The privacy paradox in blockchain: best practices for data management in crypto

June 9, 2022

Blockchains are touted as next generation databases that promise to facilitate secure and efficient transactions between unknown parties. However, one of the primary pillars of a blockchain's security is the fact that people with access to the blockchain can see the entire history of transactions executed on the blockchain – the result being that each party has an equal opportunity to verify the accuracy of information stored. But if all the information stored on the blockchain can be viewed by anyone with access to the blockchain, what happens when that information qualifies as "personal information" under Canadian privacy laws? Organizations that collect use or disclose "personal information" are subject to a variety of compliance obligations, which as we set out below, can be difficult to reconcile with certain blockchain fundamentals.

What is personal information?

In *Gordon v Canada*, the Federal Court explained that personal information is information that can be used to identify an individual if the information "permits" or "leads" to the possible identification of the individual, whether on the basis of that information alone, or when the information is combined with other information from other available sources.[1] Accordingly, a company that merely "de-identifies" or "pseudonymizes" data may still be subject to Canadian privacy law requirements because there is a possibility that such data can be "re-identified". This poses a unique challenge to the developers of blockchain infrastructure, and the businesses that operate atop blockchain infrastructure, when the metadata that is necessarily ingrained in blockchain transactions may be re-identifiable. Such metadata may constitute personal information when it reveals where transactions are sent from, who they are sent to (not necessarily the name of the recipient, but the address of the recipient), how much money was sent, and at what time.

Take decentralized applications (DApps) for example, which are built from software deployed on the blockchain (e.g., smart contracts) that are typically designed to execute business operations for companies.[2] The operations of the smart contracts that effectively facilitate the functionality of the DApps are often made publicly available to every node in the blockchain network as "bytecode", which can be reverse engineered to reveal the same transactional information as metadata in peer-to-peer transactions.

So, what does it mean if such data, stored and processed on public blockchain networks, qualifies as personal information? The result is somewhat of a paradox.

The blockchain – privacy paradox

Immutability

Records published to a blockchain cannot be deleted, but most modern privacy legislation grant individuals a "right to be forgotten". How can an individual or data subject exercise their right to be forgotten when the information recorded on a blockchain's ledger is permanent?

Transparency

The very basis of trust in decentralized networks results from the transparency of the ledger. All participants in public blockchain networks trust in the sanctity of the information because they can all see and analyze that information equally and in real time. But if all the information is transparent, it becomes accessible to anyone and may, theoretically, be used by unknown actors for unknown purposes. Accordingly, how can an entity that leverages blockchain technology to execute transactions and/or store information provide the appropriate protections for data subjects around how their information may be used or disclosed?

Accountability

Public blockchains are intentionally decentralized so that there is not one accountable entity. Moreover, the networks composed through public blockchains often span jurisdictions, and may consist of hundreds, thousands, or millions of people who all technically have the ability to inform updates to the blockchain (an ability akin to managerial decision making). Under these circumstances, how can a regulator enforce actions against the supporters of a public blockchain, when responsibilities around upkeep, management, and ongoing development are spread across a community of unassociated individuals?

Best practices for managing personal information in the blockchain context

No official recommendations or interpretations of how to process personal data on public or private blockchains have been published in Canada. However, a broad interpretation of personal information, which is customary under Canadian laws, could deter blockchain stakeholders from processing personal data on public blockchains, because data on a blockchain is accessible by anyone with access to that blockchain, and distributed/stored amongst all nodes in the public blockchain network.

In the private blockchain context, management of individual rights over personal information is possible because there are designated and accountable entities that control the number of stakeholders with access to the blockchain. Under such circumstances, stakeholders may require compliance with privacy regulations as a means of accessing the private blockchain and its associated application(s). Stakeholders may also be removed from the network for failures to comply, and a sufficiently centralized private blockchain may be overwritten by participants through collaboration to respond to certain privacy infringing incidents.

The stakeholders behind DApps in either public or private blockchain contexts also have the ability to proactively mitigate privacy law risks by designing appropriate privacy policies and implementing best practices that involve:

- **Combining on-chain and off-chain data**

The blockchain application should avoid storing personal data as a payload on the blockchain (i.e., including identifying information in the message accompanying the payment itself), and instead have blockchain transactions serve as mere pointers or an access control mechanism to more readily managed storage solutions off-chain.

- **Utilizing privacy centric technologies and cryptographic methods**

Encryption techniques currently being used by privacy-centric chains include ZK-SNARKS, Ring Confidential

Transactions, and mixing techniques, all of which are intended to mask the identity of the sender or recipient and/or allow participants to confirm transactional legitimacy by cryptographically proving that they know something without revealing the nature and identity of the information.

- **Conducting data transformations**

Other privacy enhancing encryption and destruction techniques may be used to protect an individual's privacy rights, such as hashing data or applying other data transformation techniques to personal information, and revocation of access rights to a blockchain application (or entire blockchain in a private blockchain network). However, Canadian regulators have not addressed whether such measures are sufficient to meet the demands of Canadian privacy legislation.

Organizations leveraging blockchain technology to collect, use or disclose personal information must take care to remain informed and compliant to requirements under Canadian privacy laws. For more information on how to respond to the privacy law challenges imposed by the technical realities of blockchain technology, contact Chantal Bernier, Noah Walters and Sasha Coutu at Dentons Canada LLP.

---

1. Office of the Privacy Commissioner of Canada, Metadata and Privacy: A Technical and Legal Overview (October 2014) at 6↩
2. Di Filippi, "The Interplay Between Decentralization and Privacy" The Case of Blockchain Technologies" (2016) n. 7 Journal of Peer Production: Alternative Internets 5 (SSRN) at 8. ↩

Your Key Contacts

Noah Walters
Associate, Toronto
D +1 416 361 3418
noah.walters@dentons.com

Sasha Coutu
Associate, Ottawa
D +1 613 288 2708
sasha.coutu@dentons.com