterhelt
Tel: +41 43 222 12 65 / Email: stefan.oesterhelt@homburger.ch
Stefan Oesterhelt's practice focuses on tax law, in particular international tax law, mergers and acquisitions, capital market transactions and tax litigation. He is a lecturer on tax law at the University of Sankt Gallen and regularly speaks at seminars on tax law.

Alexander Wherlock
Tel: +41 43 222 17 50 / Email: alexander.wherlock@homburger.ch
Alexander Wherlock's practice focuses on financial markets and banking law, financial services regulation as well as corporate and commercial law. Alexander Wherlock is also a member of Homburger's practice group "Technology and Digital Economy".

Homburger AG

Hardstrasse 201, 8005 Zurich, Switzerland
Tel: +41 222 10 00 / URL: www.homburger.ch

Taiwan

Robin Chang & Eddie Hsiung
Lee and Li, Attorneys-at-Law

Government attitude and definition

Prior to the end of June, 2019 while Taiwan had not promulgated any laws or regulations specifically dealing with the rise of certain applications of blockchain technology such as so-called "virtual currencies" or "cryptocurrencies", Taiwan's financial regulators had issued several press releases to announce their positions and attitude towards such developments, as well as to educate and warn the general public in Taiwan.

On 30 December 2013, both the Central Bank of the Republic of China (Taiwan) ("CBC") and Taiwan's Financial Supervisory Commission ("FSC") first expressed the government's position toward Bitcoin by issuing a joint press release ("2013 Release"). According to the 2013 Release, the two authorities held that Bitcoin should not be considered a "currency", but a highly speculative digital "virtual commodity". In another FSC press release in 2014 ("2014 Release"), the FSC ordered that local banks must not accept Bitcoin or provide any other services related to Bitcoin (such as the exchange of bitcoins for fiat currency). The FSC further issued a press release on 19 December 2017 ("2017 Release"), in which the FSC reiterated the government's positions as specified in the 2013 Release and 2014 Release.

Given the above, in light of the authorities' attitude, Bitcoin is not considered "legal tender", "currency" or a generally accepted "medium of exchange" under the current regulatory regime in Taiwan; instead, Bitcoin is deemed as a digital "virtual commodity". Please note that the government's attitude stated in the abovementioned press releases only cover Bitcoin, instead of any other types of virtual currencies/cryptocurrencies (except for initial coin offerings "ICOs" as further explained below). But we tend to think that any other virtual currencies/cryptocurrencies, if having the same nature and characteristics as Bitcoin, should also be considered as digital "virtual commodities".

Please note that, with regard to the offering and issuance of any tokens with the nature of securities (which are commonly called "security tokens", and their offering commonly called "security token offerings" ("STOs")), the FSC issued a press release on June 27, 2019 to illustrate the FSC's proposed regulations on STOs. Please see "Sales regulation" below for more details on the proposed STO regulations.

Cryptocurrency regulation

Please see "Government attitude and definition" above. So far, except for the proposed STO regulations discussed under "Sales regulation" below, no Taiwanese laws or regulations have been promulgated or amended to formally regulate "virtual currencies" or "cryptocurrencies"; therefore, currently, virtual currencies/cryptocurrencies cannot be considered "legal tender", "currencies" or a generally accepted "medium of exchange" in Taiwan.

Further, currently there exists no required licence in Taiwan for (a) operating the services of exchange between virtual currencies or virtual currencies with fiat currencies, or (b) acting as a "money transmitter" and the like in Taiwan.

Sales regulation

Sale of bitcoins or any other virtual currencies/cryptocurrencies of the same nature and characteristics

So far, except for the proposed STO regulations discussed below, there exist no laws or regulations specifically dealing with the sale of virtual currencies/cryptocurrencies. The sale of bitcoins, currently considered by the FSC as sale of a digital "virtual commodity" but not "currency", should generally be fine from a Taiwan regulatory perspective, and the general principles and rules governing "purchase and sale" under the Civil Code would apply if the consideration is cash. Also, we tend to think that the above would apply to the sale of other virtual currencies/cryptocurrencies of the same nature and characteristics as Bitcoin.

Please note that the above is subject to "ICO and token offering" as described below.

ICO and token offering

In response to the rising amount of ICOs and other investment activities regarding virtual currencies/cryptocurrencies, the FSC also expressed the following view on ICOs through the 2017 Release as mentioned above:

(1) An ICO refers to the issue and sale of "virtual commodities" (such as digital interests, digital assets, or digital virtual currencies) to investors. The classification of an ICO should be determined on a case-by-case basis. For example, if an ICO involves offer and issue of "securities", it should be subject to Taiwan's Securities and Exchange Act ("SEA"). The issue of whether tokens in an ICO would be deemed "securities" under the SEA would depend on the facts of each individual case.

(2) If any misrepresentations with respect to technologies or their outcomes and/or promises of unreasonably high returns are used by the issuer of virtual currencies or an ICO to attract investors, the issuer would be deemed to be committing fraud or illegal fund-raising.

Given the above, in an ICO (or other type of token offering, such as private token pre-sale before the ICO stage), the core issue in this regard is whether an ICO would be considered issuing "securities" under Taiwan's securities regulations. Under current Taiwan law, the offer and sale of "securities" in Taiwan, whether through public offering or private placement, are regulated activities and shall be governed in accordance with the SEA, its related regulations as well as relevant rulings issued from time to time by the FSC.

The term "securities" has a very broad (but maybe not clear enough) definition in Taiwan. According to Article 6 of the SEA, "securities" could mean government bonds, corporate stocks, corporate bonds, and other securities approved by the competent authority, and any stock warrant certificate, certificate of entitlement to new shares, and certificate of payment or document of title representing any of the above securities shall be deemed securities. Additionally, according to a recent Taiwan Supreme Court opinion, a contract or agreement would be considered securities under the SEA if it has monetary value, the nature of investment and transferability.

However, although it was advised in the 2017 Release that offering and issuance of any tokens with the nature of securities (i.e., STO) should be subject to the SEA, currently the SEA and its related regulations have not set out the relevant rules governing the filing for

such prior approval or registration. In other words, at the time of writing, no regulatory process is available in Taiwan for said prior approval or registration. Given this, in order to respond to advocates from the blockchain and cryptocurrency industries, the FSC has been planning to promulgate relevant regulations governing STOs to fill the void. For this purpose, the FSC held a public hearing on 12 April 2019, inviting views and opinions from industry experts on the proposed STO regulations. Later, on 27 June 2019, the FSC issued a press release to illustrate the FSC's proposed regulations on STOs. Some of the key points are as summarised below:

- To expressly approve security tokens as securities under the SEA: For this purpose, the FSC issued a ruling on 3 July 2019 to officially define security tokens as a type of securities under the SEA.
- To set an upper limit of the total amount of an STO programme: the contemplated amount of such upper limit is NT$30,000,000 (around US$1,000,000).
- To set qualifications for the buyers of security tokens: the contemplated qualifications are that the buyers should be limited to "professional investors" and, in case such professional investor is an individual, the upper limit of the total amount of his/her subscription would be NT$300,000 (around US$10,000).
- To require each STO to be on a single platform.
- To require that only FSC-licensed securities dealers may serve as STO platform operators, with a minimum capital amount of NT$100,000,000 (around US$3,333,333), lower than that required for a traditional FSC licensed securities dealer.

In addition to the above, the FSC will authorise the Taipei Exchange to further promulgate the relevant regulations governing STOs. In July of 2019, the FSC also announced proposed amendments to the relevant regulations governing the securities dealers conducting proprietary trading in security tokens, so corresponding further amendments to relevant securities-related regulations are expected.

Taxation

There is currently no regulation specifically governing the taxation of cryptocurrencies; however, by referring to the tax laws and tax rulings in connection with the taxation of cross-border e-commerce transactions and online sales of services, it is possible that the tax authorities might take the following stances:

(1) Business Tax (also known as value-added tax or "VAT")

The trading of cryptocurrencies on a platform within Taiwan may be deemed as a sale of services within Taiwan and thus be subject to Taiwan business tax as follows:

(i) If the seller is a Taiwan business entity, the seller will be subject to 5% VAT on the revenue.

(ii) If the seller is a Taiwanese individual, the individual should apply for tax registration and pay 5% VAT on the revenue, unless the monthly sales amount is under NT$40,000 (approx. US$1,300).

(iii) If the seller is a foreign entity with a fixed place of business in Taiwan (e.g., a Taiwan branch), the Taiwan branch should pay 5% VAT on such revenue.

(iv) If the seller is a foreign entity without a fixed place of business in Taiwan, and the purchasers of the cryptocurrencies are entirely Taiwanese entities, the seller will have no business tax issue; instead, the purchasers will become the taxpayer.

(v) If the seller is a foreign entity without a fixed place of business in Taiwan, and the purchasers of the cryptocurrencies include Taiwanese individuals, the foreign seller should apply for tax registration and pay 5% VAT on the revenue generated from the sale of the cryptocurrencies to the Taiwanese individuals, unless the monthly sales amount to the Taiwanese individuals is under NT$40,000 (approx. US$1,300).

(2) Income Tax

Any income generated from the trading of cryptocurrencies on an onshore platform ("Trading Income") may be deemed as income sourced from Taiwan and thus be subject to Taiwan income tax as follows:

(i) If the seller is a Taiwan business entity, the seller should consolidate the Trading Income into its other taxable income for calculating its Taiwan income tax payable. (The prevailing income tax rate is generally 20% on the net taxable income.)

(ii) If the seller is a Taiwanese individual, the individual should consolidate the Trading Income into its other taxable income for calculating its Taiwan income tax payable. (The prevailing highest progressive tax rate is 40% on the net taxable income.)

(iii) If the seller is a foreign entity with a fixed place of business in Taiwan (e.g., a Taiwan branch), the Taiwan branch should consolidate the Trading Income into its other taxable income and pay income tax accordingly. (The prevailing income tax rate is generally 20% on the net taxable income.)

(iv) If the seller is a foreign entity with a business agent in Taiwan, the business agent should, on behalf of the foreign entity, file an income tax return, report the Trading Income, and pay income tax accordingly. (The prevailing income tax rate is generally 20% on the net taxable income.)

(v) If the seller is a foreign entity without a fixed place of business or business agent in Taiwan, the seller should file an income tax return (the seller may engage a tax agent to file the tax return on its behalf), report the Trading Income, and pay income tax accordingly. (The prevailing income tax rate is generally 20% on the net taxable income.)

Money transmission laws and anti-money laundering requirements

As advised under "Cryptocurrency regulation" above, currently there exists no required licence for (a) operating the services of exchange between virtual currencies or virtual currencies with fiat currencies, or (b) acting as a "money transmitter" and the like in Taiwan.

As for anti-money laundering, the latest amended Money Laundry Control Act ("Taiwan AML Act") of Taiwan, which took effect on 7 November 2018, has brought the cryptocurrency platform operators into the anti-money laundry regulatory regime. However, as of now, how it will be implemented and what requirements will be imposed by the FSC (which is the main regulator of the Taiwan AML Act) are not clear at this stage in terms of anti-money laundering activities of cryptocurrency exchanges and platforms.

Promotion and testing

Taiwan's law for the fintech regulatory sandbox, the "FinTech Development and Innovation and Experiment Act" ("Sandbox Act"), was promulgated on 31 January 2018 and took effect on 30 April 2018. The Sandbox Act was enacted to enable fintech businesses to test their financial technologies.

According to the Sandbox Act, an applicant (which can be an entity or individual) needs to obtain approval from the FSC before entering the sandbox. Once the experiment begins, the experimental activities may enjoy exemptions from certain laws and regulations (such as FSC licensing requirements and certain legal liability exemptions).

After completion of the approved experiments, the FSC will analyse the results of the experiments. If the result is positive, the FSC would actively examine the existing financial laws and regulations to explore the possibility of amending them, after which the business model or activities previously tested in the sandbox could become feasible under law. Please note, however, that the sandbox entity or individual might still be required to apply for a relevant licence or approval from the FSC in order to formally conduct the activities as previously tested in the sandbox.

At the time of the writing, according to relevant news articles, there have been six applications approved by the FSC to enter into the sandbox, but none of them are related to cryptocurrencies. Nonetheless, please note that according to relevant news reports, under the proposed STO regulations as advised above, there would be an upper limit for the total amount of an STO programme, and the FSC mentioned that any proposed STO exceeding such upper limit may need to be first tested and experimented with in the regulatory sandbox.

Given so, it is possible that the relevant STO market players, as well as some controversial fintech business models and activities (e.g., ICOs), would wish to apply to the FSC to enter the sandbox. However, according to the Sandbox Act, any experimental activity needs to be "innovative". Therefore, (a) whether or not the commonly seen cryptocurrency-related activities (such as ICOs and/or STOs) would enter the sandbox, and (b) if yes, whether the result of the experiment would be considered "positive", would still depend on the FSC's then-effective policies and final decision.

Ownership and licensing requirements

As mentioned above, Taiwan has not promulgated any laws or regulations specifically dealing with "virtual currencies" or "cryptocurrencies", so there exists no ownership or licensing requirements under Taiwanese law, except for "ICO and token offering" as advised under "Sales regulation" above. Under current Taiwanese law, the offer and sale of "securities" in Taiwan are regulated activities. In other words, theoretically speaking, any offer or sale of ICOs or tokens in Taiwan needs to obtain the FSC's approval beforehand if such ICOs or tokens are considered to be "securities" under the SEA. However, currently such approval is not available under the SEA and its related regulations. But please note the proposed STO regulations as described above.

Mining

So far, no Taiwanese laws or regulations have been promulgated or amended to regulate the "mining" of Bitcoin or any other types of cryptocurrency. Mining activities are generally permitted.

Border restrictions and declaration

So far, no Taiwanese laws or regulations have been specifically promulgated or amended to impose any border restrictions on, or requirements for, declaration of holdings of cryptocurrencies.

Reporting requirements

So far, no Taiwanese laws or regulations have been specifically promulgated or amended to impose any reporting requirement for cryptocurrencies.

Estate planning and testamentary succession

So far, Taiwan's laws and regulations have not addressed this topic. Since cryptocurrencies have value, we tend to think they would be considered as "property" or "assets" from the perspective of Taiwan estate and succession law, unless they are confiscated by the government due to, for example, the commission of a criminal offence violating the prohibition of "securities" offering without prior approval from, or registration with, the FSC as required under the SEA (see our advice under "Sales regulation" above).

Robin Chang
Tel: +886 2 2763 8000 ext. 2208 / Email: robinchang@leeandli.com

Robin Chang is a partner at Lee and Li and the head of the firm's banking practice group. His practice focuses on banking, IPOs, capital markets, mergers and acquisitions, project financing, financial consumer protection law, personal data protection law, securitisation and antitrust law.

Mr. Chang advises major international commercial banks and investment banks on their operations in Taiwan, including providing advice on compliance and regulatory issues, setting up a banking branch or bank subsidiary in Taiwan and customer complaints. He has been involved in many M&A transactions of financial institutions. He has also been involved in government projects on e-payment regulations in Taiwan.

Eddie Hsiung
Tel: +886 2 2763 8000 ext. 2162 / Email: eddiehsiung@leeandli.com

Eddie Hsiung is licensed to practise law in Taiwan and New York, and is also a CPA in Washington State, U.S.A. His practice focuses on securities, M&A, banking, finance, asset and fund management, cross-border investments, general corporate and commercial, FinTech, startups, etc.

He regularly advises leading banks, securities firms, payment/credit cards and other financial services companies on transactional, licensing and regulatory/compliance matters as well as internal investigation. He is experienced in advising asset management companies and issuers on the sale of offshore funds and other investment products in Taiwan. He is familiar with derivatives and FinTech issues (ICOs, cryptocurrencies, platform operators, e-payment, digital financial services, regulatory sandbox, etc.).

Lee and Li, Attorneys-at-Law

8F, No. 555, Sec. 4, Zhongxiao E. Rd., Taipei 11072, Taiwan, R.O.C.
Tel: +886 2 2763 8000 ext. 2208 / Fax: +886 2 2766 5566 / URL: www.leeandli.com

United Arab Emirates

Abdulla Yousef Al Nasser, Flora Ghali & Nooshin Rahmannejadi
Araa Group Advocates and Legal Consultants

Government attitude and definition

Blockchain is considered the fourth industrial revolution and a hot topic. It has been the subject of numerous studies in various fields outside the payments industry to which it has often been confined in the past, which is fully saturated with technology. The UAE government considered blockchain as a foundation stone for improving productivity and to make payment processes efficient. Blockchain is the database technology behind cryptocurrencies such as Bitcoin and can work as a real-time archive for recording the history of financial transactions, contracts, physical assets and supply-chain information. There is no one person or entity in charge of the entire chain. It is an open network and everyone in the chain can see the details of each record. Every block is encrypted and can only be edited by its owner with a private key. If any change or edit is made, the entire chain is updated in real time.

The UAE government strongly supports blockchain technology and its main aim is to handle at least 50% of federal government transactions over the blockchain platform. The government has taken this initiative with the aim to make annual savings of more than AED 10 billion, almost 400 million printed documents, around 2 billion kilometres of driving and around 77 working hours per week.

In October 2016, His Highness Sheikh Hamdan Bin Mohammad Bin Rashid Al Maktoum launched Dubai's blockchain strategy. The main aim is to make Dubai fully powered by blockchain technology by 2020. In Dubai, the initiative is run by a collaboration between the Smart Dubai Office and the Dubai Future Foundation. Dubai's strategy has three main pillars: government efficiency; industry creation; and international leadership. Dubai is playing an important role in the development of blockchain technology with the creation of the Global Blockchain Council.

The UAE will use blockchain technology for digital transactions, giving each customer a unique identification number that points to their information on a secure chain. Information and data on the blockchain cannot be hacked or changed, which will ensure the digital security of national documents and transactions and eventually reduce operational costs and accelerate decision-making.

As part of this vision and as a result, the Global Blockchain Council was established to explore, discuss current and future applications, and organise transactions through the blockchain platform. The Council will highlight the implications of this innovation on the future of the business and finance sectors, and its role in facilitating transactions within the various financial and non-financial sectors, as well as increase efficiency and reliability.

Also, within its efforts in this field, the UAE's Securities and Commodities Authority ("SCA") will introduce regulations for initial coin offerings ("ICOs") in the country by the

end of 2019, a move aimed at providing companies with another avenue to raise capital through crowdfunding.

The SCA, which supervises and monitors the markets, has approved ICOs as securities and will work with the Abu Dhabi Securities Exchange and Dubai Financial Market to develop trading platforms for ICOs next year. The SCA will facilitate the Abu Dhabi and Dubai stock markets with the adoption of the latest blockchain technology, using cryptography, for the issuance of ICOs.

Cryptocurrency is an encrypted digital currency that operates using blockchain technology. Unlike fiat currency, which is regulated by a single entity such as a central bank, cryptocurrencies are validated through a decentralised system whereby any party participating in the process can verify the transactions that take place.

Cryptocurrency generally received a warm welcome in UAE but also experienced a more mixed reception from the regulators' side. To strengthen its vision, the UAE Government recently issued regulations on the use of cryptoassets, including cryptocurrencies. Generally speaking, there are specific pieces of legislation that cover cryptocurrencies. Financial regulatory authorities in the UAE issued warnings against the risk involved in certain cryptocurrencies and ICOs. The UAE Central Bank's position remains uncertain to some extent as digital payment rules explicitly prohibit virtual currencies, but continued to make a clear statement that these restrictions do not apply to cryptocurrencies. However, only a few free zones have issued licences to those business entities dealing with cryptocurrencies.

Clearly, the UAE Government is committed to developing its own cryptocurrency. Dubai developed its own cryptocurrency in October 2017 named EMCASH, which is used as part of a payment system for school fees and governmental services. It was launched as a joint venture between Emcredit Limited and The Object Tech Group Limited, a UK-based company. In December, another cryptocurrency was announced, which is used for payments in cross-border transactions with Saudi Arabia. It is clear that the UAE Government has taken the initiative with cryptocurrencies, so there is no doubt that the regulatory regime will be developed accordingly.

Cryptocurrency regulation

In the UAE, the Securities and Commodities Authority, the governmental body that regulates the UAE's financial and commodities markets, issued a circular on 2 April 2018 (the "Circular") in which it warned investors against digital, token-based fundraising activities which include ICOs. The SCA reiterated that it does not recognise, regulate or supervise any ICOs, and by investing in any ICOs, the investors are doing so at their own risk. Through the Circular, the SCA raised awareness surrounding the risks associated with ICOs. In particular, the SCA highlighted that:

- some ICOs are not subject to regulation and therefore may be subject to fraud risks;
- ICOs may be issued abroad, and are therefore subject to foreign laws and regulations that can be difficult to verify; this means that tracking and recovering funds in cases where ICOs have collapsed may prove to be extremely difficult;
- ICO trading on the secondary market is subject to opaque, volatile pricing and may possess insufficient liquidity;
- investors, in particular retail investors, may not be able to comprehend the risks, costs, and expected returns associated with ICOs; and

- the information made available to potential investors through the White Paper or otherwise may be unaudited and/or incomplete and may present the relevant investment in an unbalanced and/or misleading manner.

The Abu Dhabi Global Markets (the "ADGM")

The Government of Dubai has sought to promote the use of blockchain technology by introducing the "Dubai Blockchain Strategy". Upon successful implementation of this strategy, Dubai aims to become the first "blockchain powered government". Following on from this, the Dubai Land Department ("DLD") is developing its own blockchain system to record all real estate contracts and link DLD with utility companies such as the Dubai Electricity & Water Authority. The blockchain system will also allow tenants to make payments electronically, resulting in such transactions being paperless and therefore cost-efficient.

The DLD aims to push all boundaries by allowing transactions to be completed without requiring parties to appear in person before any government entity.

Financial institutions such as banks are also turning to blockchain technology to not only improve efficiency of their Know Your Customer ("KYC") processes but to also assist in complying with anti-money laundering requirements. The ADGM has launched an e-KYC utility project with a consortium of UAE financial institutions which aims to develop a governance framework to set out the requirements of the e-KYC utility using distributed ledger technology.

The legal sector may also witness another interesting development – smart contracts. A smart contract is a digital contract that automatically verifies fulfilment of conditions and then executes agreed terms. This will, in turn, contribute to Dubai's aim to have paperless transactions.

With the aim of providing another platform for companies, the UAE's Securities and Commodities Authority will introduce the ICO rules in the country in 2019. The SCA has recognised ICOs as securities, and in partnership with the Abu Dhabi Securities Exchange and Dubai Financial Markets, will develop trading platforms for ICOs by 2021.

The identical treatment depends on (1) geographical location, and (2) how the applicable regulator classifies or sees them in that area. The activities of the financial free zones are regulated by its own regulators; for example, in the DIFC, the Dubai Financial Services Authority ("DFSA").

On 13 September 2017, the DFSA issued a warning to potential investors of ICOs. In its warning, the DFSA made it clear that it does not regulate "these types of product offerings or license firms in the DIFC to undertake such activities". In addition, the DFSA urged potential investors to exercise caution and undertake their own due diligence to better understand the associated risks before engaging with firms offering such investments in the DIFC, and/or before making any financial contributions towards such investments. Additionally, the Financial Services Regulatory Authority ("FSRA"), in the ADGM, has discretion as to how to classify and control cryptocurrency. The ADGM, through the FSRA, issued its own guidance to investors proposing to invest in ICOs. The guidance provided by the ADGM on 8 October 2017 (the "Guidelines"), aims to inform investors of the legal and regulatory treatment of raising funds through ICOs in the ADGM.

The Guidelines should be read in conjunction with the Financial Services and Markets Regulations 2015 ("FSMR"). If tokens in an ICO are assessed for characteristics of a 'Security', then such tokens can be classified as 'Security Tokens' and thus may be subject to the ADGM's regulatory obligations/requirements.

Guidance Note 3.10 further clarifies that not all ICOs will constitute an 'Offer of Securities' under the Market Rules or FSMR. If the tokens do not exemplify the features and characteristics of securities, the offer of such tokens is not likely to be an 'Offer of Securities' (each as defined in the FSMR and the ADGM Glossary) and neither is the trading of such tokens likely to constitute a 'Regulated Activity' under the FSMR.

If an issuer is proposing an ICO in or from the ADGM, then it should aim to approach the FSRA at the earliest opportunity to ensure it can rely on certain exemptions and avoid falling foul of the ADGM regulatory regime.

On 30 April 2018, the FSRA published a consultation paper on a proposed framework to administer spot cryptoasset activities to be undertaken in the ADGM. It is clearly evident that the FSRA is seeking to instil proper governance, transparency and oversight in and over cryptoasset activities. The proposed cryptoasset regulatory framework supplements the FSRA's Guidance on Initial Coin/Token Offerings and Crypto Assets released in 2017. However, until the proposed framework comes into force, ICOs comprising tokens which exhibit the characteristics of securities will continue to be treated as such within the FSRA's regulatory framework.

Following this uncertainty in the market that reached the extent of prohibition, the Governor of the UAE Central Bank published a statement clarifying that the regulations do not apply to cryptocurrencies, crypto exchanges, or underlying technology such as blockchain technology. The Governor added that virtual currencies were under review by the UAE government and that appropriate legal regulations would be issued in due course.

Until the regulatory framework is amended or new regulations are issued to deal with virtual currencies, the regulatory framework remains valid, and technically speaking the UAE Central Bank can take action against existing and proposed businesses dealing in virtual currencies.

In the rest of the UAE, cryptocurrencies are deemed to be a commodity or securities which fall under the control of the UAE's Securities and Commodities Authority, or if they are deemed to be a currency like AED they fall under the control of the UAE Central Bank. There is always the possibility of overlap in the responsibilities and cooperation between the two regulators.

United Arab Emirates SCA Chairman and Finance Minister Sultan bin Saeed Al Mansouri recently announced that the SCA has approved a plan to recognise digital tokens as securities and to introduce a specific framework and manage cryptoasset operations, including ICOs, exchanges and other intermediaries. Following the review of the UAE Securities Regulator of Best Global Practices, the SCA's project is one of several initiatives aimed at ensuring that the securities industry in the UAE generally complies with best international standards.

According to a statement made by SCA, the new regulations will address the full range of the issuance cycle associated with crypto-fundraising, including: "*... the type of issue (private/public), the entities that can make the issuing and the legislative requirements thereof, such as, inter alia, registration and fees, Blockchain operators, the targeted entities by issue type, the minimum content of the prospectus (white paper), liability thereof, and whether registration is or is not required by issue type*." It is hoped that the new framework will include detailed regulations covering key risks, such as money laundering, anti-terrorism financing, consumer protection, technical governance and safe custody. The proposed resolution will come into force once it is published in the UAE's Official Gazette.

The announcement signals a change in the position of the SCA, which previously stated that it neither restricted nor authorised ICOs. The SCA's decision to recognise digital tokens as securities and to introduce a specific framework for controlling cryptoasset activity marks an important step in achieving better control over digital securities and commodities in the UAE. It remains to be seen how the newly proposed legislative framework will apply in practice. As noted, it is still unclear whether the new regulatory framework will consider all digital tokens, including "utility tokens", as securities, and whether these will be covered by the SCA. Digital tokens issuers should seek legal advice as soon as possible to protect them from the risk of law violations.

The DFSA would like to make it clear that it does not currently regulate these types of product offerings or licence firms in the DIFC to undertake such activities. Accordingly, before engaging with any persons promoting such offerings in the DIFC, or making any financial contribution toward such offerings, the DFSA urges potential investors to exercise caution and undertake due diligence to understand the risks involved.

In January 2017, the UAE Central Bank released the Regulatory Framework for Electronic Payment Systems ("Stored Value Restrictions"). The regulations were issued to regulate payments and stored value. They make only one scant reference to virtual currencies and define them as a digital unit used as a medium of exchange, a unit of account, or a form of stored value. The rules stipulate that they are not protected, but are confused and suggest that their use is prohibited. In February 2017 and October 2017, the UAE Central Bank made statements that were published in the media clarifying that trading in Bitcoin or other cryptocurrencies and altcoins was not covered by the Stored Value Regulations. The view of the UAE Central Bank was that trading in cryptocurrencies was a "tolerated practice".

There have also been some noteworthy announcements of transactions and investments that would be available in Bitcoin. One Dubai real estate property announced that it would sell property units in Bitcoin.

In January 2018, Emirates NBD announced that it would cease to process "suspicious" Bitcoin-related transfers that affected account holders on cryptocurrency trading platforms. The bank later clarified that it did not prohibit customers from engaging in transactions with trading platforms trading in digital assets but was restricted to prohibiting suspicious transactions flagged for financial crime.

Like US and EU regulators, the UAE is spending immense energy, talent and resources in order to address the reality of virtual currencies whilst defining a common regulatory framework.

Sales regulation

Sales of cryptocurrencies in the UAE are mainly regulated by the DIFC, ADGM and the rest of the UAE.

As per the statement issued by the DFSA, the official regulator of the DIFC, it does not grant licences to any company to issue cryptocurrencies in the DIFC.

In ADGM, a new regulatory framework for cryptocurrencies named 'Operating a Crypto Asset Business' ("OCAB") has been introduced under the regulations. OCAB is broadly drafted because it is a regulatory activity and includes almost all aspects related to cryptocurrency. Pursuant to the OCAB framework, however, market intermediaries (e.g., broker dealers, custodians, asset managers) dealing in or managing cryptoassets, and cryptoasset exchanges, need to be licensed/approved by FSRA as OCAB Holders. Only

activities in 'Accepted Crypto Assets' will be permitted. Capital formation activities are not provided for under the OCAB framework, and such activities are not envisaged under the Market Rules (MKT). For clarification, the OCAB framework is not intended to apply to initial token or coin offerings (whether digital securities or utility tokens), or other capital formation/capital raising purposes. For details on FSRA's regulatory treatment of ICOs, digital securities and utility tokens please refer to the FSRA's ICO Guidance. Cryptoasset activities include: (a) buying, selling or exercising any right in Accepted Crypto Assets (whether as principal or agent); (b) managing Accepted Crypto Assets belonging to another person; (c) making arrangements with a view to buying, selling or providing custody of Accepted Crypto Assets to another person (whether as principal or agent); (d) marketing of Accepted Crypto Assets; (e) advising on the merits of buying or selling Accepted Crypto Assets or any rights conferred by such buying or selling; and (f) operating (i) a Crypto Asset Exchange, or (ii) as a Crypto Asset Custodian.

In the case of the rest of the UAE, there are no express regulations prohibiting or regulating the sale of cryptocurrencies except the E-payment Regulations.

Taxation

Value Added Tax ("VAT") is a newly introduced tax system in UAE, which only came into effect on January 1, 2018; therefore virtual currencies have not yet fallen under the VAT system. The applicability of tax on cryptocurrencies is subject to the UAE's Federal Law No. 8 of 2017 and is determined by the Federal Tax Authority ("FTA") of UAE. The FTA is the authorised authority to frame regulations regarding the taxation of cryptocurrency. If the virtual currencies are deemed to be "goods" or "services" for the purpose of VAT law, then the value of the purchase is taxable under VAT. Currently, personal income tax or other taxes are not in force in the UAE, so no other taxes are applicable for cryptocurrencies.

Money transmission laws and anti-money laundering requirements

Transactions on a blockchain can only go through if all the members approve, which limits the chances of fraud and money laundering, as the digital currency cannot be forged or damaged and can be moved across borders with ease. It also facilitates the shopping process across social media and websites.

The Financial Service Regulatory Authority requires OCAB licensees to set adequate regulations, including setting appropriate daily limits, for example on daily cash deposits, and the technology necessary to meet their regulatory obligations such as KYC, transaction identification and reporting and risk management requirements like margin limits.

As per the E-Payment Regulations, both individual limits and maximum daily limits are applicable in the rest of the UAE, but these are not applicable to cryptocurrencies.

Several anti-money laundering laws exist in the UAE, including Federal Law No. 4 of 2002 regarding both money laundering and financial terrorism, subsequently amended by Federal Law No. 9 of 2014 (the "AML Law") and Cabinet Resolution No. 38 of 2014 (the "AML Regs"). The AML Law has a broad definition of 'property', and includes almost all items under this definition, and so it covers cryptocurrencies. There are other anti-money laundering laws applicable to cryptocurrencies, depending on the location of the company.

Promotion and testing

The GCC financial centres have responded with new rules to regulate this fast-growing

investment area, attract more companies operating in the digital currency industry, and encourage innovation in this space.

DMCC

Free zone operator Dubai Multi Commodities Centre ("DMCC") has announced that gold trader Regal RA DMCC is the first company in the Middle East to obtain a licence to trade cryptocurrencies.

The company will offer the storage of Bitcoin, Ethereum and other currencies in a vault at DMCC's Almas Tower headquarters in Jumeirah Lake Towers, DMCC said in a statement reported by Bloomberg.

DIFC

FinTech Hive at the DIFC, the region's first and biggest FinTech accelerator and hub, also announced MoUs with three new FinTech hubs – FinTech Saudi, Milan's FinTech District and FinTech Istanbul. The agreements bring the size of FinTech Hive's network of strategic partnerships to 14 FinTech hubs in various parts of the world.

FinTech was one of the hot topics this year, offering a chance for investors, entrepreneurs and members of the business community to learn more on the potential of these fast-growing markets and the opportunities to thrive in this fast-changing sector.

ADGM

The Abu Dhabi Global Market, the International Financial Centre in Abu Dhabi, has launched its framework to regulate spot cryptoasset activities, including those undertaken by exchanges, custodians and other intermediaries in the ADGM. This follows the successful completion of a public consultation on the introduction of a robust cryptoasset regulatory framework by the ADGM's Financial Services Regulatory Authority on 28 May 2018.

The framework is designed to address the full range of risks associated with cryptoasset activities, including risks relating to money laundering and financial crime, consumer protection, technology governance, custody and exchange operations. This new framework is one of the ADGM's many efforts and ongoing commitment to bolster the economic diversification of Abu Dhabi through innovation and sustainable initiatives.

In February, the ADGM launched a framework to regulate spot cryptoasset activities, a step towards developing a safer marketplace for digital currencies.

The Digital Asset Kiosk Machine in Galleria Mall, on Al Maryah Island next to the ADGM, is an initiative of financial services brokerage firm World Credit Savings, regulated by the Financial Services Regulatory Authority of the ADGM.

Customers can buy digital currencies such as Bitcoin via a vending machine in Abu Dhabi for the first time following the launch of a crypto assets kiosk.

The first officially approved Digital Asset Kiosk Machine started operating in Abu Dhabi Global Market – the emirate's financial free zone – earlier this week, allowing users to insert cash or credit cards in exchange for Bitcoin or other currencies given as a paper receipt for their records.

SCA

The UAE's Securities and Commodities Authority will introduce regulations for initial coin offerings in the country by the end of the first half of 2019, a move aimed at providing companies another avenue to raise capital through crowdfunding.

The SCA, which supervises and monitors the markets, has approved ICOs as securities and will work with the Abu Dhabi Securities Exchange and Dubai Financial Market to develop trading platforms for ICOs next year.

Mining

The mining of virtual currencies is not a regulated practice in the UAE, or in any of the free zones within the UAE. The activity of mining is also not covered in any previous legislation that would be applicable.

Even within the ADGM, the FSRA does not consider the mining of cryptocurrencies to be a regulated activity. The amended FSMA specifically excludes "the development, dissemination or use of software for the purpose of creating or mining a Crypto Asset" from its regulated activities.

ADGM

Abu Dhabi-based cryptoasset exchange, Matrix Exchange, announced on July 12, 2019 that it has received an In-Principle Approval ("IPA") from the Financial Services Regulatory Authority of the ADGM to operate as a cryptoasset exchange and custodian in the ADGM.

The IPA is an important milestone; subject to regulatory approvals by the FSRA, Matrix Exchange aims to be a recognised regulated crypto asset exchange in the Middle East.

With a particular focus on the UAE market, Matrix Exchange is also dedicated to establishing a world-class regulated exchange for international investors.

Reporting requirements

The FSRA is the only authority that monitors blockchain activity and cryptocurrency to prevent money laundering and the financing of terrorism. Further, the only authority issuing licences for certain cryptocurrency activities is the DMCC, which include but are not limited to activities involving real estate, gold, silver, tea, etc. There are reporting requirements for cryptocurrency payments made only for the purpose of VAT as per the tax authority regulations, as if virtual currencies are deemed to be "goods" or "services", the value of a purchase is taxable under VAT. Currently, personal income tax or other taxes are not in force in the UAE, so no other taxes are applicable for cryptocurrencies.

Sources

1. https://www.bloomberg.com/news/articles/2018-02-12/dubai-trader-gets-first-middle-east-license-in-cryptocurrencies.
2. https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf.
3. https://www.thenational.ae/business/technology/quicktake-blockchain-set-to-change-the-public-and-private-sectors-1.799496.
4. https://government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021.
5. https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176671/united-arab-emirates.
6. https://www.vantageasia.com/uae-cryptocurrency-and-legal-framework/.
7. https://www.thenational.ae/business/markets/uae-to-finalise-initial-coin-offering-regulations-in-mid-2019-regulatory-says-1.804770.

8. http://www.mondaq.com/x/821846/fin+tech/Initial+Coin+Offerings+In+The+United+Arab+Emirates.
9. https://www.dubaifuture.gov.ae/our-initiatives/global-blockchain-council/.
10. https://www.smartdubai.ae/initiatives/blockchain.
11. https://www.government.ae/en/about-the-uae/strategies-initiatives-and-awards/local-governments-strategies-and-plans/dubai-blockchain-strategy.
12. https://www.adgm.com/.
13. https://www.webopedia.com/TERM/C/cryptocurrency-mining.html.
14. https://www.difc.ae/newsroom/news/difc-drives-innovation-through-landmark-agreements-global-financial-forum-2019/.
15. https://uae-consult.com/en/blog-en/dubai-issues-licenses-for-cryptocurrency-firms.
16. https://www.dfsa.ae/MediaRelease/News/DFSA-Issues-General-Investor-Statement.
17. https://gulfbusiness.com/dubai-gold-trader-obtains-first-middle-east-cryptocurrency-licence/.
18. https://www.difc.ae/newsroom/news/difc-drives-innovation-through-landmark-agreements-global-financial-forum-2019/.
19. https://gulfnews.com/technology/bitoasis-aims-to-be-fully-licensed-in-adgm-this-year-1.62050634.
20. https://www.adgm.com/media-center/announcement-listing-page/media-releases/adgm-launches-crypto-asset-regulatory-framework.
21. https://www.thenational.ae/business/money/cryptocurrency-kiosk-machine-launches-in-abu-dhabi-global-market-1.855974.
22. https://www.thenational.ae/business/markets/uae-to-finalise-initial-coin-offering-regulations-in-mid-2019-regulatory-says-1.804770.
23. https://news.bitcoin.com/pr-matrix-exchange-receives-approval-from-abu-dhabi-global-market/.
24. https://www.vantageasia.com/cryptocurrency-law-asia/.
25. https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176671/united-arab-emirates.
26. https://www.khaleejtimes.com/business//banking-finance/what-you-need-to-know-about-cryptocurrencies-in-the-uae.
27. https://www.vantageasia.com/uae-cryptocurrency-and-legal-framework/.
28. https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176671/united-arab-emirates.
29. https://www.loc.gov/law/help/cryptocurrency/world-survey.php.
30. https://cryptoslate.com/uae-government-accepts-cryptocurrencies-as-securities-to-legalize-icos-in-2019/.
31. https://www.thenational.ae/business/money/how-the-world-s-governments-are-handling-cryptocurrencies-1.716776.
32. https://www.al-mirsal.com/2017/02/16/the-legal-status-of-bitcoin-in-the-united-arab-emirates/.
33. http://www.mondaq.com/x/677158/fin+tech/The+Impact+Of+Blockchain+And+Cryptocurrencies+In+UAE.

34. https://cointelegraph.com/news/dubai-the-blockchain-oasis-of-the-uae-from-public-to-private-sector.
35. https://thelawreviews.co.uk/edition/the-virtual-currency-regulation-review-edition-1/1176671/united-arab-emirates.
36. https://cointelegraph.com/news/united-arab-emirates-will-introduce-ico-regulation-in-first-half-of-2019-regulator-notes.
37. https://prifinance.com/en/cryptocurrency-license/uae/.

Abdulla Yousef Al Nasser
Tel: +971 505 581 810 / Email: a.alnasser@araalaw.com

Adv. Abdullah is the chairman and founder of Araaa Group Advocates and Legal Consultants, as of 2007. He is a highly proficient and diligent lawyer and has represented some of the most high-profile companies and individuals as clients involving notable cases and complex arbitration matters, criminal and commercial cases with a total value of over $10 billion.

Adv. Abdullah is a fellow member of the UAE Lawyers Association and is a lawyer before the Ministry of Justice, Dubai Courts, Federal Courts i.e. Court of First Instance, Court of Appeal, and Court of Cassation, and the Department of Justice in Abu Dhabi in various degrees and types. He is an expert and a qualified arbitrator registered with Dubai International Arbitration Centre (1998–2005) and is licensed as a Private Notary by Dubai Courts. Additionally, Adv. Abdullah is also a published author on the protection offered for electronic cheques.

Flora Ghali
Tel: +971 502 617 093 / Email: f.ghali@araalaw.com

Flora is a senior legal consultant at Araa Group Advocates and Legal Consultants with 19 years of experience in the UAE and Egypt. She has first-rate drafting skills and is well practised in legal matters relating to civil and commercial disputes, real estate claims, construction claims, labour claims, insurance, compensation claims, litigation, rental disputes, family law drafting contracts, etc., which enables her to provide clients in high-value cases with commercially minded, practical and highly reliable advice. Flora has been licensed by the Department of Dubai Legal Affairs as a legal consultant since 2014 and, prior to joining our team, was a valued Senior Lawyer at Flora Ghali Law Firm in Egypt (2008–2014), a Senior Lawyer at Naheed Lami El-Far Law Firm from (2003–2008), and a lawyer at Fathi Rageb Firm for legal consulting (2001–2003).

Nooshin Rahmannejadi
Tel: +971 567 546 160 / Email: n.rahmannejadi@araalaw.com

Nooshin has practised as a legal consultant in Dubai since 2012, and brings an impressive expertise in complex disputes and advises a broad variety of clients, including major property developers in the real estate market. She has an extensive working knowledge of the UAE and Islamic Sharia Laws and her experience enables her to give practical and valuable legal advice regarding complicated substantive, procedural and jurisdictional matters to all clients. Her main areas of practice are banking, maritime, real estate and property, employment, and trademark litigation. She is licensed by the Department of Dubai Legal Affairs as a legal consultant.

Araa Group Advocates and Legal Consultants

Office no. 535-536(A), Office Tower no. 04, Al Ghurair Center, Deira, Dubai, United Arab Emirates
Tel: +971 422 22 511 / URL: www.araalaw.com

United Kingdom

Stuart Davis, Sam Maxson & Andrew Moyle
Latham & Watkins LLP

Government attitude and definition

Although still actively developing, current UK policy thinking in relation to cryptocurrencies was set out by the UK Cryptoassets Taskforce in its *Final Report*[1] (the "**Taskforce Report**"), published in October 2018.

The Taskforce Report identifies cryptocurrencies as a subset of the broader category 'cryptoasset'. It defines the latter as "a cryptographically secured digital representation of value or contractual rights that uses some type of [distributed ledger technology] and can be transferred, stored or traded electronically".[2] Within this overarching category, the Taskforce Report identifies three sub-categories and offers the following (non-legislative) definitions:

"A. **Exchange tokens** – which are often referred to as 'cryptocurrencies' such as Bitcoin, Litecoin and equivalents. They utilise a [distributed ledger technology] platform and are not issued or backed by a central bank or other central body. They do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or for investment.

B. **Security tokens** – which amount to a 'specified investment' as set out in the Financial Services and Markets Act (2000) (Regulated Activities) Order […]. These may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits. They may also be transferable securities or financial instruments under the EU's Markets in Financial Instruments Directive II […].

C. **Utility tokens** – which can be redeemed for access to a specific product or service that is typically provided using a [distributed ledger technology] platform."[3]

Although UK financial regulators have issued warnings in relation to investment in cryptoassets,[4] they are not subject to a blanket prohibition or ban in the UK. However, as indicated by the definitions set out in the Taskforce Report, some will be subject to financial regulation (see *Cryptocurrency regulation* below).

Despite publication of the Taskforce Report, UK policy towards cryptocurrencies is still developing. In particular, the authorities making up the Taskforce are continuing to conduct further substantive work in relation to cryptocurrencies. For example, the UK Financial Conduct Authority ("**FCA**") recently consulted on[5] and published[6] regulatory guidance in relation to cryptoassets (including cryptocurrencies) (the "**FCA Guidance**"). It has also recently consulted[7] on a proposed ban on the sale, marketing and distribution of derivatives and exchange traded notes referencing cryptoassets (including cryptocurrencies) to all retail consumers. As discussed further in *Money transmission laws and anti-money laundering requirements* below, HM Treasury has consulted[8] on the implementation of the Fifth EU Money Laundering Directive ("**5MLD**") in the UK and is expected to consult separately with a view to determining whether the existing financial regulatory perimeter should be

extended to capture certain kinds of cryptoassets that are not currently caught (such as Bitcoin, Litecoin and Ether).

Cryptoassets (including cryptocurrencies) are not considered money or equivalent to fiat currency in the UK. For the time being, the Bank of England has also ruled out issuing a central bank digital currency.[9]

Cryptocurrency regulation

As noted above, there is no blanket prohibition or ban on cryptocurrencies in the UK. Nor does the UK does have a bespoke financial regulatory regime for cryptocurrencies. Accordingly, whether or not a given cryptocurrency is subject to financial regulation in the UK depends on whether it falls within the general financial regulatory perimeter established under the Financial Services and Markets Act 2000 ("**FSMA**") or, as discussed in *Money transmission laws and anti-money laundering requirements* below, under the payment services and electronic money regime established under the Payment Services Regulations 2017 ("**PSRs**") and the Electronic Money Regulations 2011 ("**EMRs**").

This is reflected in the cryptoasset "taxonomy" set out in the FCA Guidance which broadly follows the definitions set out in the Taskforce Report, but which has been refined by the FCA as follows:

<table>
<tr><th>Taskforce Report taxonomy</th><th>FCA Guidance taxonomy[10]</th></tr>
<tr><td rowspan="2">Security tokens – which amount to a 'specified investment' as set out in the Financial Services and Markets Act (2000) (Regulated Activities) Order […]. These may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits. They may also be transferable securities or financial instruments under the EU's Markets in Financial Instruments Directive II […].</td><td>Security tokens: These are tokens that amount to a 'Specified Investment' under the Regulated Activities Order (RAO), excluding e-money. These may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits. They may also be transferable securities or other financial instrument under the EU's Markets in Financial Instruments Directive II (MiFID II). These tokens are likely to be inside the FCA's regulatory perimeter.</td></tr>
<tr><td>E-money tokens: These are tokens that meet the definition of e-money under the Electronic Money Regulations (EMRs). These tokens fall within regulation.</td></tr>
<tr><td>Exchange tokens – which are often referred to as 'cryptocurrencies' such as Bitcoin, Litecoin and equivalents. They utilise a [distributed ledger technology] platform and are not issued or backed by a central bank or other central body. They do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or for investment.</td><td rowspan="2">Unregulated tokens:
Any tokens that are not security tokens or e-money tokens are unregulated tokens. This category includes utility tokens which can be redeemed for access to a specific product or service that is typically provided using a DLT platform.
The category also includes tokens such as Bitcoin, Litecoin and equivalents, and often referred to as 'cryptocurrencies', 'cryptocoins' or 'payment tokens'. These tokens are usually decentralised and designed to be used primarily as a medium of exchange. We sometimes refer to them as exchange tokens and they do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or for investment.</td></tr>
<tr><td>Utility tokens – which can be redeemed for access to a specific product or service that is typically provided using a [distributed ledger technology] platform.</td></tr>
</table>

In summary, the FCA Guidance taxonomy splits cryptoassets into regulated and unregulated cryptoassets. The Taskforce Report definitions of exchange tokens and utility tokens are retained and these two sub-categories of cryptoassets comprise "unregulated tokens" in the FCA Guidance taxonomy. Cryptoassets that constitute electronic money are split out from the Taskforce Report sub-category of security tokens, instead being labelled as "e-money tokens", and these two sub-categories of cryptoassets (i.e., security tokens other than e-money tokens and e-money tokens) comprise "regulated tokens" in the FCA Guidance taxonomy.

The kinds of instruments that are regulated under FSMA are set out in exhaustive fashion in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 ("**RAO**"). These are known as "specified investments" and include instruments such as shares, bonds, fund interests and derivative contracts. Therefore, in order to determine whether a given cryptocurrency is subject to financial regulation in the UK, it is necessary to analyse whether it matches the definition of any specified investment in the RAO. Those cryptoassets that do are labelled "security tokens" in the FCA Guidance and will typically be subject to UK financial regulation.

As stated by the FCA: "Any tokens that are not security tokens or e-money tokens [as to which see *Money transmission laws and anti-money laundering requirements*] are unregulated tokens."[11] In practice, this analysis proceeds predominantly on the basis of an 'intrinsic' assessment of a given cryptocurrency, focused on the rights or entitlements granted to holders, rather than being based on 'extrinsic' factors, such as the intended or actual use of the relevant cryptocurrency or other contextual factors relating to the cryptoasset (such as whether a platform to which the cryptoasset relates is currently operational or whether the network underlying the cryptoasset is decentralised).[12]

Although characterisation of cryptocurrencies in this way must be undertaken on a case-by-case basis in order to determine definitively whether they are subject to UK financial regulation, the FCA Guidance provides useful indicators of the likely outcome of any such analysis. 'Classic' cryptocurrencies (such as Bitcoin, Litecoin and Ether) which are not centrally issued and give no rights or entitlements to holders are labelled "exchange tokens" in the Taskforce Report and "unregulated tokens" in the FCA Guidance. As explained in the FCA Guidance, exchange tokens "typically do not grant the holder any of the rights associated with specified investments".[13] Accordingly, in the FCA's view:

> "Exchange tokens currently fall outside the regulatory perimeter. This means that the transferring, buying and selling of these tokens, including the commercial operation of cryptoasset exchanges for exchange tokens, are activities not currently regulated by the FCA.
>
> "For example, if you are an exchange, and all you do is facilitate transactions of Bitcoins, Ether, Litecoin or other exchange tokens between participants, you are not carrying on a regulated activity."[14]

It is, therefore, clear that Bitcoin, Litecoin and Ether are not currently subject to financial regulation in the UK. Cryptocurrencies with substantially similar features (i.e., those that are not centrally issued and do not grant any rights or entitlements to holders) are also currently likely to be unregulated in the UK. The fact that they may be used for speculative investment purposes in addition to being used as a means of exchange should not impact this conclusion.

One increasingly popular type of cryptoasset which is typically more difficult to characterise for financial regulatory purposes than classic cryptocurrencies is 'stablecoins'. Broadly, a stablecoin is a cryptoasset which by design seeks to maintain a stable market value through

pegging the value of the stablecoin to an underlying asset (such as gold or USD). Often, stablecoins are primarily intended to be utilised as a means of exchange much like classic cryptocurrencies. Pegging the value of a stablecoin to an underlying asset can be achieved in a variety of ways, and the precise structure adopted by a given stablecoin will determine whether it is classified as a specified investment in the UK. For example, a 'fully-collateralised' stablecoin issued by a central issuer, which is pegged to an underlying reference asset through the issuer holding the relevant underlying reference asset, is likely to constitute a specified investment (or, indeed, electronic money) if holders of the stablecoin have rights or entitlements in relation to the underlying reference asset. It is presently possible, however, to structure a stablecoin such that it is unregulated in the UK.

However, it is important to note that even if a given cryptocurrency is not a specified investment other than electronic money (i.e., not a security token following the FCA Guidance), certain activities in relation to such cryptocurrencies can still be subject to UK financial regulation and cryptoassets that constitute electronic money (i.e., e-money tokens following the FCA Guidance) are subject to regulation.

For example, offering to enter into derivative contracts which reference unregulated cryptocurrencies as their underlying (such as cryptocurrency contracts for differences or Bitcoin futures) way of business is likely to constitute a regulated activity in the UK for which a person would require authorisation from the FCA. Indeed, such derivatives are also the subject of the proposed FCA ban on their sale, marketing and distribution to retail customers. Establishing, operating, marketing or managing a fund which offers exposure to unregulated cryptocurrencies by way of business may also be subject to UK financial regulation. Furthermore, money transmissions laws and anti-money laundering legislation may also apply to activities carried out in relation to unregulated cryptocurrencies (see *Money transmission laws and anti-money laundering requirements* below).

Sales regulation

The principal sales regulation that is potentially applicable to sales of cryptocurrencies in the UK falls into three broad categories: i) UK prospectus requirements; ii) the UK restriction on financial promotions; and iii) consumer protection and online/distance selling legislation.

UK prospectus requirements

FSMA, in conjunction with the EU Prospectus Regulation, imposes requirements for an approved prospectus to have been made available to the public before: a) transferable securities are offered to the public in the UK; or b) a request is made for transferable securities to be admitted to a regulated market situated or operating in the UK.[15] Unless an exemption applies (public offers made to qualified investors are, for example, exempt), a detailed prospectus containing prescribed content must be drawn up, approved by the FCA (or the appropriate EEA member state financial regulator where the UK is not the home state of the issuer of the transferable securities) and published before the relevant offer or request is made.

However, these requirements only apply to offers or requests relating to transferable securities. Transferable securities for these purposes are anything which falls within the definition of transferable securities in the second EU Markets in Financial Instruments Directive ("**MiFID II**") which captures, for example, shares, bonds, and depository receipts (and instruments which give their holders similar rights or entitlements).

Therefore, in order to determine whether these requirements apply to the sale of a given cryptocurrency in the UK, it is necessary to determine whether the cryptocurrency in question

is a transferable security. Referring back to the FCA Guidance, only cryptocurrencies that are security tokens (i.e., only those cryptocurrencies that amount to a specified investment under the RAO other than electronic money) may be transferable securities.[16] As noted above, classic cryptocurrencies (such as Bitcoin, Litecoin and Ether) and cryptocurrencies with substantially similar features to classic cryptocurrencies are likely to be regarded as unregulated exchange tokens, rather than security tokens. Accordingly, the UK prospectus requirements should not apply to the sales of such cryptocurrencies.

UK restriction on financial promotions

FSMA contains a restriction on financial promotions which applies independently of the UK prospectus requirements. In summary, the restriction is that a person who is not appropriately authorised must not, in the course of business, communicate an invitation or inducement to engage in investment activity in a way which is capable of having an effect in the UK unless the communication is approved by an appropriately authorised person or an exemption applies.

For these purposes, the concept of engaging in investment activity is further defined by reference to "controlled activities" and "controlled investments", which are set out in exhaustive fashion in the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 ("**FPO**"). Therefore, in order to determine whether the restriction on financial promotions applies to the sale of a given cryptocurrency, it is necessary to determine whether it involves the performance of a controlled activity or a controlled investment by reference to the definitions of each which are set out in the FPO.

Typically, sales of classic cryptocurrencies (such as Bitcoin, Litecoin and Ether) and cryptocurrencies with substantially similar features to classic cryptocurrencies should not engage the UK restriction on financial promotions although analysis of the sale in question must be undertaken on a case-by-case basis in order to determine definitively that this is the case (and related offerings such as funds providing exposure to unregulated cryptocurrencies may well trigger the restriction). Furthermore, even if a particular sale of cryptocurrencies were *prima facie* to engage the restriction a number of potentially helpful exemptions exist, of which the most likely to be relevant are those relating to financial promotions which are made to investment professionals, sophisticated investors and high-net-worth individuals/companies.

General advertising, online/distance selling and consumer protection legislation

In addition to sales regulation that arises out of the UK financial regulatory framework, there is a raft of general advertising, online/distance selling and consumer protection legislation that is potentially applicable to sales of cryptocurrencies or the offering of services related to cryptocurrencies (such as exchange or wallet services) in or from the UK.

Some, like the Consumer Rights Act 2015 or the Consumer Protection from Unfair Trading Regulations 2008, only apply in relation to consumers (typically defined as individuals acting outside of their trade, business, craft or profession) but where they do, provide consumers with significant statutory rights and remedies against supplies of goods, services and digital content and impose restrictions on the kinds of contractual terms that can be enforced against consumers. Others, like the Electronic Commerce (EC Directive) Regulations 2002, are of more general application and impose requirements on businesses established in the UK that offer or provide goods or services digitally. The application of such legislation may also depend on whether or not the business being conducted is subject to UK financial regulation.

Taxation

Currently, there are no bespoke UK tax rules applicable to cryptocurrencies. Therefore, existing tax principles and rules apply generally although uncertainty remains as to their application, particularly in relation to business and corporate tax.

Although there is no definitive policy towards the taxation of cryptoassets (including cryptocurrency) in the UK, the UK tax authority HM Revenue and Customs ("**HMRC**") published in December 2018 a policy paper entitled *Cryptoassets for individuals*,[17] which set out its views about how individuals who hold exchange tokens (as defined in the Taskforce Report) are to be taxed. Notably, the policy paper states that "HMRC will publish further information about the tax treatment of cryptoasset transactions involving businesses and companies"; however, this is yet to be forthcoming at the time of writing. Furthermore, the policy paper makes clear that the views contained within it are relevant only to the taxation of exchange tokens (which includes classic cryptocurrencies such as Bitcoin), and that for security tokens and utility tokens different tax treatments may need to be adopted. However, beyond this, classification of cryptoassets is not determinative of their tax treatment which will depend on the nature and use of the cryptoasset in question.

Having said that, the policy paper includes the following helpful general points:

- Capital Gains Tax ("**CGT**") and Income Tax ("**IT**") may apply to dealings in cryptocurrencies depending on the circumstances. HMRC has clarified that it does not regard cryptocurrencies as currency or money, and that it does not consider buying and selling cryptocurrencies to be the same as gambling (which largely rules out arguments that cryptocurrencies could be exempt from taxation).
- In most cases, HMRC expects that buying and selling of cryptocurrencies by an individual will amount to personal investment activity meaning that individuals will typically have to pay CGT on any gains they realise upon disposal of the cryptocurrencies (which includes not only selling them for fiat currency but also using them to pay for goods and services, giving them away to another person and exchanging them for another kind of cryptoasset).
- However, if (exceptionally, in HMRC's view) an individual is engaged in a trade of dealing in cryptocurrencies (to be determined in accordance with the existing approach taken towards determining whether an individual is engaged in trading securities and other financial instruments for tax purposes), IT would take priority over CGT, being applied to the individual's trading profits.
- Individuals will be liable to pay IT and National Insurance contributions on cryptocurrencies which they receive as a form of payment from their employer, as a result of mining activity or "airdrops" (unless the cryptocurrencies received via the airdrop are not in return for, or in expectation of, a service or as part of a relevant trade). In these circumstances, the cryptocurrencies will be taxable as miscellaneous income unless their receipt is considered part of a trade (in which case they will be taxable as part of the individual's trading profits).
- A charge to CGT may also arise if an individual subsequently disposes (other than in the course of a relevant trade) of cryptocurrencies received from their employer, as a result of mining activity or airdrops regardless of whether or not IT was payable on their receipt.

Money transmission laws and anti-money laundering requirements

Money transmission laws

The principal UK laws relevant to money transmission are the PSRs and the EMRs. Together the PSRs and EMRs establish a regulatory framework applicable to persons performing payment services (including, for example, money remittance and issuing electronic money) in the UK which includes authorisation, organisational, regulatory capital, safeguarding and conduct of business requirements. Whether this framework applies depends on whether a service involves payment services or electronic money as defined by the PSRs and EMRs, respectively.

Payment services as defined by the PSRs necessarily involve funds. Cryptocurrencies are not considered funds for these purposes. Therefore, products and services involving only cryptocurrency (such as a crypto-to-crypto exchange) will not normally involve payment services. Important exceptions to this are products or services relating to what the FCA Guidance terms "e-money tokens". Take, for example, a stablecoin structured in a way that means it constitutes electronic money – issuing or providing wallet services in relation to such a stablecoin would be likely to trigger the application of both the PSRs and EMRs.

Conversely, where fiat currency is involved (for example, in the context of a fiat-to-crypto exchange) there will be funds and so further analysis would need to be conducted to determine whether payment services are being provided and, if so, the precise application of the regulatory regime established by the PSRs and EMRs.

Anti-money laundering requirements

UK anti-money laundering ("**AML**") requirements are principally contained in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("**MLRs**").

The MLRs implement the Fourth EU Money Laundering Directive in the UK and impose various requirements on businesses that are within their scope, including: the requirement to perform a firm-level AML risk assessment, organisational requirements relating to AML (including systems and controls and record-keeping requirements), customer due diligence obligations when establishing a business relationship with a customer or when transacting above a certain threshold, and ongoing monitoring obligations. The MLRs only apply to those businesses that have been identified as the most vulnerable to the risk of being used for money laundering or terrorist financing. Accordingly, they apply to the following "relevant persons":

- credit institutions;
- financial institutions;
- auditors, insolvency practitioners, external accountants and tax advisers;
- independent legal professionals;
- trust or company service providers;
- estate agents;
- casinos; and
- high-value dealers.

Generally speaking, this means that providers of products and services related to unregulated cryptocurrencies (i.e., classic cryptocurrencies and cryptocurrencies with substantially similar features to classic cryptocurrencies) are not presently subject to the MLRs provided

that their activities in relation to such cryptocurrencies do not require them to be authorised and they are not otherwise a relevant person (for example, an estate agent acting in relation to a house purchase involving Bitcoin).

However, this is subject to change with the impending implementation of 5MLD in the UK. 5MLD must be implemented in the UK by 10 January 2020 and, as noted in *Government attitude and definition* above, HM Treasury is currently consulting on this.

At a minimum, the scope of the UK AML regime will be extended to capture fiat-to-crypto cryptocurrency exchanges and cryptocurrency custodial wallet providers regardless of whether they are otherwise regulated as a consequence of 5MLD. However, it remains to be seen whether the HM Treasury will choose to "gold-plate" 5MLD when implementing it in the UK and apply UK AML requirements to other intermediaries/service providers in relation to cryptocurrencies. For example, in its recent consultation, it invited feedback from stakeholders as to whether entities offering crypto-to-crypto cryptocurrency exchange services or entities responsible for "the publication of open-source software (which includes, but is not limited to, non-custodian wallet software and other types of cryptoasset related software)"[18] should be brought within the scope of the UK AML regime. Those involved in the provision of products and services relating to cryptocurrencies should, therefore, monitor developments in this area closely.

Promotion and testing

In November 2018, the FCA established a formal Innovation Division which encompasses the regulator's various initiatives relating to innovation in financial services that it has developed over the last five years. Notably in relation to promotion and testing, beneath this umbrella, sit:

- The FCA's Regulatory Sandbox, which allows both authorised and unauthorised businesses which meet certain eligibility criteria to test innovative financial services propositions in the market with real consumers. Firms which successfully apply to participate in the Sandbox may benefit from the various Sandbox 'tools' which the FCA can deploy to facilitate real world testing such as restricted authorisation, individual guidance, informal steers, waivers and no-enforcement action letters.
- The Global Financial Innovation Network, which grew out of the FCA's proposal to create a global sandbox, seeks to provide a more efficient way for innovative firms to interact with regulators, helping them navigate between countries as they look to scale new ideas. This is for firms wishing to test innovative products, services or business models across more than one jurisdiction.
- The FCA's Innovation Hub, which offers direct support from the FCA to eligible innovative businesses by providing a dedicated contact for innovator businesses that are considering applying for authorisation or a variation of permission, need support when doing so, or do not need to be authorised but could benefit from FCA support.

Ownership and licensing requirements

The nature and form of property rights that may exist in relation to cryptocurrencies under English law is currently untested. In the interests of improving legal certainty in this regard, the UK Jurisdiction Taskforce of the UK government's LawTech Delivery Panel ("**UKJT**") recently consulted on what it perceives to be the principal issues of legal uncertainty about the status of cryptoassets (including cryptocurrencies) and smart contracts under English

private law. These include questions focused on: whether and how cryptoassets can be characterised as personal property; whether cryptoassets are amenable to concepts such as possession and bailment; whether and how security interests may be granted over cryptoassets; and how cryptoassets should be treated for the purposes of UK insolvency law. A legal statement summarising the current status of cryptoassets (including cryptocurrencies) under English private law is expected to be published by the UKJT shortly.

As to licensing requirements, whether or not a person requires authorisation to perform their activities in relation to cryptocurrencies in the UK will depend on whether they are conducting "regulated activities" as defined by FSMA. As noted in *Cryptocurrency regulation* above, a person's activities in relation to cryptocurrencies may still be subject to UK financial regulation even where the underlying cryptocurrency involved is not a specified investment. A classic example of where this might be the case is that of establishing, operating, marketing or managing a fund which offers exposure to unregulated cryptocurrencies by way of business – this kind of activity may well trigger licensing requirements in the UK. For the time being, cryptocurrencies are also unlikely to be permissible for inclusion in fund products (for example, exchange-traded funds) that require approval from the FCA: it is made clear in the Taskforce Report that the FCA will not authorise or approve the listing of a transferable security or a fund that references exchange tokens unless it has confidence in the integrity of the underlying market and that other regulatory criteria for funds authorisation are met.

Mining

Mining cryptocurrencies is permitted in the UK and, as noted above, there is no bespoke financial regulatory regime for cryptocurrencies in the UK which expressly regulates this activity. Mining of cryptocurrencies is also unlikely to fall within the existing UK financial regulatory perimeter (for example, mining Bitcoin is not currently subject to UK financial regulation).

Border restrictions and declaration

There are currently no border restrictions or requirements to declare cryptocurrency holdings when entering the UK. Individuals carrying cash in excess of EUR 10,000 must declare this to HMRC on entering the UK from a country outside the EU, but cryptocurrencies are not regarded as cash for these purposes.

Reporting requirements

No bespoke reporting requirements apply to cryptocurrencies in the UK. Reporting requirements that arise as a result of exiting financial regulation or AML legislation could, however, apply in relation to transactions in cryptocurrencies.

* * *

Endnotes

1. *Cryptoassets Taskforce: Final Report* (26 October 2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf <accessed 1 August 2019>.
2. *Final Report* (n 1), 2.10.

3. *Ibid.*, 2.11.
4. For example, at the time of writing, both the Financial Conduct Authority and Bank of England websites warn that anyone investing in cryptoassets (including cryptocurrencies) should be prepared to lose all of the money invested https://www.fca.org.uk/consumers/cryptoassets, https://www.bankofengland.co.uk/research/digital-currencies <accessed 1 August 2019>.
5. FCA, *CP19/3: Guidance on Cryptoassets* (23 January 2019) https://www.fca.org.uk/publication/consultation/cp19-03.pdf <accessed 1 August 2019>.
6. FCA, *PS19/22: Guidance on Cryptoassets* (31 July 2019) https://www.fca.org.uk/publication/policy/ps19-22.pdf <accessed 1 August 2019>.
7. FCA, *CP19/22: Prohibiting the sale to retail clients of investment products that reference cryptoassets* (3 July 2019) https://www.fca.org.uk/publication/consultation/cp19-22.pdf <accessed 1 August 2019>.
8. HM Treasury, *Transposition of the Fifth Money Laundering Directive: consultation* (15 April 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD__web.pdf <accessed 1 August 2019>.
9. "We are not planning to create a central bank-issued digital currency." Bank of England website https://www.bankofengland.co.uk/research/digital-currencies <accessed 1 August 2019>.
10. As set out here: https://www.fca.org.uk/firms/cryptoassets <accessed 1 August 2019>.
11. https://www.fca.org.uk/firms/cryptoassets <accessed 1 August 2019>.
12. This is consistent with the approach taken in the FCA Guidance. See, for example, paragraphs 42, 45, 49 and 65 to 67 of the FCA Guidance: *PS19/22* (n 6), Appendix 1.
13. *PS19/22* (n 6), Appendix 1 41.
14. *Ibid.*, 43 to 44.
15. The FCA maintains a list of UK regulated markets: https://register.fca.org.uk/shpo_searchresultspage?preDefined=RM&TOKEN=3wq1nht7eg7tr <accessed 1 August 2019>.
16. Electronic money does not fall within the definition of transferable securities.
17. HMRC, *Cryptoassets for individuals* (19 December 2019) https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals <accessed 1 August 2019>.
18. *Transposition of the Fifth Money Laundering Directive: consultation* (n 8), 2.38.

Stuart Davis
Tel: +44 20 7710 1821 / Email: stuart.davis@lw.com

Stuart Davis is an associate in the Financial Institutions Industry Group in the firm's London Office. Mr. Davis has a wide range of experience advising broker-dealers, investment, retail and private banks, technology companies, market infrastructure providers, investment managers, hedge funds and private equity funds on complex regulatory challenges. Mr. Davis has considerable experience advising clients on the domestic and cross-border regulatory aspects of cutting edge FinTech initiatives, including technology innovations in market infrastructure, trading, clearing and settlement, lending (including crowd-funding), payments and regulatory surveillance. Recently, Mr. Davis has advised a number of financial institutions on the impact of MAR and MiFID II on their businesses, and has been heavily involved with assisting institutions on their FX remediation projects, market conduct issues, best execution compliance, CASS compliance, systems and controls, governance, regulatory reform and the implications of Brexit for financial institutions.

Sam Maxson
Tel: +44 20 7710 1823 / Email: sam.maxson@lw.com

Sam Maxson is an associate in the London office of Latham & Watkins.
Mr. Maxson regularly advises a wide range of clients (including banks, insurers, investment firms, financial markets infrastructure providers, and technology companies) on all aspects of financial regulation. Mr. Maxson has a particular focus on FinTech and InsurTech, advising both established and emerging businesses on the application of global financial regulation to new and novel uses of technology in finance and insurance. His expertise also extends to the increasingly widespread interest in cryptoassets and "tokenisation" of financial markets.

Andrew Moyle
Tel: +44 20 7710 1078 / Email: andrew.moyle@lw.com

Andrew Moyle is the Global Co-Chair of Latham & Watkins' FinTech Industry Group and a partner in the London office. He has more than 20 years of experience in providing commercial legal advice on the structuring, negotiation, implementation, and management of complex technology and outsourcing transactions. Mr. Moyle advises clients ranging from traditional financial institutions to new technology incumbents on the "tech" in FinTech, including on payments and transfers, InsurTech, and virtual currencies. In his broader technology practice, Mr. Moyle advises clients on commercial contracts and collaborations, cloud computing, outsourcing, digital and disruptive technology, telecommunications technology, and enterprise systems. He regularly engages as the lead legal advisor on outsourcing programs, strategic sourcing functions, and transformation initiatives. In addition to financial services, he also advises clients in leisure, energy, retail, and the natural resource sectors.

Latham & Watkins LLP

99 Bishopsgate, London EC2M 3XF, United Kingdom
Tel: +44 20 7710 1000 / Fax: +44 20 7374 4460 / URL: www.lw.com

USA

Josias N. Dewey
Holland & Knight

Government attitude and definition

In the United States, cryptocurrencies have been the focus of much attention by both Federal and state governments. Much of the Federal government's focus has been at the administrative and agency level, including the Securities and Exchange Commission (the "**SEC**"), the Commodities and Futures Trading Commission (the "**CFTC**"), the Federal Trade Commission (the "**FTC**") and the Department of the Treasury, through both the Internal Revenue Service (the "**IRS**") and the Financial Crimes Enforcement Network ("**FinCEN**"). While there has been significant engagement by these agencies, little formal rulemaking has occurred. Generally speaking, Federal agencies and policymakers have praised the technology as being an important part of the U.S.'s future infrastructure and the need for the U.S. to maintain a leading role in its development. While there are still some skeptical of the technology's promise, many policymakers have publicly acknowledged the risk of over-regulating. Others have cautioned lawmakers from passing legislation that would drive investment in the technology overseas.

Several state governments have proposed and/or passed laws affecting cryptocurrencies and blockchain technology, with most of the activity taking place in the legislative branch. There have generally been two approaches to regulation at the state level. Some states have tried to promote the technology by passing very favorable regulations exempting cryptocurrencies from state securities laws, money transmission statutes and other state regulatory requirements. These states hope to leverage investment in the technology to stimulate local economies and improve public services. One example, Wyoming, has been mentioned as a state seeking a broader impact on its economy. Wyoming's legislature passed a bill exempting cryptocurrencies from property taxation. The state has been praised for becoming the most crypto-friendly jurisdiction in the country. Another state, Colorado, passed a bipartisan bill promoting the use of blockchain for government record-keeping. Other states have taken steps to legalize Bitcoin as a payment option for taxation purposes. Along with Georgia, Arizona had pledged to become the first U.S. state to start accepting taxes in cryptocurrency; but in November 2018, Ohio became the first state to allow state taxes to be remitted in the form of Bitcoin.

On the other hand, authorities in at least 10 other states, like California and New Mexico, have issued warnings about investing in cryptocurrencies. Others, like New York, have passed laws generally considered restrictive, and as a result, have seen a number of cryptocurrency-based companies exit the New York market. On the other hand, a number of large virtual currency exchanges, such as Gemini, obtained New York state trust company charters. The strict regulatory oversight is seen as a positive by many customers, especially institutional investors who desire to mitigate custodial risk.

There is no uniform definition of "cryptocurrency," which is often referred to as "virtual currency," "digital assets," "digital tokens," "cryptoassets" or simply "crypto." While some jurisdictions have attempted to formulate a detailed definition for the asset class, most have wisely opted for broader, more technology-agnostic definitions. Those taking the latter approach will be better positioned to regulate as and when the technology evolves.

Sales regulation

The sale of cryptocurrency is generally only regulated if the sale (i) constitutes the sale of a security under state or Federal law, or (ii) is considered to have constituted money transmission under state law, or pursuant to FinCEN's regulations, the sale was done as part of a money services business ("**MSB**") under Federal law. In addition, futures, options, swaps and other derivative contracts that make reference to the price of a cryptoasset that constitutes a commodity are subject to regulation by the CFTC under the Commodity Exchange Act. In addition, the CFTC has jurisdiction over attempts to engage in market manipulation with respect to those cryptoassets that are considered commodities. The likelihood of the CFTC asserting its authority to prevent market manipulation is much higher today as a result of both the CBEO and the CME offering futures linked to the price of Bitcoin.

Securities laws

At the Federal level, the SEC generally has regulatory authority over the issuance or resale of any token or other digital asset that constitutes a security. Under U.S. law, a security includes "an investment contract," which has been defined by the U.S. Supreme Court as an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).

In determining whether a token or other digital asset is an "investment contract," both the SEC and the courts look at the substance of the transaction, instead of its form. In 1943, the U.S. Supreme Court determined that "the reach of the [Securities] Act does not stop with the obvious and commonplace. Novel, uncommon, or irregular devices, whatever they appear to be, are also reached if it be proved as matter of fact that they were widely offered or dealt in under terms or courses of dealing which established their character in commerce as 'investment contracts,' or as 'any interest or instrument commonly known as a 'security'." *SEC v. C.M. Joiner Leasing Corp.*, 320 U.S. 344, 351 (1943). It has also been said that "Congress' purpose in enacting the securities laws was to regulate investments, in whatever form they are made and by whatever name they are called." *Reves v. Ernst & Young*, 494 U.S. 56, 61 (1990).

The SEC has been clear on its position that even if a token issued in an initial coin offering ("**ICO**") has "utility," the token will still be deemed to be a security that is regulated under the Securities Act if it meets elements of *Howey* test. On February 6, 2018, in written testimony to the U.S. Senate Banking Committee, the Chairman of the SEC stated as follows:

> Certain market professionals have attempted to highlight the utility or voucher-like characteristics of their proposed ICOs in an effort to claim that their proposed tokens or coins are not securities. Many of these assertions that the federal securities laws do not apply to a particular ICO appear to elevate form over substance. The rise of these form-based arguments is a disturbing trend that deprives investors of mandatory protections that clearly are required as a result of the structure of the transaction.

> Merely calling a token a 'utility' token or structuring it to provide some utility does not prevent the token from being a security.

In a more nuanced speech delivered in June 2018, William Hinman, the SEC's Director of Corporate Finance, stated:

> Returning to the ICOs I am seeing, strictly speaking, the token – or coin or whatever the digital information packet is called – all by itself is not a security, just as the orange groves in *Howey* were not. Central to determining whether a security is being sold is how it is being sold and the reasonable expectations of purchasers. When someone buys a housing unit to live in, it is probably not a security. But under certain circumstances, the same asset can be offered and sold in a way that causes investors to have a reasonable expectation of profits based on the efforts of others. For example, if the housing unit is offered with a management contract or other services, it can be a security.

Later in the same speech, Mr. Hinman made clear that a digital token that might initially be sold in a transaction constituting the sale of a security, might thereafter be sold as a non-security where the facts and circumstances have changed over time, such that the Howey test is no longer met. In April 2019, Hinman's comments were reinforced when the SEC published a written framework for determining when a digital token would be considered a security. Noting that the determination often came down to whether there was an expectation of profit based on the efforts of others, the SEC noted, "[w]hen a promoter, sponsor, or other third party (or affiliated group of third parties) … provides essential managerial efforts that affect the success of the enterprise, and investors reasonably expect to derive profit from those efforts, then this prong of the test is met." At the same time, the SEC issued its first "no action" letter involving digital tokens. Issued to TurnKey Jet, Inc., the SEC stating that it would not pursue enforcement against the sale of TurnKey's digital tokens under the following circumstances:

TKJ will not use any funds from Token sales to develop the TKJ Platform, Network, or App, and each of these will be fully developed and operational at the time any Tokens are sold:

- the Tokens will be immediately usable for their intended functionality (purchasing air charter services) at the time they are sold;
- TKJ will restrict transfers of Tokens to TKJ Wallets only, and not to wallets external to the Platform;
- TKJ will sell Tokens at a price of one USD per Token throughout the life of the Program, and each Token will represent a TKJ obligation to supply air charter services at a value of one USD per Token;
- if TKJ offers to repurchase Tokens, it will only do so at a discount to the face value of the Tokens (one USD per Token) that the holder seeks to resell to TKJ, unless a court within the United States orders TKJ to liquidate the Tokens; and
- the Token is marketed in a manner that emphasizes the functionality of the Token, and not the potential for the increase in the market value of the Token.

While consistent with the SEC's prior guidance, the TurnKey no-action letter is of limited value to many considering a token sale given the extremely narrow scope of facts set forth on the letter.

If a digital asset is determined to be a security, then the issuer must register the security with the SEC or offer it pursuant to an exemption from the registration requirements. For offerings that are being made under a federal exemption from securities registration, the SEC places fewer restrictions on the sale of securities to "accredited investors." An

individual investor is an "accredited investor" only if he or she (i) is a director or executive officer of the company issuing the securities, (ii) has an individual net worth (or joint net worth with a spouse) that exceeds $1 million, excluding the value of the investor's primary residence, (iii) has an individual income that exceeds $200,000 in each of the two most recent years, and has a reasonable expectation of reaching the same individual income level in the current year, or (iv) has a joint income that exceeds $300,000 in each of the two most recent years, and has a reasonable expectation of reaching the same joint income level in the current year. See SEC Rule 501(a)(5).

In addition to Federal securities laws, most states have their own laws, referred to as blue sky laws, which are not always preempted by Federal law. Anyone selling digital assets likely to constitute a security should check with counsel about the applicability of state blue sky laws. Of particular importance, there are certain exemptions from registration under Federal law that do not preempt the application of state blue sky laws.

The determination that a token constitutes a security raises several other concerns, including (i) the requirement that a person be a broker-dealer licensed with the SEC and a member of FINRA in order to facilitate the sale of securities or to act as a market maker or otherwise constitute a dealer in the asset, and (ii) the asset can only trade on a licensed securities exchange or alternative trading system ("**ATS**") approved by the SEC. In January 2019, tZERO launched the first SEC-registered ATS dedicated to trading security tokens. In addition, several others are seeking approval to operate ATS platforms for crypto.

Money transmission laws and anti-money laundering requirements

Under the Bank Secrecy Act (the "**BSA**"), FinCEN regulates MSBs. On March 18, 2013, FinCEN issued guidance that stated the following would be considered MSBs: (i) a virtual currency exchange; and (ii) an administrator of a centralized repository of virtual currency who has the authority to both issue and redeem the virtual currency. FinCEN issued guidance that stated as follows: "An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person." See FIN-2013-G001, Application of FinCEN's Regulations to Person's Administering, Exchanging or Using Virtual Currencies (March 18, 2013).

An MSB that is a money transmitter must conduct a comprehensive risk assessment of its exposure to money laundering and implement an anti-money laundering ("**AML**") program based on such risk assessment. FinCEN regulations require MSBs to develop, implement, and maintain a written program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. The AML program must: (i) incorporate written policies, procedures and internal controls reasonably designed to assure ongoing compliance; (ii) designate an individual compliance officer responsible for assuring day-to-day compliance with the program and Bank Secrecy Act requirements; (iii) provide training for appropriate personnel, which specifically includes training in the detection of suspicious transactions; and (iv) provide for independent review to monitor and maintain an adequate program.

All U.S. persons are prohibited from doing business with foreign nationals who are on the Specially Designated Nationals and Blocked Entities List ("**SDN List**") of the U.S. Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"). OFAC provides an updated and searchable version of its SDN List at: sanctionssearch.ofac.treas.gov. OFAC

requires all U.S. citizens to "block" (i.e., freeze) the assets of individuals and companies who are engaging in transactions with (i) countries that are subject to U.S. economic sanctions ("blocked countries"), (ii) certain companies and entities that act as agents for such countries ("blocked parties"), and (iii) certain individuals that act as agents for such countries ("specially designated individuals" or "**SDNs**"). It is important to have a compliance program in place to avoid (or mitigate) receiving civil and criminal penalties from OFAC for non-compliance. See 31 C.F.R. Part 501 (OFAC Reporting Regulations); OFAC Economic Sanctions Enforcement Guidelines (Nov. 9, 2009).

On February 13, 2018, in response to a letter from Senator Ron Wyden, an official within the Treasury Department issued a correspondence that called into question whether an ICO issuer was *de facto* an MSB, which was required to register with FinCEN. While there were several flaws in the logic set forth in the letter, it remained an area of concern for anyone considering a token sale. On May 9, 2019, FinCEN published, "*Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*." The May report did not provide any new guidance. Instead, the report sought to consolidate past guidance in a comprehensive and more consistent manner.

State laws on money transmission vary widely but can generally be grouped into a few categories. Most states define money transmission as including some or all of three types of activities: (1) money transmission; (2) issuing and/or selling payment instruments; and (3) issuing and/or selling stored value. A few states only regulate these activities when "money" is involved, and define money as "a medium of exchange that is authorized or adopted by a domestic or foreign government." Generally, state money transmission laws apply to any entity that is either located in the state or is located outside of the state (including in a foreign jurisdiction) but does business with residents of the state.

Taxation

In March 2014, the IRS declared that "virtual currency," such as Bitcoin and other cryptocurrency, will be taxed by the IRS as "property" and not currency. See IRS Notice 2014-21, Guidance on Virtual Currency (March 25, 2014). Consequently, every individual or business that owns cryptocurrency will generally need to, among other things, (i) keep detailed records of cryptocurrency purchases and sales, (ii) pay taxes on any gains that may have been made upon the sale of cryptocurrency for cash, (iii) pay taxes on any gains that may have been made upon the purchase of a good or service with cryptocurrency, and (iv) pay taxes on the fair market value of any mined cryptocurrency, as of the date of receipt.

For an individual filing a federal income tax return, the gains or losses from a sale of virtual currency that was held as a "capital asset" (i.e., for investment purposes) are reported on (i) Schedule D of IRS Form 1040, and (ii) IRS Form 8949 (Sales and Other Dispositions of Capital Assets). Any realized gains on virtual currency held for more than one year as a capital asset by an individual are subject to capital gains tax rates. Any realized gains on virtual currency held for one year or less as a capital asset by an individual are subject to ordinary income tax rates. The IRS requires, on Form 8949, for each virtual currency transaction, the following information be disclosed: (i) a description of the amount and type of virtual currency sold; (ii) the date acquired; (iii) the date the virtual currency was sold; (iv) the amount of proceeds from the sale; (v) the cost (or other basis); and (vi) the amount of the gain or loss. It should be noted that the record-keeping requirements of IRS Form 8949 can be particularly onerous for those who have used cryptocurrency to make numerous small purchases of goods or services throughout the year.

For transactions completed on or after January 1, 2018, the Internal Revenue Code now prohibits the use of Section 1031(a) for cryptocurrency transactions and requires a taxpayer to recognize taxable gain or loss at the time that any cryptocurrency is converted into another cryptocurrency. Section 13303 of P.L. 115-97 (the tax act signed into law on December 22, 2017) changes Section 1031(a) to state as follows: "No gain or loss shall be recognized on the exchange of real property held for productive use in a trade or business or for investment if such real property is exchanged solely for real property of like kind which is to be held either for productive use in a trade or business or for investment."

For transactions completed on or prior to December 31, 2017, the IRS has not issued any guidance on whether different cryptocurrencies are "property of like kind" that would qualify for non-recognition of gain under Section 1031(a). Generally speaking, exchanges between different cryptocurrencies are usually done by either (i) a simultaneous swap of one cryptocurrency for another, or (ii) a deferred exchange, in which one cryptocurrency is sold for cash, followed by the purchase for cash, of a different cryptocurrency.

For transactions completed on or prior to December 31, 2017, Section 1031(a)(1) of the Internal Revenue Code states the following: "No gain or loss shall be recognized on the exchange of property held for productive use in a trade or business or for investment if such property is exchanged solely for property of like kind which is to be held either for productive use in a trade or business or for investment." In 26 C.F.R. 1.1031(a)-2(b), "like kind" is defined as follows: "As used in section 1031(a), the words like kind have reference to the nature or character of the property and not to its grade or quality. One kind or class of property may not, under that section, be exchanged for property of a different kind or class." It should be noted that, in order to attempt to utilize the tax treatment of Section 1031(a) for transactions done on or prior to December 31, 2017, (i) each transaction must comply with certain requirements set forth in IRS regulations (such as the use, in certain instances, of a "qualified intermediary"), and (ii) the taxpayer must file a Form 8824 with the IRS.

There is a risk that the IRS could use its prior revenue rulings on gold bullion as a basis for taking the position that, for transactions completed on or prior to December 31, 2017, different cryptocurrencies are not "property of like kind" under Section 1031(a). In Rev. Rul. 82-166 (October 4, 1982), the IRS ruled that an exchange of gold bullion for silver bullion does not qualify for non-recognition of gain under Section 1031(a). The IRS stated: "Although the metals have some similar qualities and uses, silver and gold are intrinsically different metals and primarily are used in different ways. Silver is essentially an industrial commodity. Gold is primarily utilized as an investment in itself. An investment in one of the metals is fundamentally different from an investment in the other metal. Therefore, the silver bullion and the gold bullion are not property of like kind."

The IRS also stated in Rev. Rul. 79-143 (January 5, 1979) that an exchange of $20 U.S. gold numismatic-type coins and South African Krugerrand gold coins does not qualify for non-recognition of gain under Section 1031(a). The IRS stated: "The bullion-type coins, unlike the numismatic-type coins, represent an investment in gold on world markets rather than in the coins themselves. Therefore, the bullion-type coins and the numismatic-type coins are not property of like kind."

Promotion and testing

Arizona has become the first state in the U.S. to adopt a "regulatory sandbox" to shepherd the development of new emerging industries like fintech, blockchain and cryptocurrencies within its borders. The law will grant regulatory relief for innovators in these sectors who

desire to bring new products to market within the state. Under the program, companies will be able to test their products for up to two years and serve as many as 10,000 customers before needing to apply for formal licensure.

Ownership and licensing requirements

Cryptocurrency fund managers that invest in cryptocurrency futures contracts, as opposed to "spot transactions" in cryptocurrencies, are required to register as a CTA and CPO with the CFTC and with the National Futures Association ("**NFA**"), or satisfy an exemption. Also, because of additions to the Dodd-Frank Act, cryptocurrency hedge fund managers that use leverage or margin would also need to register with the CFTC and NFA. The Dodd-Frank Act amended the Commodities Act to add new authority over certain leveraged, margined, or financed retail commodity transactions. The CFTC exercised this jurisdiction in an action against BFXNA INC. d/b/a BITFINEX in 2016. Fund managers should be cautious when using margin/leverage as it may require them to register as a CTA and CPO with the CFTC and register with the NFA.

The Investment Company Act of 1940 (the "**Company Act**"), the Investment Advisers Act of 1940 (the "**Advisers Act**"), as well as state investment advisor laws, impose regulations on investment funds that invest in securities. The Company Act generally requires investment companies to register with the SEC as mutual funds unless they meet an exemption. Cryptocurrency funds, and hedge funds generally, can be structured under one of two exemptions from registration under the Investment Company Act. Section 3(c)(1) allows a fund to have up to 100 investors. Alternatively, Section 3(c)(7) allows a fund to have an unlimited number of investor (but practically it should be limited to 2,000 to avoid being deemed a publicly traded partnership under the Securities Exchange Act) but requires a significantly higher net worth suitability requirement for each investor (roughly $5 million for individuals, $25 million for entities). As a general rule, most startup funds are structured as 3(c)(1) funds because of the lower investor suitability requirements.

Until the SEC provides more guidance on classifying individual cryptocurrencies as securities or commodities, the likelihood of many cryptocurrencies being deemed securities is high. As such, we recommend that cryptocurrency funds that invest in anything other than Bitcoin, ether, Litecoin, and the handful of other clearly commodity coins, comply with the Company Act preemptively. For most startup funds, this would mean limiting investors within a given fund to less than 100 beneficial owners.

Regardless of whether a startup cryptocurrency fund manager is required to register as a CPO/CTA with the CFTC under the Commodities Act, register or seek exemption from the SEC as an investment advisor (under the Adviser's Act), or investment company (under the Company Act), every cryptocurrency fund manager will be subject to the fraud provisions of the CFTC and/or the SEC. In September 2017, the CFTC announced its first anti-fraud enforcement action involving Bitcoin. These anti-fraud actions can be taken by the SEC and CFTC regardless of the cryptocurrency fund's exempt status.

Mining

The general rule of thumb regarding Bitcoin mining remains relatively straightforward. If you are able to own and use cryptocurrency where you live, you should also be able to mine cryptocurrency in that location as well. If owning cryptocurrency is illegal where you live, mining is most likely also illegal. There are few, if any, jurisdictions in the U.S. where

possession of cryptocurrency is illegal. Plattsburgh, New York, however, is likely the only city in the U.S. to have imposed a ban (temporary) on cryptocurrency mining, which was lifted in March 2019.

Border restrictions and declaration

A group of U.S. lawmakers had previously proposed a requirement that individuals declare their cryptocurrency holdings when entering the U.S., but to date no such requirement has gone into effect. It would be difficult to enforce such a requirement given a person is not required to possess any physical item when crossing into the U.S.

Reporting requirements

We are not aware of any broadly applicable reporting requirements specific to cryptocurrency in the U.S.

Estate planning and testamentary succession

Cryptocurrency, such as Bitcoin, has value and therefore is increasingly likely to become an estate asset. While there are few, if any laws, specific to cryptocurrency, due to the nature of cryptocurrencies, typical wills and revocable living trusts may not be well suited to efficiently transfer this new type of asset. Consequently, new estate planning questions and clauses may be needed.

While cryptocurrency is not sufficiently mature to allow existing legal structures to promulgate a complete set of rules and regulations, cryptocurrency's technological character allows estate planning to protect the intent of clients holding cryptocurrency. However, the lack of statutory structure necessitates proactive steps. Accordingly, someone who wants greater certainty of bequeathing cryptocurrency to their heirs will need to provide specific and detailed written instructions in your estate planning documents. The information that you will need to include will depend upon the type of virtual currency wallet that you have.

There are wide range of cryptocurrency wallets that are available at this time. The current types of cryptocurrency wallets include: (i) a single device software wallet in which you hold the private keys (example: bitpay wallet); (ii) a multiple device web wallet in which you hold the private keys (example: blockchain wallet); (iii) a multiple device web wallet in which you do not hold the private keys (example: coinbase wallet); (iv) a USB hardware dongle wallet in which you hold the private keys (example: trezor wallet); and (v) a "paper wallet" in which the private keys and public keys are written down (which can be later loaded into a software wallet of your choice to be spent).

The instructions that you provide in a will (for your personal representative) or in a declaration of trust (for the successor trustee of a revocable living trust) should be written in a manner that is easy to understand for individuals who are not familiar with cryptocurrency. For example, in the case of a single device software wallet in which you hold the private keys, instructions could include (i) a description of the name and version of the wallet software, (ii) a description of the name and version of the operating software system of the wallet device (i.e., iOS, Android, MacOS, Windows or Linux), (iii) a description of the types of virtual currency held by the wallet, (iv) either the long-form private and public keys for the wallet or the 12 word "seed" BIP39 or BIP44 recovery phrase for the wallet, and (v) step-by-step instructions (which may include screenshots) showing how the wallet can be restored onto a new device, if the current wallet device cannot be accessed.

As transfers from a Bitcoin wallet and most other wallets are irrevocable, private key information about your cryptocurrency accounts will need to be kept in a secure manner. Security can be enhanced by storing the private key information in a safe-deposit box or vault, which could only be accessed after your death by the personal representative designated in your will (or the successor trustee designated in your revocable living trust).

Josias N. Dewey
Tel: +1 305 374 8500 / Email: joe.dewey@hklaw.com

Joe Dewey is a financial services and real estate partner in Holland & Knight's Miami office and is considered a thought leader on blockchain technology. Mr Dewey regularly represents banks and other financial institutions across the entire spectrum as measured by assets and scale, from community to global money center banks. Mr Dewey spends a considerable amount of time at the convergence of human prose legal contracts, as well as computational contracts, based primarily on computer code. This includes smart contracts that can be implemented on Hyperledger Fabric (or IBM's Blockchain service), Ethereum (both public and permissioned versions) and R3's Corda platform. Mr Dewey spends a considerable amount of his practice in this space assisting clients in identifying optimal distributed ledger use cases and developing proof of concept applications. He can assist in the transition from proof of concepts (PoCs) to production systems built by our clients' primary technology solutions providers.

Holland & Knight

701 Brickell Avenue, Suite 3300, Miami, FL 33131, USA
Tel: +1 305 374 8500 / Fax: +1 305 789 7799 / URL: www.hklaw.com

Venezuela

Luisa Lepervanche
Mendoza, Palacios, Acedo, Borjas, Páez Pumar & Cía. (Menpa)

Government attitude and definition

The Venezuelan government has had an ambivalent attitude towards cryptocurrency.

On the one hand, it has taken on obligations to promote the use of cryptocurrency, both in the public and private spheres; it has created its own cryptocurrency, called the Petro; it has taken additional steps to promote cryptocurrencies (such as the creation of special zones for paying with Petro and other cryptocurrencies, granting special authorisations to ensure that contracts may be paid in Petro, fixing prices, salaries, etc. in Petro, among others). On the other hand, the government has, from time to time, imprisoned cryptocurrency miners and threatened to close cryptocurrency operations that deal with foreign exchange transactions.

As indicated, the government has taken steps to promote cryptocurrency use in Venezuela, to the extent that it created its own cryptocurrency: the Petro. Further, pursuant to certain regulations, the bolivar is supposedly linked to the value of the Petro.[1] Also, the government has used the value of Petro to establish minimum wages, taxes, public prices, etc.

Government promotion of the use of cryptocurrencies, in general, and the Petro in particular

As an introduction, below is a brief background of the rules regulating money in Venezuela.

Article 318 of the Constitution provides that the bolivar is the "monetary unit" of Venezuela. This is ratified by Article 106 of the Law on the Central Bank of Venezuela (*Ley del Banco Central de Venezuela*). Therefore, the legal tender in Venezuela is the bolivar. There are two exceptions to this rule: the possibility of issuing common monetary units issued in the context of integration agreements regarding Latin-America and the Caribbean; and the possibility of issuing communal money (*monedas comunales)* issued by *comunas*, which is a complicated concept that refers to basic social groups. None of these exceptions currently apply to cryptocurrency.

Due to hyperinflation, in 2018, amounts expressed in bolivars were huge. Whether the amounts referred to prices, to salaries, to the value of goods, etc., they had become extremely high amounts – sometimes so high that systems did not recognise them. As a solution, the President ordered a monetary conversion, that is, he created a "new" bolivar (called the Sovereign Bolivar, *Bolivar Soberano*), which was represented by dividing the previous bolivar value by 100,000. This entered into force on August 20, 2018.[2]

Pursuant to the Constitution and the law, only bolivars (now Sovereign Bolivars) represent legal tender. Cryptocurrencies do not represent legal tender. However, Venezuela – particularly the Executive Branch and the Constitutional Assembly[3] – have made important efforts to promote the use of cryptocurrency.

In April 2018 the Constitutional Assembly issued a constitutional decree regulating cryptocurrencies.[4] It mandates, under Article 9, that Venezuela must promote, protect and guarantee the use of cryptocurrencies as a means of payment of obligations, both by the public sector and the private sector, not only in Venezuela but also abroad. Other instruments referred to below also reflect similar obligations. Accordingly, Venezuela is making efforts, at least theoretically, to promote cryptocurrencies. However, these efforts may extend beyond its legal powers and may even be impossible, in fact, to achieve.

First, Venezuela is, in theory, bound to promote, protect and guarantee the use of cryptocurrencies by the public and private sectors. The obligation to promote may prove both possible and legal. Venezuela may create incentives, benefits, discounts, etc. But it cannot guarantee the use of cryptocurrencies because, as indicated, only bolivars are of legal tender in Venezuela, so forcing (by guaranteeing) the use of cryptocurrencies would violate both the Constitution and the law.

Second, Venezuela bound itself not only to promote, protect and guarantee the use of cryptocurrencies in Venezuela, but also abroad. Needless to say, even in practical terms, complying with such obligation is going to prove difficult (if not impossible).

Venezuela's own cryptocurrency – the Petro

In December 2017, by Presidential Decree, the government authorised the issuance of the Petro, a cryptocurrency "backed" (*respaldada*) by Venezuelan oil reserves.[5] In January 2018, it published the first Petro whitepaper,[6] which it then modified in March.[7] In February, the Executive affected the potential development of a portion of the oil reserves in the Orinoco Belt to "back" (*respaldar*) the issuance of Petro.[8] In April, the Constitutional Assembly issued the Constitutional Decree, further regulating the Petro and approving the decision to affect the oil reserves to serve as "backing for the creation and issuance of the Venezuelan cryptocurrency Petro" (*como respaldo para la creación y emisión de la criptomoneda venezolana Petro*).[9] In October, Venezuela published the third version of the Petro whitepaper.[10]

However, even if the Petro is a cryptocurrency, in our opinion, it also qualifies as public debt – even if an atypical one. And, because it qualifies as such, its issuance breaches the Constitution and the law.

Qualification of the Petro

The Petro qualifies as public debt under the Law on the Financial Administration of the Public Sector (*Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Financiera del Sector Público*). Article 80 provides that the issuance of securities and the granting of guarantees, *inter alia,* qualify as public debt transactions. The Petro falls within both categories.

First, Petro qualify as securities under Venezuelan law. This assertion probably requires a paper of its own, but for purposes of this analysis, let us state that they constitute a unilateral promise by the issuer – Venezuela – represented in dematerialised documents issued *en masse*, which grant their holders certain rights (*e.g.* the right to benefit from the eventual exploitation of a portion of oil reserves, the right to pay debts to the Republic at a certain rate determined by oil prices, the right to receive Petro under the Staking savings plan, etc.). Other Venezuelan authors have also categorised Petro as securities.[11]

Second, when issuing Petro, the government affected part of the reserves of the Orinoco Belt to back the cryptocurrency. It did so by means of the Presidential Decree issued in February 2018, confirmed by the Constitutional Decree issued in April 2018. Further, both

the Presidential Decree creating the Petro in December 2017 and the whitepaper published in January 2018 refer to the Petro being backed by oil. Significantly, the whitepaper published in October 2018 refers to the Petro being backed by natural resources. The efficiency of the guarantee has been questioned in economic terms,[12] as well in legal ones – these are addressed below. Yet, its inefficiency or its illegality does not change the fact that a guarantee was granted regarding the Petro. Again, Venezuelan commentators share this point of view.[13]

Accordingly, since Petro qualify as securities under Venezuelan law, and guarantees were granted regarding their issuance, Petro would fall within the scope of the definition of Article 80 of the Law on the Financial Administration of the Public Sector, thus being public debt – a very unusual type, but still public debt. The National Assembly – the Venezuelan equivalent of the U.S. Congress – has taken this position.[14] This was also the initial position of the government of the United States of America, through the Office of Foreign Assets Control, which on its website for Frequently Asked Questions on Venezuela-Related Sanctions indicated the following: "A currency with these characteristics would appear to be an extension of credit to the Venezuelan government…"[15]

Legality of the Petro

The fact that the issuance of Petro is equivalent to the issuance of public debt means that the Petro is both unconstitutional and illegal.

First, pursuant to Article 312 of the Constitution and to Article 98 of the Law on the Financial Administration of the Public Sector, public debt must be approved by law. Laws in Venezuela are issued by the National Assembly, by mandate of Article 202 of the Constitution. The National Assembly did not enact a law approving the issuance of Petro. Further, the National Assembly has denounced its unconstitutionality and illegality on such grounds.[16]

Second, Article 12 of the Constitution and Article 3 of the Organic Law on Hydrocarbons (*Ley Orgánica de Hidrocarburos*) prohibit encumbering oil reserves. Further the Law on the Financial Administration of the Public Sector also prohibits guaranteeing public debt transactions with public assets. Accordingly, the granting of the guarantee violates the Constitution and the law.

Pursuant to Article 25 of the Constitution and Article 19 of the Organic Law on Administrative Proceedings (*Ley Orgánica de Procedimientos Administrativos)*, acts that violate constitutionally vested rights are null and void. Therefore, the issuance of Petro is null and void pursuant to Venezuelan law.

Enactment of different regulations and agreements promoting cryptocurrencies

A few examples are as follows:

a) The Superintendence on Cryptocurrency and Connected Activities *(Superintendencia de Criptoactivos and Actividades Conexas,* now called SUNACRIP) and the Zamora Municipality, Miranda State, have executed agreements to grant certain benefits to taxpayers who cancel their taxes in Petro and other cryptocurrencies, as well as authorizing virtual mining.

b) The President has created special zones for mining and negotiating with Petro and other cryptocurrencies, which it has called "Petro Zones".[17]

c) Several resolutions enacted by the Ministry of Transport, which refer to payment of certain obligations due to the National Institute of Civil Aviation (*Instituto Nacional de Aeronaútica Civil*, INAC), the Institute of the International Airport of Maiquetía

(*Instituto Aeropuerto Internacional de Maiquetía*, IAIM) and the Bolivarian Airports Company (*Empresa del Estado Bolivariana de Aeropuertos*, BAER), provide that prices are established in Petro and that obligations may be paid in Petro and other cryptocurrencies, among others.

d) In the context of promotion of youth employment (*Gran Misión Chamba Segura*), the President imposed an obligation to create conditions to develop and strengthen a cryptocurrency "ecosystem", which would allow young people to be instructed regarding blockchain technology, digital mining, virtual trading, virtual exchanges, digital wallets, etc.

e) In the context of the economic emergency, the President has been granted powers to incorporate cryptoassets into the economy.

f) The Ministry of Economy and Finance (*Ministerio de Economía y Finanzas*) authorised the Superintendence of Insurance Activities (*Superintendencia de la Actividad Aseguradora*) to, in turn, authorise the issuance of bonds to guarantee certain obligations derived from public contracts paid in Petro.

g) Venezuela tried – and failed – to negotiate with India payment of their oil exports in Petro.

h) Earlier this year, the Agency on Intellectual Property (*Servicio Autónomo de Propiedad Intelectual*, SAPI) ordered that foreign corporations should only pay taxes and other obligations owed to SAPI in Petro. Such order was later reversed.

i) Additional taxes, levies, etc. have been established in Petro, even if they are payable by conversion to bolivars.

j) The minimum wage has also been informally established by reference to Petro.

k) The Supreme Tribunal of Justice has issued decisions ordering that damages be calculated in Petro.[18]

The validity of some of these instruments may be questionable. But, at least rhetorically, Venezuela has shown a positive attitude towards cryptocurrencies, which have not necessarily been translated into practice. However, the government has not always been consistent with this promotion.

Consistency of promotion and enforcement

First, in the past few years, different police forces (including the anti-money laundering task force) have apprehended cryptocurrency miners.

Second, certain government officials had also criticised and threatened persons dealing in cryptocurrencies. For instance, the Executive Vice-President of Venezuela (now Vice-President for the Economic Area) issued a statement in June 2018 criticising the "imposition" of "speculative cryptocurrencies' prices" and threatening to "severely punish" the culprits. This needs to be understood in the current local context: a foreign currency exchange control system has been in place in Venezuela since 2003, which has given rise to a parallel foreign currency market (which at times has been illegal), which the government has heavily criticised and sometimes tried to control. Cryptocurrency transactions have been used to circumvent the exchange controls regime. Therefore, the former Vice-President's threats, based on the exchange controls considerations, incidentally affected cryptocurrency ones.

However, the Executive's parlance has changed since July 2018 regarding exchange controls and there now seems to be a more tolerant approach towards the parallel market. In fact, the Constitutional Assembly enacted a constitutional decree abrogating punishments related

to the exchange regime (*Decreto Constituyente mediante el cual se establece la Derogatoria del Régimen Cambiario y sus Ilícitos*), published in the Official Gazette Nº 41.452, on August 2, 2018. Since that date, the Venezuelan government has taken a tolerant attitude towards exchange transactions, including cryptocurrency ones. However, this may change, as it has in fact done in the past 16 years of exchange limitations and controls.

Based on the above, we can argue that Venezuela has taken a positive view of cryptocurrencies – even promoting them – to the extent of issuing its own (illegal and unconstitutional) cryptocurrency, the Petro. Yet, to the extent that cryptocurrency use leads to circumventing exchange controls, the government's position will depend on the stance it takes, at any given moment, regarding exchange controls. At the time of writing this article, the governmental stance, as indicated above, is tolerant and flexible on exchange issues and transactions.

Cryptocurrency regulation

Regulation specific to cryptocurrencies

Instead of taking the more conservative approach of other jurisdictions, which have applied existing rules on commodities, capital markets, etc., to cryptocurrency transactions, Venezuela has issued regulations applicable specifically to cryptocurrencies and has even created a controlling body to supervise and control them: SUNACRIP (initially called SUPCACVEN).

The relevant regulations currently in force are the following: the Constitutional Decree on Cryptoassets and the Sovereign Cryptocurrency Petro, referred to above, published on April 9, 2018; and the Constitutional Decree on Cryptoassets Integral System, published on January 30, 2019.

Specific rules shall be addressed below, in each relevant section. However, two general ideas are important at this point:

1) The regulations contain both explicit and implicit controls and limitations. For instance, on the one hand, the Constitutional Decree on the Cryptoassets Integral System explicitly imposes, under Article 30, a registration obligation on all individuals and corporations who conduct activities related – directly or by connection – to cryptoassets; and Article 28 establishes an obligation for the exchanges (*casas de intercambio*) to obtain licences. On the other hand, the same decree establishes, among the powers vested in SUNACRIP under Article 11 (numbers 4, 9 and 12), the power to authorise and grant permits in connection with cryptoasset-related activities. Thus, although prior authorisation or permission is not expressly required by the rules, an implicit obligation to obtain such authorisation or permit is inferred from the rules. The rules detailing registration are referred to below.
2) Regulating cryptocurrencies via the Constitutional Decrees violates the Constitution for two reasons.
    - First, the Constitution provides, under Article 112, the right to economic freedom, that is, the right of every person to pursue their economic activities of choice, without limitation other than those provided by Constitution or law. The Constitution (which dates from 1999) establishes no limitation regarding cryptoassets. The law – which must be understood, as indicated above, as that enacted by the National Assembly (as opposed to the Constitutional Assembly) – does not provide limitations regarding this subject either.

- Second, Article 156 (32) of the Constitution limits legislation of certain matters (including commercial issues) to the national authorities; and Article 187 (1) mandates that the National Assembly legislates regarding matters reserved to the national authorities. This is known as *reserva legal*. Accordingly, commercial matters are part of the *reserva legal*, that is, only subject to regulation by law enacted by the National Assembly.

Therefore, a law is needed both to establish limitations on the right to economic freedom and to regulate commercial matters. Regulating cryptoassets qualifies as both and, thus, may only be done by law, and not by Constitutional Decree.

Accordingly, even if the regulations regarding cryptoassets exist, they are unconstitutional and, thus, null and void.

Apart from these regulations, which, as indicated, are targeted directly at cryptocurrency, certain other general rules, which are addressed below, may also be applicable.

Sales regulation

As indicated below, all activities related – directly or indirectly – to cryptoassets are regulated by the decrees enacted by the Constitutional Assembly, which were published in the Official Gazette on April 9, 2018 and January 30, 2019, pursuant to which both registration and authorisation requirements are applicable to individuals and corporations that conduct activities related to cryptocurrencies:

1) Article 30, which creates the Registration System, refers to the registration requirement extending to cryptocurrency miners, virtual exchanges, entities dedicated to saving or intermediation with cryptoassets, as well as to the suppliers of goods or services to persons who conduct such activities.
2) The implicit authorisation requirement provided for under Article 11 (numbers 4, 9 and 12) refer to (i) persons who participate in the system, (ii) corporations dedicated to intermediation in cryptoassets, (iii) corporations dedicated to virtual wallets, (iv) corporations dedicated to mining activities, and (v) the use of equipment intended for digital mining. To understand number (i) above, please take into account that under Article 6, the Cryptoassets Integral System is formed by "principles, rules and procedures, applied to individuals and corporations, public and private entities, include Communal Councils and other forms of Popular Power that interact with the purpose of guaranteeing that cryptoassets and related technologies are incorporated in the Bolivarian Republic of Venezuela". Accordingly, the aforementioned system seems to include all players in the cryptoasset community.
3) Articles 27 and 28 regulate the exchanges (*casas de intercambio*). The latter establishes that the powers of each exchange shall be determined by the specific Operation License (*Licencia de Operación*) granted by SUNACRIP. This matter was further addressed under a resolution that regulates operations of exchanges.[19] This resolution establishes, under Article 4, two types of licences: (i) general licences (which do not have restrictions regarding activities); and (ii) specific licences (that only authorise the exchanges to conduct certain activities). Further, the licences shall also limit other issues regarding the exchanges' activities, such as cryptocurrencies, foreign currency, types of users, etc.[20]

Summarising, based on the above, certain authorisation and registration requirements apply to any individual or corporation that conducts activities related directly or indirectly to

cryptoassets. This includes, as explained below, those wishing to acquire or sell cryptocurrency, and those involved in personal remittances in cryptocurrencies.

First, SUNACRIP issued the Resolution that regulates the Integral Registry of Cryptoasset Services (RISEC).[21] Pursuant to Article 4, all individuals and corporations that engage in activities related to the Cryptoassets Integral System are subject to registration.

A joint interpretation of several provisions seems to imply that all persons who participate in the cryptoasset market, in any capacity, need to register before the RISEC. First, Article 6 defines "users" as individuals or corporations that **acquire or use** goods or services based on cryptoassets or related technology. Second, Article 8 indicates the procedure for users to register before RISEC, and Article 9 provides the documentation needed for such registration. Third, references to users may also be found under several other provisions (such as Articles 7 and 11). The above may be interpreted as leading to the conclusion that even individuals and corporations who only wish to buy or sell cryptocurrency also need to register with RISEC, which – if so – we deem to be extremely unpractical.

Second, SUNACRIP has also issued a Resolution applicable to the receipt and transfer of personal remittances (*remesas*) in cryptocurrency in Venezuela.[22] Under Article 3, all individuals who send remittances to or receive remittances in Venezuela are subject to the aforementioned resolution. Such resolution establishes certain formalities, commissions, procedures, etc. Additionally, pursuant to Article 5, there is a limitation on the amount of cryptoassets that may be transferred monthly to Venezuela: the equivalent of 10 Petro per month.

Finally, regarding registration and authorisation issues, the Constitutional decree published in January 2019 establishes fines on those who conduct any activity related to cryptoassets without due authorisation. Additional penalties are established regarding other issues (such as altering or interfering with information technologies, damaging or modifying information technologies, etc.). In some cases, such penalties include prison terms. In any case, we question the validity of these penalties, since this is subject to the *reserva legal* addressed above, which also covers criminal matters, as well as due to the principle of legality (which mandates that penalties may only be imposed by a previously enacted law: *nullum crimen nulla poena sine lege*).

In addition to these rules, which are specifically tailored to address cryptocurrency, we believe that other rules, not specifically drafted, may be applicable. For instance, we believe this to be the case for securities regulations.

First, it may be possible that the Capital Markets Law (*Ley del Mercado de Valores*) also applies. Indeed, to the extent that a particular cryptocurrency or token also qualifies as a security under such law, it may as a result be applicable too. Other jurisdictions have taken the position that in order to determine whether cryptocurrencies or tokens qualify as securities, the particular characteristics of each cryptoasset must be analysed. Further, they have defended that in such case capital markets rules and controls would apply.

We believe this may be the case in Venezuela too. In fact, as explained above, certain cryptocurrencies – the Petro being a good example – may qualify as securities too. Further, the Capital Markets Law, under Article 46, mandates that, in case of doubt, the National Superintendence of Securities (*Superintendencia Nacional de Valores*, SUNAVAL) shall have the final right to determine if a particular asset qualifies as a security. If SUNAVAL were to determine that a certain cryptocurrency qualifies as a security, then all the capital markets rules would be applicable to the particular ICO and/or related activities.

We believe the authorities are not interpreting this matter from the perspective of dual control or regulations. There is no evidence of a joint approach by SUNACRIP and SUNAVAL. However, from a strictly legal point of view, this would be, in our opinion, the correct approach.

Taxation

Except as detailed below, the tax authorities and regulators have not issued tax rules regarding cryptocurrencies in particular. Accordingly, transactions relating to cryptocurrencies would be regulated by general rules on the matter.

However, the following tax-related issues are relevant:

a) Venezuela has assumed a general obligation to promote the use of cryptocurrencies. It has also taken on a specific obligation to accept payment of taxes by means of cryptocurrencies in the agreements between SUPCACVEN and the Zamora Municipality. Further, it has assumed such obligations particularly with respect to Petro in the different versions of the Petro's whitepaper.

b) Article 7 of the Presidential Decree, which creates "Petro zones", provides an exception regarding customs duties for the import of goods related to electronic equipment, computer equipment, software licences, hardware, electric power plants, air conditioning units, support equipment, etc. used in connection with cryptocurrency mining. Such exception would apply in Margarita Island, Los Roques, Territorio Insular Francisco de Miranda, Paraguaná and Ureña – San Antonio, and would last for two years, beginning on March 22, 2018.

c) Article 17 of the 2019 Constitutional Decree provides a similar exception regarding taxes and custom duties for the import of goods and technical equipment, and imported, exported or in-transit goods, which are necessary for SUNACRIP's role. A presidential authorisation is required in this case.

d) A Presidential Decree established that all taxes generated due to transactions conducted in cryptocurrency need to be calculated and paid in the same cryptocurrency in which the transaction was conducted.[23] Transactions related to (i) securities traded in the stock exchanges, and (ii) export of goods and services, were exempted from this obligation. However, to the best of our knowledge, such mandate has not been implemented by the tax authority (probably because certain regulations necessary for such implementation are still pending).

Money transmission laws and anti-money laundering requirements

Few specific rules regarding these matters have been formally enacted in connection with cryptocurrencies, and these are addressed specifically to exchanges (*casas de intercambio*).

Indeed, Article 6 of the resolution published on March 2019 regarding exchanges specifically indicates that such entities must comply with applicable legislation regarding anti-money laundering, specifically referring to: (i) the Organic Law on Organized Crime, Terrorism Financing and Proliferation of Mass Destruction Weapons; (ii) recommendations issued by the Financial Action Task Force (FATF), referred to by its name in Spanish: GAFI; and (iii) the Drugs Law.

Article 6 further establishes an obligation to notify SUNACRIP and the Prosecutor General's Office regarding any irregular movement detected in transactions, that may constitute money laundering, financing of terrorism, proliferation of weapons of mass destruction, drug

trafficking, and other related crimes. Failure to report may lead to dissolution and liquidation of the exchange, cancellation of its registration before the Commercial Registry, as well as to the imposition of penalties (of both administrative and criminal nature), among others.

Regarding all other stakeholders, general rules on anti-money laundering and related activities would be applicable to cryptocurrencies and, in the case of cryptocurrencies which also qualify as securities, the specific rules on the matter enacted in connection with the capital market would also be applicable.

Promotion and testing

As already indicated, Venezuela is bound to promote the use of cryptocurrencies.

Also, as referred to above, Venezuela has created two types of special "environments" for the promotion and development of cryptocurrencies.

First, the Zamora Municipality has in theory created a special space for (i) cryptocurrency mining, and (ii) payment of taxes in cryptocurrency.

Second, the President has created the "Petro Zones", which also have benefits from the point of view of mining (including the custom tax benefits referred above) and payment in cryptocurrencies (e.g. gas prices).

Ownership and licensing requirements

Activities related – either directly or indirectly – to cryptoassets are subject to prior authorisation, and individuals and corporations conducting them are subject to registration,

However, in our opinion, this would not extend to ownership. However, as indicated above, buying and selling cryptocurrencies may be interpreted as seeming to require registration before RISEC, which, as indicated, seems extremely unpractical.

Mining

As indicated, mining cryptocurrency in Venezuela is permitted, subject to prior authorisation, pursuant to Article 11.9 of the Constitutional decree dated January 2019 and registration, pursuant to Articles 29 and 30 thereof.

Border restrictions and declaration

The only specific rules regarding these matters have been enacted in connection to remittances, as addressed above.

Therefore, general rules would be applicable. For instance, the Law on the Central Bank of Venezuela and the Organic Law Against Organized Crime and Financing of Terrorism (*Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo*) contain limitations regarding import and export of fiat money, under Articles 118 and 137 in the case of the first law, and import and export of money or securities by individuals entering or leaving the country, under Article 22 in the second one. We believe none of these are extensible to cryptocurrency transactions.

Reporting requirements

No rules regarding these matters have been formally enacted specifically in connection to cryptocurrencies. General rules may be extensible to cryptocurrencies.

Estate planning and testamentary succession

There are no special rules regarding this matter. We have not been privy to any estate planning or succession by testament containing cryptocurrency holdings in Venezuela.

* * *

Endnotes

1. Asamblea Nacional Constituyente. *Decreto Constituyente mediante el cual se acuerda apoyar los anuncios del Presidente Nicolás Maduro Moros sobre el Programa de Recuperación y Prosperidad Económica*. Official Gazette Nº 41.452, August 2, 2018, Article 1: "the value [of VES] shall be anchored on the value of the Petro…".
2. The efficiency of the conversion is doubtful since, again due to hyperinflation, amounts have increased substantially, although not reaching pre-conversion levels yet.
3. The Constitutional Assembly is a body elected in 2017. References to its validity and functions are made below.
4. The validity of this decree is highly questionable. First, the Constitutional Assembly was elected amidst very controversial circumstances (which included the technical company hired to conduct the election having stated that the electoral authority announced more votes than those actually cast), which may render its appointment null and void. Yet, we shall refer to only one of those circumstances: the basis for the election violated the principle of universal vote, which is a right recognised under Article 63 of the Constitution. Such violation occurred because the principle of "one person – one vote" was not respected, since certain categories (workers, women, natives, etc.) had the right to cast more than one vote, while other persons did not. Accordingly, the election of the Constitutional Assembly is null and void. Second, the Constitutional Assembly – even setting aside the nullity of the election – was elected to enact a new Constitution, not to enact other regulations. Some may argue that the Constitution, under Article 347, empowers the Constitutional Assembly to enact a new legal system (*ordenamiento jurídico*). However, that must be understood in the context of its mandate: the Constitutional Assembly would be allowed to enact new regulations only to the extent necessary to make the legal system compatible with the new Constitution. This is not the case. Further, the Constitutional Assembly has not even enacted the new Constitution.
5. President. *Decreto Nº 3.196, mediante el cual se autoriza la creación de la Superintendencia de los Criptoactivos y actividades conexas venezolana*. Official Gazette Nº 6.346 (E), December 8, 2017, Preamble. This decree was abrogated by Constitutional Assembly by means of the *Decreto Constituyente sobre el Sistema Integral de Criptoactivos*, published in the Official Gazette Nº 41.575, on January 30, 2019, which further regulates cryptocurrencies as addressed below.
6. Venezuela. "Petro. Papel Blanco. Versión Beta 0.9. Propuesta Financiera. 30 de enero 2018." Available at http://pandectasdigital.blogspot.com/2018/01/whitepaper-libro-blanco-del-petro.html (last visited 7/20/2018).
7. Venezuela. "Petro. Papel Blanco. Beta 1.0. Propuesta Financiera y Tecnológica. 15 de marzo 2018". Available at http://www.elpetro.gob.ve/pdf/esp/Whitepaper_Petro_es.pdf (last visited 7/20/2018).

8. President. *Decreto Nº 3.292 mediante el cual se determina como respaldo para la implementación de operaciones de intercambio financiero y comercial a través de criptoactivos, el desarrollo potencial de 5.342 MMBN de Petróleo Original en Sitio (POES) pesado y extrapesado, de acuerdo a una certificadora internacional independiente, localizado en el Bloque Ayacucho 01, de la Faja Petrolífera del Orinoco Hugo Chávez Frías*. Official Gazette Nº 41.347. February 23, 2018.
9. Constitutional Assembly. *Decreto Constituyente sobre Criptoactivos y la Criptomoneda Soberana Petro*. Official Gazette Nº 6.370 (E), April 9, 2018, Articles 5 and 12.
10. Venezuela. "Petro. Hacia la Revolución Digital." Available at https://www.petro.gob.ve/files/petro-whitepaper.pdf.
11. LEPERVANCHE, Luisa and ACEDO SUCRE, Manuel. *A few ideas on Petros and other cryptocurrency transactions in Venezuela*. Available at http://www.menpa.com/serve/file/assets%2Fuploads%2FEFEE5A71CC346147C.pdf (last visited 7/20/2018). CAPRILES BAENA, Gonzalo. Petro, la "moneda virtual" del gobierno venezolano. Available at http://www.cavecol.org/wp-content/uploads/2018/02/BDE-5-PETRO.pdf (last visited 7/20/2018). HERNÁNDEZ, José Ignacio. *¿Es el petro una operación de crédito público?* Available at https://prodavinci.com/es-el-petro-una-operacion-de-credito-publico/ (last visited 7/20/2018).
12. MONALDI, Francisco J. *Is the Petro Truly Backed by Oil Reserves?* February 27, 2018. Available at https://www.caracaschronicles.com/2018/02/27/petro-truly-backed-oil-reserves/ (last visited 7/20/2018).
13. LEPERVANCHE, Luisa y ACEDO SUCRE, Manuel*, op. cit*. CAPRILES BAENA, Gonzalo, *op.cit*. HERNÁNDEZ, José Ignacio, *op.cit*.
14. National Assembly. *Acuerdo sobre la emisión de la criptomoneda Petro. 9 de enero de 2018.* Available at https://es.scribd.com/document/368773539/Acuerdo-sobre-la-emision-de-la-criptomoneda-Petro#from_embed (last visited 7/20/2018).
15. However, this version of the FAQs was eliminated when the new Executive Order 13827, dated March 19, 2018, was issued. Such order prohibits transactions on any "digital currency, digital coin, or digital token". After the issuance of said order, the position of the OFAC changed, and now reflects that Petros are forbidden under the new Executive Order, as evidenced in https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#venezuela, question Nº 564 (last visited 7/20/2018).
16. National Assembly. *Acuerdo sobre la emisión de la criptomoneda Petro. 9 de enero de 2018*; referred to above.
17. President. *Decreto Nº 3.333, mediante el cual se crean como Zonas Petro: La Isla de Margarita, Estado Nueva Esparta. Los Roques, Territorio Insular Francisco de Miranda. Paraguaná, Estado Falcón. Ureña-San Antonio, Estado Táchira, a los fines de incorporarlas al desarrollo de la Minería Virtual y el uso de cripto-activos como elementos estructurales de la diversificación de fuentes de divisas tanto para el desarrollo nacional como de las actividades económicas propias de las citadas áreas*. Official Gazette Nº 41.366. March 22, 2018.
18. On October 31, 2018, the Political-Administrative Chamber issued the first decision in this regard.

19. Vicepresidencia Sectorial de Economía. *Providencia mediante la cual se regula la operatividad de las Casas de Intercambio en el Sistema Integral de Criptoactivos*. Official Gazette Nº 41.609. April 3, 2019.
20. Pursuant to the information of SUNACRIP, as of August 1, 2019, all licences granted by SUNACRIP qualify as general licences: https://sunacrip.gob.ve/casas.html.
21. SUNACRIP. *Providencia mediante la cual se regula el Registro Integral de Servicios en Criptoactivos (RISEC)*. Official Gazette Nº 41.578. February 4, 2019.
22. SUNACRIP. *Providencia aplicable al trámite de remesas en criptoactivos en la República Bolivariana de Venezuela*. Official Gazette Nº 41.581. February 7, 2019.
23. President. *Decreto N1 35 en el marco del Estado de Excepción y de Emergencia Económica, mediante el cual los sujetos pasivos que realicen operaciones en el territorio nacional en moneda extranjera o criptodivisas, autorizadas por la ley, deben determinar y pagar las obligaciones en moneda extranjera o criptodivisas.* Official Gazette Nº 6.420 (E). December 28, 2018.

Luisa Lepervanche
Tel: +58 212 909 1611 / Email: llepervanche@menpa.com

Luisa Lepervanche graduated from the Law School of Universidad Católica Andrés Bello, *cum laude* and specialised in corporate law at Universidad Metropolitana. Later, she participated in the International Program of Hydrocarbons Management at Instituto de Estudios de Educación Superior (IESA). She is a Partner at Menpa, after re-joining the firm after being Legal Counsel to The Coca-Cola Company for Venezuela and the Caribbean. She has taught commercial law, legal analysis and human rights and has worked on human rights issues. Her practice focuses on corporate law, M&A, banking and finance, international sanctions, project financing and debt restructuring, real estate issues, public law and *pro bono* work. Luisa has written several legal articles. She is a member of the Legal Committee of the *Cámara Venezolana Americana de Comercio e Industria* (Venamcham). Luisa is fluent in Spanish and English.

Mendoza, Palacios, Acedo, Borjas, Páez Pumar & Cía. (Menpa)

Urb. Las Mercedes, Calle Veracruz con Calle Cali, Torre Aba, Piso 1 y 2, Caracas, 1060, Venezuela
Tel: +58 212 909 1611 / URL: www.menpa.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

- **Alternative Real Estate Investments**
- **AI, Machine Learning & Big Data**
- **Banking Regulation**
- **Bribery & Corruption**
- **Cartels**
- **Commercial Real Estate**
- **Corporate Tax**
- **Employment & Labour Law**
- **Energy**
- **Fintech**
- **Fund Finance**
- **Initial Public Offerings**
- **International Arbitration**
- **Litigation & Dispute Resolution**
- **Merger Control**
- **Mergers & Acquisitions**
- **Pricing & Reimbursement**

Strategic partner: