Torkin Manes
Barristers & Solicitors

Torkin Manes LegalPoint

Technology, Privacy & Data Management

April 2022

Blockchain: Opportunities and Legal Considerations

By Roland Hung, Lisa R. Lifshitz and Olivia Veldkamp

Blockchain is a distributed ledger technology that is most widely known for its application with Bitcoin. Despite this claim to fame, blockchain technology has potential far beyond Bitcoin or other crypto-currencies. Some of its most attractive features include high data accuracy and robust security at a relatively low cost. As with any useful technology, it also presents unique legal issues. This article will discuss what blockchain is and highlight the major legal issues it presents.

What is Blockchain?

Blockchain is a distributed ledger upon which transactions are anonymously recorded. The “distributed” aspect means that the same data is recorded across a network of many computers or servers, known as “nodes.” This means that if one node were to record data differently from the others, either through a mistake or a malicious act, the other nodes would easily be able to locate the defective node and correct the ledger. This provides high fidelity of the data. There is no single vulnerable point in which a hacker could target, thus contributing to its robust security.

The “ledger” aspect consists of the eponymous chain of blocks. As transactions occur, they are recorded, time stamped and added to a block. Each block records a limited amount of data and is shared with the network of nodes once it is “full.” Nodes called “miner nodes” compete to solve an arbitrary complex algorithm associated with the block, a step that is designed to prevent bad actors from gaming the system. Once the miner nodes solve the algorithm, the block will have a “Proof of Work” and all nodes in the network must verify it. The block is then added to the chain and becomes immutable. This process creates a linear chain of information that has been verified for accuracy and is very difficult to alter.

Legal Considerations of Blockchain

There are many legal considerations when using blockchain, but this article will only highlight three major considerations: (i) jurisdiction; (ii) privacy; and (iii) intellectual property.

1. Jurisdiction

The decentralized nature of the nodes muddies the water for the legal jurisdiction applicable to the blockchain transaction. Nodes can be located anywhere in the world. Theoretically, a given transaction could be governed by the applicable law in any jurisdiction where there is a node. Legal regimes across the world vary greatly and it may be difficult (and in some cases impossible) for a blockchain to comply with the applicable laws in every jurisdiction in which it has a node.

It is, therefore, essential that contracting parties include an exclusive governing law and jurisdiction clause when using a blockchain solution. Failure to do so may result in costly and redundant litigation across jurisdictions in the event of a dispute.

2. Privacy

One of the defining characteristics of blockchain is transparency. This can be a benefit where the user has an interest in promoting trust and believes transparency will further that goal.

Unsurprisingly, the downside is that such transparency comes with privacy concerns. This is of special note where the blockchain stores personal information or enough metadata for an observer to infer personal information. Industries such as banking and healthcare handle particularly sensitive data, which often must be kept secure and confidential by law. Blockchain users should, therefore, consider how privacy and transparency are balanced in their unique situation.

One way to manage this balance is to consider using a Permissioned Blockchain rather than a Permissionless Blockchain. In a Permissionless Blockchain, any user can become a node using a pseudonym without having to reveal identifying information. In a Permissioned Blockchain, only a restricted group can become nodes and their actual identities are known to the other users. Permissioned Blockchains include Private Blockchains (also known as “Managed Blockchains”), in which there is a central authority that can act as a gatekeeper for nodes.

Generally, a Permissionless Blockchain will have better security due to the increased number of nodes making it difficult for malicious actors to alter data. However, a Private Blockchain can provide better privacy since it restricts those who can join the network. Users can also consider using a Consortium Blockchain, which is a Permissioned Blockchain governed by a group of entities rather than a single entity. A Consortium Blockchain offers a more balanced trade-off.

Finally, businesses can improve privacy by encrypting the data on the blockchain.

3. Intellectual Property

Blockchain can be a valuable asset in terms of the software and business processes themselves, and with respect to the underlying data set. Businesses may wish to consider how they can protect this value. Depending on the case, it may be possible to patent a blockchain in certain jurisdictions if there are otherwise patentable elements combined with the computerized element (See *Amazon.com Inc., Re*, 2011 CAF 328). Businesses that invest in blockchain development will have to consider whether it would achieve greater benefits to protect intellectual property rights in their software or opt for a more “open innovation” approach.

Blockchain vendors should also consider the extent to which they can capitalize on the value of the data set. This can be negotiated by contract with customers and will depend heavily on the given situation. For example, a customer may negotiate more aggressively if they feel they will gain a competitive edge through maintaining intellectual property rights to the data. They may prefer to license the data for the term of the agreement rather than allow the vendor to maintain rights indefinitely.

Conclusion and Recommendations

The use of blockchain has high potential. Businesses that wish to do so should consider the applicable jurisdiction and use clear, exclusive governing law and jurisdiction clauses to promote legal certainty. They should also encrypt their data and consider whether a Private or Consortium Blockchain might be

appropriate to provide greater data privacy. Finally, they should carefully consider whether the software can (or should) be patented and what intellectual property rights they may wish to maintain over the underlying data.

For more information about legal considerations around blockchain, please contact a member of Torkin Manes' Technology, Privacy & Data Management Group.

Authors

Roland Hung
Counsel

Tel: 780 914 1786
rhung@torkinmanes.com

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com

Olivia Veldkamp
Student-Articling

Tel: 416 863 1220 Ext. 243
oveldkamp@torkinmanes.com