大成 DENTONS

Blockchain and smart contracts

ACC Phoenix
March 2019

STAFFORD MATTHEWS

Managing Partner, Silicon Valley

Dentons

Why smart contracts and blockchain?

What the Internet does

And does not do.

Why smart contracts and blockchain?

- The **Internet** was originally designed as a peer-to-peer means of sending messages and communicating **information**.
- It was not designed as **e-commerce** platform.
- As it has evolved the Internet has **split** between these two functions.

Why smart contracts and blockchain?

- As a “**marketplace of ideas**”, the distribution of **information** on the Internet can be relatively **untrusted.**
- Information is **published by anyone** and everyone in theory can judge for themselves.

Why smart contracts and blockchain?

- But as a marketplace for **goods and services - a marketplace of “value”:**

  The Internet has not fundamentally altered the **basic mechanism** of how individual and corporate parties **transact** their business.

Why smart contracts and blockchain?

- The **form** of the transaction may be **digital.**
- For example, parties may use **email** to exchange **digital copies** of contracts and other documentation, or electronically **transmit** funds, or license and **download** books or films in digital form in exchange for credit card charges.
- But **no real change** from traditional **brick and mortar** transactions.

Central Authority model

Created by Adrien Coquet
from Noun Project

Most commercial transactions are **not peer-to-peer** and still require a **central** or **controlling authority** or other **“trusted” intermediary** to conduct the exchange.

Central Authority model

- These **central authorities** include banks, credit card companies, trust and escrow companies and various online platforms.
- Where parties who **do not know each other** exchange money for goods and services or otherwise promise to hold or transfer assets:

  The **need** for **trust and security** is **high**.

Outer limits of central authority

There are structural **challenges** with the **trusted authority** model for Internet transactions:

- As trusted platforms **scale,** there can be a **concentration** of transactions and **power** in a increasingly smaller number of key companies acting as trusted authorities.
- For example, in 2016 three online retailers accounted for **65 percent** of all cross-border purchases on the Internet.

Outer limits of central authority

- Another baseline issue relates to the direct or indirect ownership, collection and use of **personal data** for commercial purposes.
- Use of the trusted authority model requires **disclosure** of personal data to the authority and **retention** and secure **control** of that data by the authority.

Outer limits of central authority

- The third issue is **scalability** itself. It can become increasing difficult to scale a system moderated by a single authority or group of authorities.
- Compare a **distributed model** that democratizes the spread of technology. Examples: the **personal computer** rather than the mainframe; the **smart phone** rather than the personal computer; **distributed** power generation.

Decentralized Ledger as a Solution

- The proposed solution to the issues raised by the centralized authority model is known as:

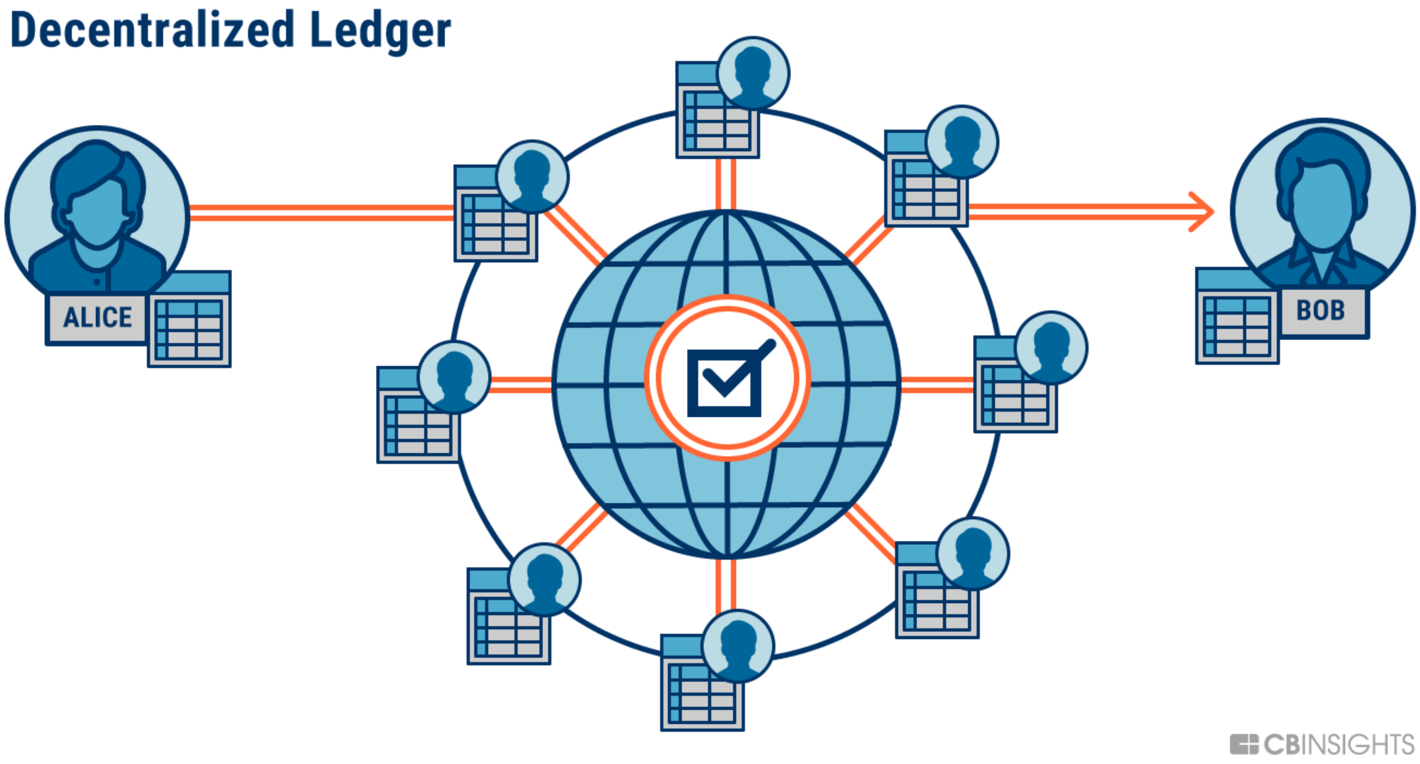
  Decentralized or **distributed ledger technology [DLT]**.

Decentralized Ledger Technology

The basic concept of **DLT** is that:

- Transactions are conducted **peer-to-peer**.
- An identical record of every transaction is **distributed** to and held by **every computer on a network** rather than by a single central authority.

Decentralized Ledger Technology

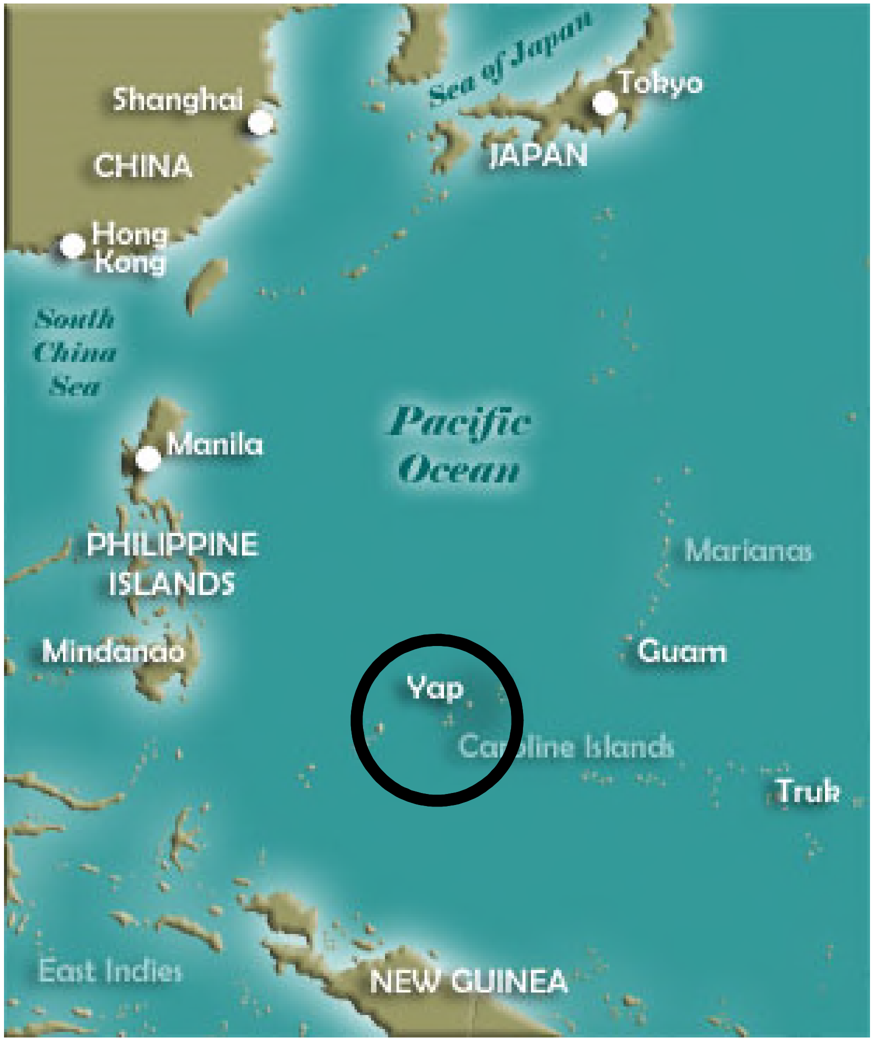


Decentralized Ledger Technology

- Decentralized ledger technology is a version of the general principle that:

  “The **smartest person** in the room is always – the **room.”**

Decentralized Ledger Network - the Prequel



Decentralized Ledger Network

Decentralized Ledger Network

Blockchain and Smart Contracts

Connection to Smart Contracts

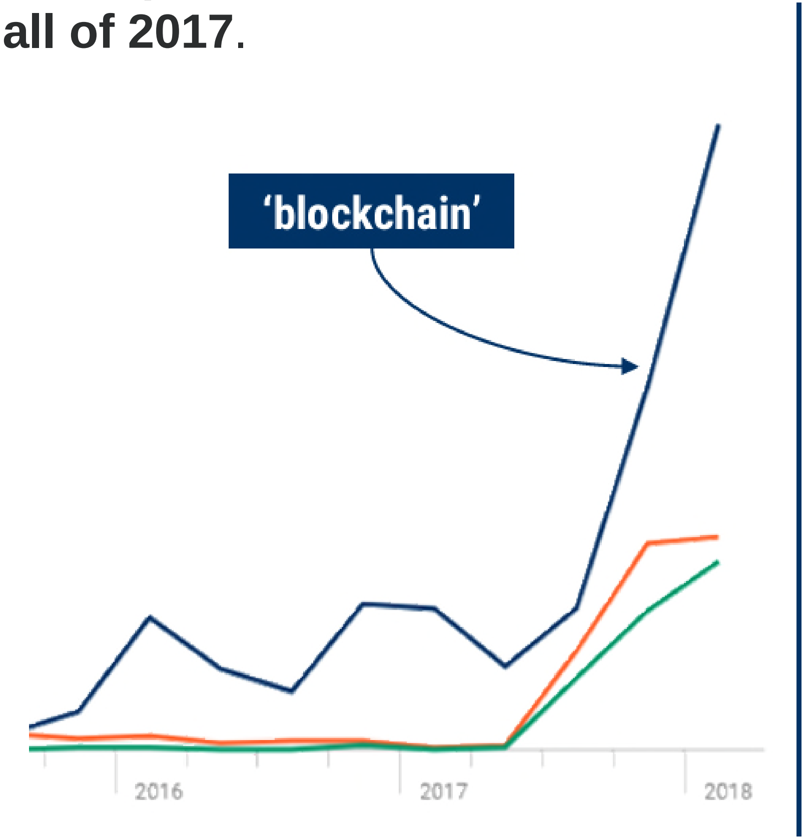
- **Blockchain** is a **subset** of decentralized ledger technology.
- Blockchain currently is the **incumbent platform** or application that implements the **decentralized ledger technology**. It has been in use in some form for the last 10 years.
- There are **alternatives** to blockchain being developed, including Hedera Hashgraph Platform and IOTA Tangle.

Connection to Smart Contracts

- **Smart contracts** in turn are a **subset of blockchain.**
- Smart contracts are a form of computer code that automates the execution and enforcement of contracts. The computer code comprising smart contracts is **embedded** in and operates on the **blockchain platform**.

Blockchain as a Solution - Why Now?

- "Blockchain" was mentioned close to 300 times on Q1 2018 US corporate earnings calls, double all of 2017.



CBINSIGHTS

Blockchain as a Solution - Why Now?

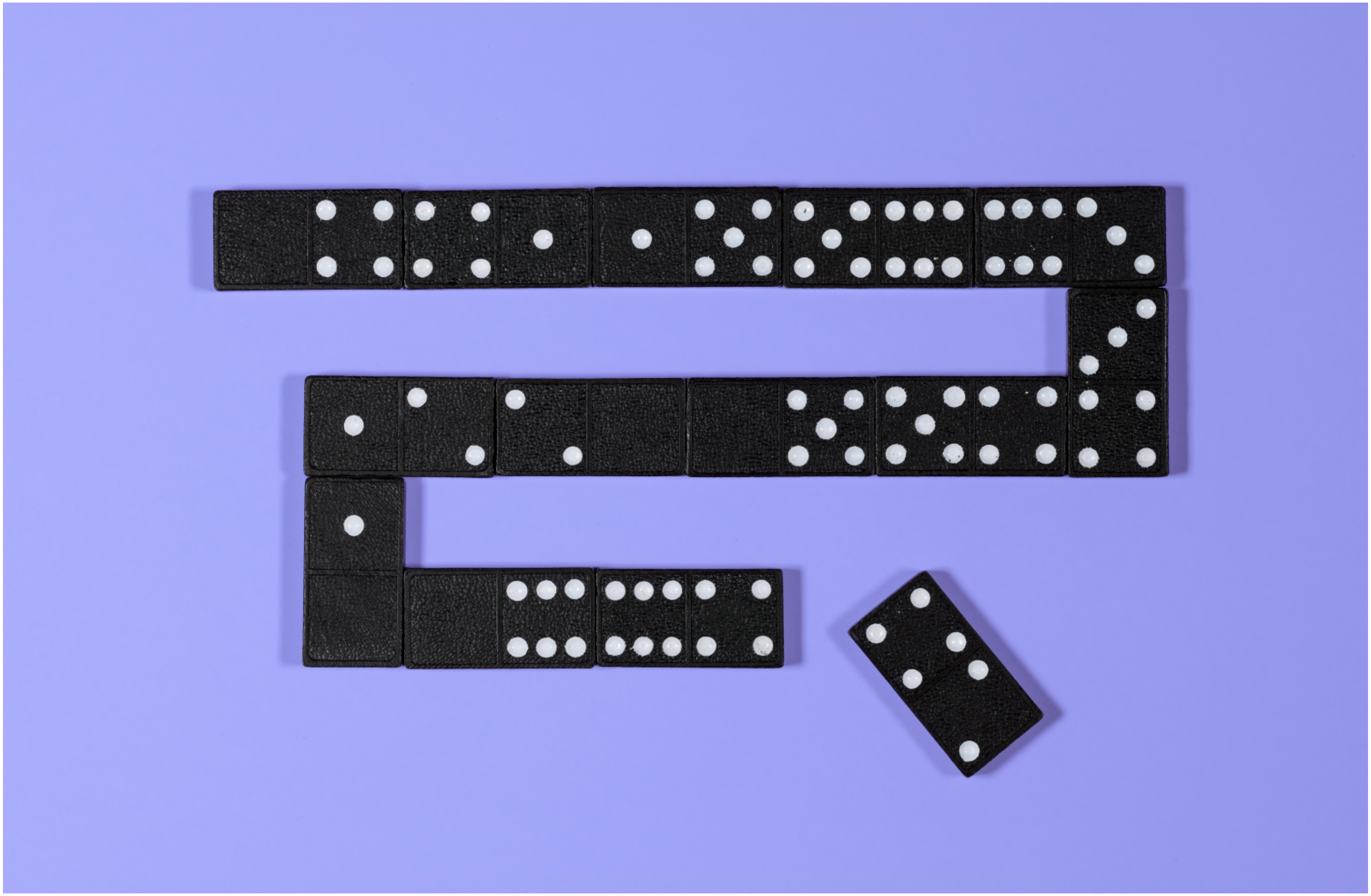
- A survey conducted by Deloitte indicates that **42 percent** of key companies in the consumer products and manufacturing industries plan to invest at least $5 Million in 2019 in blockchain technologies.*

*Deloitte LLP, “New tech on the block”, May 2018.

What is a blockchain?

Created by Adrien Coquet
from Noun Project

Technology
Innovation



What is a blockchain?

Blockchain is

(a) a software **database** that resides on a computer network that

(b) permits all parties within the network to enter into and record **transactions** and other **data** in a linked series of cells

(c) using a **decentralized** and **shared digital ledger**

(d) once entered, the data is **immutable** and **cannot be changed**.

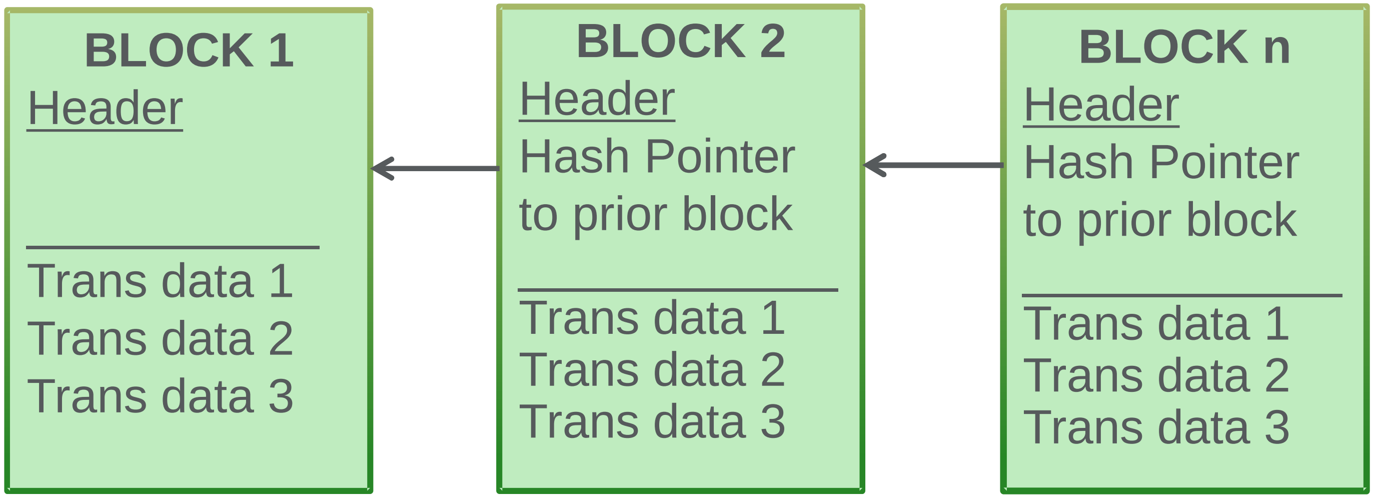
What is a blockchain?

- In a pure blockchain there is **no central authority** who decides what goes on the blockchain or holds the only authorized copy of the transaction.

■ Blockchain Technology Basics

Blockchain Technology Basics

- The blockchain holds data on a computer network in a series of cells ["**blocks**“] that are **chained** together in chronological order.



Blockchain Technology Basics

- Each block is connected to the **prior block** by means of a link known as a cryptographic "**hash**". The hash is generated mathematically generally is 256 bits in length.
- This "hash" is how each block in the chain is **locked**.

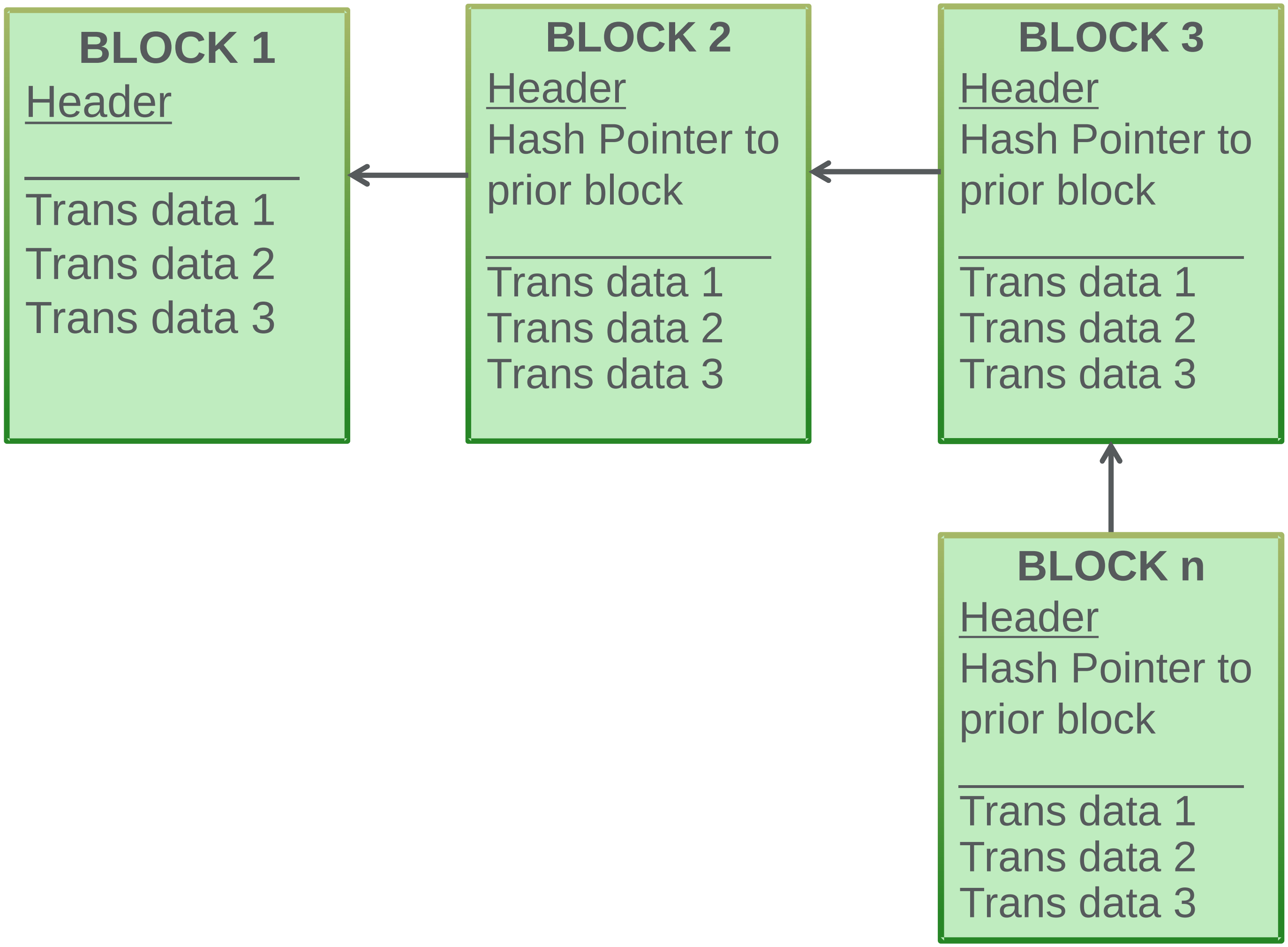
Steps in a new blockchain transaction

- A party initiating a **new transaction** [such as a transfer of bitcoins] first broadcasts the data to the entire blockchain network using system software.
- The computers in the blockchain network [known as "nodes"] then compete with each other to **validate** the transaction using pure math to solve difficult puzzles. Solving the problem requires very substantial computing power.

Steps in a new blockchain transaction

- The first one to solve the math problem (a “**miner**”) gets paid in digital currency.
- The new block containing the new transactions is then **validated** by additional processes and locked into **end of the chain.**

Steps in a new blockchain transaction



BLOCK 1
Header

Trans data 1
Trans data 2
Trans data 3

BLOCK 2
Header
Hash Pointer to prior block

Trans data 1
Trans data 2
Trans data 3

BLOCK 3
Header
Hash Pointer to prior block

Trans data 1
Trans data 2
Trans data 3

BLOCK n
Header
Hash Pointer to prior block

Trans data 1
Trans data 2
Trans data 3

Steps in a new blockchain transaction

- If someone tries to alter or **tamper with** the data in Block A, then the hash of that data contained in the following Block B will conflict and the change will not be accepted by the network.
- Each block in the chain thus once linked is designed to be **immutable** and not modified or deleted.

Steps in a new blockchain transaction

- As part of this process, the parties are issued **public and private keys** so they can conduct the transaction on the blockchain.

Steps in a new blockchain transaction

- Exact copies of the current blockchain ledger containing all of the transactions in the **entire** chain are **updated** and **distributed** to **every computer** in the network on a continuous basis.
- In this manner the entire blockchain database at any point in time is **shared** as the distributed ledger.

Steps in a new blockchain transaction

Key Point:

- Anyone attempting to hack into or tamper with any existing block thus would have to alter **at least a majority** of the individual copies of the current blockchain ledger then distributed to all of the members in the network – which could number in the hundreds of thousands or more.
- This is the essential feature of the distributed ledger technology.

Which Blockchain?

- Anyone can download the relevant software and create their own blockchain.
- There are basically **three types** of blockchains:

(1) **Public** or "**permissionless**" blockchains, which are open to the public and are generally fully transparent. Bitcoin and most other cryptocurrencies use this type of blockchain.

Which Blockchain?

(2) **Hybrid** or **consortium** blockchains, which may have a large number of affiliated participants.

(3) **Private** blockchains, where the shared database of transactions is limited to a certain **specified group** of participants or parties**.**

Which Blockchain?

- Both consortium and private blockchains are referred to as "**permissioned**" blockchains.
- This is because counterparties and other participants can be granted **different degrees of access and authority** to initiate and interact with the block-chained transaction. Smart contracts used by corporations generally will be in permissioned blockchains.

Blockchain – Main Uses

Blockchain has three main categories of uses:

- Creation and execution of **smart contracts**.
- **Peer-to-peer transfer of digital assets** at the human or institutional level, including the creation and exchange of cryptocurrencies - such as Bitcoin.
- Storing and validation of **digital records** such as stocks and land title.

Blockchain – Main Uses

- The issuance and trading of **cryptocurrencies** such as **Bitcoin** are outside the scope of this presentation, but have been the main driver of blockchain development up to this time.

Blockchain as Hype

There are **sceptics:** Wired Magazine had a May 2018 article entitled "187 Things the Blockchain Is Supposed to Fix“. Wired included the following key Blockchain priorities:

Skynet*

The movie industry's **accounting** practices

Fake news

Authenticity in **cannabis** sales

Paying for things with your **face**

*See The Terminator v. Basically Everybody (1984) et seq.

■ Smart contracts

What is a smart contract?

- **Blockchain** technology is not **only** a string of static data records stored in blocks.
- It is possible using certain versions of blockchain software to also store **executable computer programs** within the blockchain to perform functions.

What is a smart contract?

A "smart contract" is **computer code:**

- embedded in a **blockchain** or [eventually] other form of **decentralized ledger** that
- incorporates all or part of a written **legal agreement** and
- transfers digital assets or vests rights or is otherwise triggered when a set of **pre-defined terms and conditions** are satisfied.

What is a smart contract?

Key Points:

- The "**smart contract**“ once written can be **self-executing** and **autonomous**, without the need for further action by the parties.
- A form of **robotics for commercial contracts.**

Smart Contract Examples

- **Smart contracts** do not have to be complex and can be used to perform a few **simple functions** repetitively for a large group of transactions or agreements.
- The key to **smart** contracts is their ability to obtain and handle **variable data** and to automatically process and **act** on those variables.

Smart Contract Examples

- **Example**: (a) Green transfers **ownership** of securities or other digital assets into the **blockchain**; (b) Blue is required to **pay** $5X for the assets on a certain date, but $8X for the assets if Event A occurs prior to that date.
- The smart contract determines **whether** Event A has **occurred**, and then **self-executes** by (i) paying Green $5X or $8X and (ii) transferring ownership of the securities to Blue.

Why? Limits of current contracts

- **“Bespoke” contracts** do not scale well.
- **Proliferation of parties** decreases efficiencies.
- **Verification of performance is** an issue as **number** of contracts and **locations** of performance scale.
- **Trust** is an issue especially in cross-border transactions where **local courts** must enforce performance and payment obligations.

Smart Contract Example: Insurance

Smart automobile insurance policy:

- Track driver using sensors.
- All data would be **continuously and permanently added** to the blockchain along with traffic citations and other external data for each policyholder.
- The smart policy automatically (i) **increases or decreases** the **premium** based on the data and (ii) **withdraws** payment from the driver's bank account.

Smart Contract Example: Supply Chain

- Increased complexity in the **cross-border manufacturing and distributing** of goods.
- New legal and compliance obligations for **supply chain transparency** require companies to trace, document and report the source of products and their components.*

*See for example the California Transparency in Supply Chains Act of 2010, California Civil Code Section 1714.43, which focuses on prevention of human trafficking and use of child labor in manufacturing.

Smart Contract Example: Supply Chain

- Use of smart contract: **Coordination of numerous counterparties**; tracking and verification of **source** of components; **supply chain transparency** under applicable law.
- Bar codes or RFID or IOT devices or other sensors would automatically **identify and track** each **individual component** and upload data to the blockchain as its status changes.

Other Smart Contract Use Cases

- **Stocks:** Trading and registration of shares of corporate stock. Several states including Delaware have recently enacted statutes permitting use of blockchain as the official stock ledger.
- **Financial Instruments:** Trading of derivatives or other financial instruments.
- **Trade Finance:** Automated issuance of or substitution for letters of credit, guarantees and trade finance instruments.

Other Smart Contract Use Cases

- **Clinical Trials:** Automated obtaining and tracking of required patient consents; standardization of patient inquiries; and secure sharing of personal medical information across institutions.
- **Scientific Research:** Real-time secure sharing of medical or other scientific research between institutions to avoid the “silo” effect; automated nondisclosure terms to protect patent and other IP rights; automatic release of grant funds.

Smart Contract Technology

Building of Smart Contracts

How is a smart contract **constructed** using a blockchain?

Building of Smart Contracts

- There are **competing versions of blockchain software**, similar to competing versions of computer system software such as Microsoft and Apple.
- For example, **Bitcoin** has its own blockchain system for the issuance and transacting of the Bitcoin cryptocurrency as an alternative to fiat currencies such as dollars and Euros.

Ethereum Blockchain System

- The main blockchain software used for smart contracts is **Ethereum**.
- **Ethereum** is a separate open-source, public, blockchain-based distributed computing platform and operating system.

Our Founder

Vitalik Buterin, Russian-Canadian, born January 31, 1994 (age 25 **now**). University of Waterloo [dropped out]. Invented Ethereum at age 19. Net worth > $500 Million.

Ethereum Blockchain System

The difference is that unlike Bitcoin, the **Ethereum platform** also contains additional critical features:

- **Smart contract (computer code) functionality** permitting self-executing contract terms and conditions to be embedded in the blockchain.
- The ability to perform **computations** within the blockchain.

Ethereum Blockchain System

- The ability to obtain **extrinsic or external data** from third parties outside of the blockchain using a function called an "**oracle**".
- The ability to **combine** this external data with the executable computer code within the blockchain to perform smart contract functions.
- **Decentralized Applications (Dapps)** run on top of the platform to add functions.

■ Building a Smart Contract - Steps

Building a Smart Contract: Step 1: Agreement

- Two or more parties must **negotiate** a written legal contract or use a **form contract** from one of the parties or an affiliation group containing their agreement.
- The contract must include specific transactions or other rights and obligations that vest or are executed upon **specified sets** of conditions.

Building a Smart Contract: Step 2: Conditions

The parties **must set**:

- **All of the conditions** to be automated under their agreement
- All **permutations** of each of those conditions
- The **intended result or instruction** in each case.

Building a Smart Contract: Step 2: Conditions

The set conditions can be **internal** to the contract:

- The **manufacture or shipping or delivery** of a product
- A schedule of **due dates** for payments
- **Expiration** of inspection rights or warranties
- A form of **deliverable** or notice by a party.

Building a Smart Contract: Step 2: Conditions

The set conditions can be **external** to the contract:

- Acts or omissions of **third parties**
- Accidents or weather or climate events or other **acts of God**
- Other events of **force majeure**
- Financial or product **market triggers**
- **Changes** in legal or financial status

Building a Smart Contract: Step 3: Coding

- The smart part of a contract requires the writing of a **computer program or code** which incorporates all of the set conditions and results, so that the contract will automatically be performed when those conditions are triggered.
- In Ethereum the main programming language for writing smart contracts is **Solidity**.

Building a Smart Contract: Step 3: Coding

Key Point:

- A smart contract therefore always has **two versions:** the human language version and the machine code version.

Building a Smart Contract: Step 3: Coding

Written Contract:

- Human language
- All parts of agreement
- Freely modifiable in writing by the parties.
- Subject to interpretation

Smart Version:

- Machine computer code
- Only transactions to be automated
- Embedded into blockchain or other ledger
- Cannot be changed - only added to.

Building a Smart Contract: Step 4: Blockchain

- The smart contract code is **published** to the blockchain or other decentralized ledger network by the parties.
- The smart contract code is **verified** and then "written" into a block in the blockchain or other ledger.
- The parties are issued **public and private keys** so they can conduct the transaction on the blockchain.

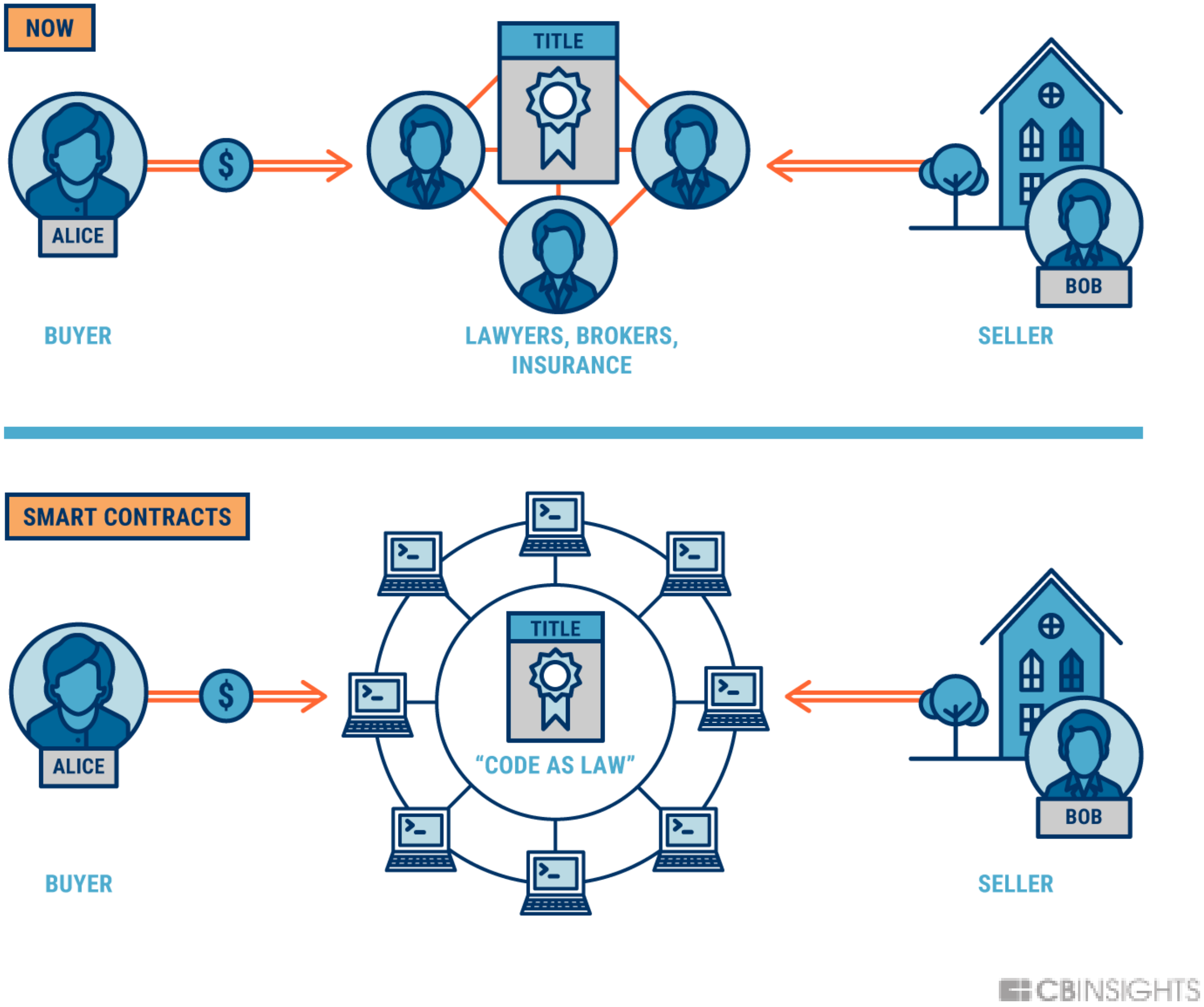
Building a Smart Contract: Step 5: Execute

- **Execution** of the transaction is triggered:
  - by a message sent by a party validated by its **private key** or
  - by the **objective satisfaction** of external or other **events or conditions** coded into the program.
- The transaction [such as transfer of funds or title] is **automatically performed** pursuant to the smart contract code.

Building a Smart Contract: Step 6: Recording

- The **completed transaction** [for example: sale of property; payment of royalties; delivery of shipment] is verified and written into a new block in the chain.
- All of the computers [nodes] which are part of the relevant network are then distributed **updated copies of the ledger** which show that the transaction is completed.

Building a Smart Contract



Building a Smart Contract

- A smart contract generally will **not be the whole agreement** but only those portions of the contract that are highly **process-based,** can be represented in executable **computer code**, and can be **usefully automated** in a manner that is more efficient and easier to scale than human processing.

Building a Smart Contract

- In its current stage, **better suited to industrial scale** or **repetitive** forms and transactions rather than "one off" agreements.

Legal Issues

There are number of **legal and functional issues** that can arise from the use of smart contracts in their **present stage** of development.

Legal Issues

A. Offer and acceptance

- Parties to a contract must evidence acceptance of the terms and conditions of the agreement.
- There are debates in the relevant circles as to whether existing **electronic signature acts** are sufficient to meet legal standards or whether **additional legislation** is necessary to validate blockchain smart contracts.

Legal Issues

- What rules apply if the statute requires that the contract be "**written**"?
- The Electronic Signatures in Global and National Commerce Act (“**ESIGN Act**”) and the Uniform Electronic Transactions Act (“**UETA**”) and equivalent statutes in several states provide grounds for enforcement of smart contracts once electronically signed.

Legal Issues

- The digital **acceptance** by the parties of a smart contract will need to be by a method evidencing clear **notice** of and an **agreement** to the terms of the contract rather than by mere **implication of assent**.
- Enterprises in particular need to be mindful of the issues of enforceability currently raised by "**browse-wrap"** agreements for online goods and services.

Legal Issues

- A number of courts for example have recently held "browse-wrap" agreements **unenforceable** where the subject party was deemed to not have received sufficient notice of the terms of the contract or to not have consented under the relevant facts and circumstances.*

E.g., Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171 (9th Cir. 2014) ; *Hines v. Overstock.com, Inc.,* 380 F. App'x 22, 24 (2d Cir. 2010); *Cvent, Inc. v. Eventbrite, Inc.,* 739 F. Supp. 2d 927 (E.D. Va. 2010); *Be In, Inc. v. Google Inc.*, 2013 WL 5568706 (N.D. Cal. Oct. 9, 2013).

Legal Issues

B. “Lost in Translation”: Smart Contract Coding

- Written contract terms need to be converted into **computer language** to be embedded as a smart contract in a blockchain. This needs to be done with **complete precision**.
- After a smart contract is added to the blockchain it is immutable and cannot be changed.

Legal Issues

- It is essential that legal counsel and its software coding counterparts establish procedures so there are **no gaps or mistakes** as between the two versions.
- Use of a "**sandbox**" to test and validate smart contract code is necessary before it is embedded in the blockchain.
- Development and use of **preapproved smart contract templates** will limit but cannot eliminate this risk.

Legal Issues

- How does the other side **verify** that the smart contract version prepared by a party is the same as the written term sheet or agreement for the transaction?
- Which party is **liable** in the event of coding errors in the contract?

C. Data Protection and Privacy

European Union GDPR right of erasure [to be "forgotten"] and right to correct data:

- How is personal information on the blockchain deleted or corrected if immutable?
- Who is the controller of the data, especially in public permissionless blockchains?
- Where is the data held?

Legal Issues

- How is the data anonymized? Is cryptographically hashing of the data sufficient? Public keys may be personal information covered by GDPR.
- Possibility of opt-outs and opt-ins as part of smart contract.
- Note: European Union Blockchain Observatory & Forum Report: https://www.eublockchainforum.eu/reports

Legal Issues

D. Noncompliance with other Laws

- Virtual organizations [Distributed Autonomous Organizations (DAOs)] formed on the blockchain instead of incorporated under local laws. The entity established and governed through smart contracts.
- DAOs that issue digital tokens in initial coin offerings [ICOs] as a form of equity subject to US federal securities laws.

[https://www.sec.gov/news/press-release/2017-131]

Legal Issues

E. Ambiguities of Human Contracts

- There are basic **inherent challenges** in the process of converting from the written contract to the **self-executing** digital one.
- One is the use of **qualifying terms** used continuously to bridge the gap in human language contracts.

Legal Issues

- For example, written contracts contain provisions requiring **good faith** or **reasonable efforts**, **reasonable notice** or other qualifiers such as **materiality**.
- New logic and **semantics** required objectify and quantify concepts
- Similar to challenges faced in designing and building a fully **autonomous self-driving vehicle.**

Legal Issues

- Use of **AI** and **machine learning** to develop the logic will probably be required.

Legal Issues

F. Irrevocability of Smart Contract Code

- Once the smart contract is embedded into the distributed ledger it is irrevocable and cannot be changed or deleted and will be **self-executing**. This is the equivalent of a **transactional doomsday machine.**
- This can be **corrected** by the parties adopting and embedding a **revised** smart contract to supplement the existing block-chained one **but only if both agree.**

Legal Issues

What happens when there is:

- A **mistake** of law or fact.
- Other **defects** in the underlying written contract or in the smart contract or there is a **dispute as to meaning or performance** and the parties do not agree to correct.
- Unanticipated **future events**, such as bankruptcy of a party.
- **Fraud** in the inducement.

Legal Issues

- Under discussion are the required use of “**kill switches**” in smart contracts that would **prevent self-execution** if:
  - One of the parties files for **bankruptcy**
  - A court of law issues an **injunction** against performance of the contract.
- Without a kill switch or other similar mechanism, how do you **stop** the smart contract from self-executing?

Legal Issues

G. Jurisdictional Issues

- Which is the **controlling** agreement: written or digital?
- Enforceability of smart contracts in **cross-border** transactions when different rules apply in the relevant jurisdictions, including choice of law provisions.
- What is the **location** of the smart contract for jurisdictional purposes?

Legal Issues - The End Times

H. Rise of the [Uniform Contracts] Machines

- The **front end complexity** associated with building out smart contracts will accelerate the drive to adopt **uniform contracts** in industries: to maximize **interoperability** and **scalability** just as with any other **standard technologies** [see: electric plugs; mobile cellular transmissions; DVDs].

Legal Issues

- **Growing convergence** in standardizing commercial contracts such as non-disclosure agreements [NDAs], supply agreements, online terms and conditions.
- **Certain industries are already there**: ISDA [International Swaps and Derivatives Association] standard agreements for certain financial transactions; NVCA [National Venture Capital Association] model legal documents for startups.

Legal Issues

- It is inevitable that **smart contracts** and **decentralized ledger technologies** will accelerate this convergence to uniform contract standards.

#

"The desire for safety stands against every great and noble enterprise.”

— Tacitus, 100 AD

STAFFORD MATTHEWS

Partner, Silicon Valley
Dentons US LLP
1530 Page Mill Road, Suite 200
Palo Alto, California 94304 USA
T +1 650 798 0380
M +1 415 815 9850
stafford.matthews@dentons.com

Dentons is an international legal practice providing client services worldwide through its member firms and affiliates. This publication is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. Please see dentons.com for Legal Notices.