BUDDLEFINDLAY

Blockchain, what is it and why does it matter?

Simon Jensen

31 May 2017

Blockchain is a hot topic at present. We've been writing about it for a while now and appreciate that it can be a hard topic to get your head around. In this article we set out to provide a brief summary of what blockchain is, what some of the issues are and why it is such a big deal. Sections of this article are taken from a more detailed paper written by Buddle Findlay partner Simon Jensen for the New Zealand Law Society's Cyber Law conference held in April 2017. The paper is available from the Law Society.

What is it?

A blockchain is a digital ledger, shared across multiple people or organisations (nodes) in a distributed network. The nodes in the network work to verify the authenticity of transactions undertaken on the network and if a consensus amongst those nodes is reached, the transaction will be validated. In many blockchains, each node in the network has a copy of the block-by-block transaction record.

A blockchain can be used to record data, often but not exclusively financial transactions, in a way that is:

- Immutable - it cannot be hacked or altered in retrospect if the network has sufficient scale because the hacker would need to control 51% of the nodes
- Reliable - it is resistant to failure of an individual or groups of nodes on the system because the chain of transactions are generally stored on every single node
- Distributed - it does not require a central authority to oversee and regulate transactions as the blockchain is governed by its protocol, which will often be open source.

The sum of these attributes, and in particular the distributed nature of the technology, mean that blockchains can be relied on to carry out functions that have in the past had to be carried out by trusted intermediaries such as stock exchanges, clearing houses and lawyers. This could potentially have significant cost and time benefits for a wide variety of transactions people undertake all the time.

Blockchains can be 'permissionless' or 'permissioned'. A 'permissionless' blockchain is one that is open and anyone can join. A 'permissioned' blockchain is one where only certain organisations or individuals are allowed to join. This meansa broader set of regulations can be enforced between those organisations or individuals, and the rules of the network itself can be more easily agreed upon and updated.

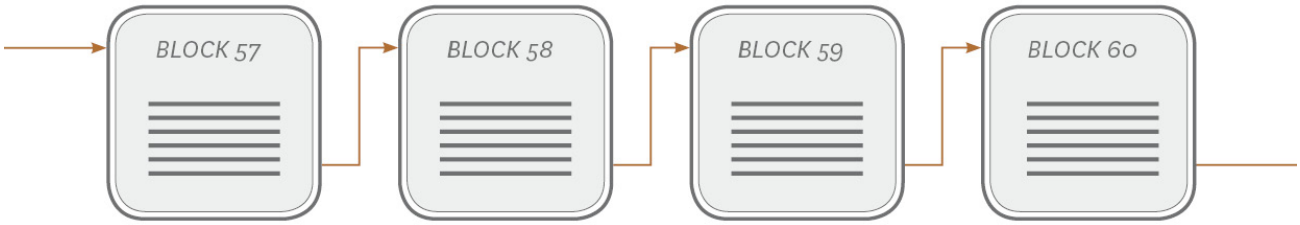
Some of the key attributes of blockchain technology, such as its distributed nature, participant anonymity and immutability, give rise to a number of regulatory issues with blockchain technology in New Zealand, such as:

- **Anti-money laundering**: New Zealand's anti-money laundering legislation is about identifying an entity that is undertaking certain financial activities and imposing obligations on them. With a permissionless blockchain, it will likely be difficult to identify any entity that offers these financial activities to customers (as most transactions will be occurring bilaterally on the participants' own behalf). Without such an entity, there will be no obligations to conduct customer due diligence or suspicious transaction reporting, and a number of transactions that would traditionally fall within the scope of the anti-money laundering legislation will be excluded from monitoring
- **Insolvency**: The nature of the transactions on blockchains like Bitcoin (which we describe below) is that they cannot be undone. They are 'immutable'. Where an asset is transferred on a blockchain it may be difficult (even with a court order) to get property returned. While parties to a transaction may be able to submit an unwind of that transaction on to the blockchain, that will be problematic if the property has subsequently been dealt with and other parties are required to effect the unwind. It may be very hard to unwind blockchain transactions where current insolvency rules relating to voidable transactions might otherwise require it.

Bitcoin

The original and most famous example of a blockchain is the cryptocurrency Bitcoin, which was created in 2009 by an unknown developer using the pseudonym “Satoshi Nakamoto”.

On the Bitcoin blockchain anyone can create a transaction. For the transaction to be valid it must contain the cryptographic signature of the account from which bitcoin is being sent - effectively the account password. Transactions are then broadcast to the entire network, where Bitcoin 'miners' compete to create new blocks of valid transactions, with a new block created every ten minutes on average. Creating a new block also creates a number of new Bitcoins (currently 12.5 bitcoins per block) which are paid to the miners along with any transaction fees paid by participants. Each new block contains a link to the previous block, preventing earlier blocks from being removed or tampered with.



Bitcoin is an example of a 'permissionless' blockchain, where anyone can download the software and join. Further, as Bitcoin transaction data is not encrypted and anyone on the network can view the details of a transaction, Bitcoin is an open and non-private blockchain. If a Bitcoin user wants to keep his or her transaction details private, they may do so by remaining anonymous (which has caused issues with anti-money laundering regulators around the world).

Smart contracts

There are a range of opinions about what a smart contract is exactly, but the better term for smart contract applications using blockchain technology is probably 'self-executing contracts'. Most commentators seem to agree that smart contracts involve:

- Programs that define a set of rules such as "if A happens, then do B"
  - those rules (and the execution of those rules) are stored and replicated on a blockchain
  - the rules facilitate the automated performance of a set of contractual obligations without the need for human interventions
- The blockchain being updated as the obligations are performed (e.g. to show payment or the transfer of assets).

It's easy to see that if aspects of contracts (in particular relating to their execution) could be automated using a blockchain there could be significant advantages, including:

- Decreased transaction costs
- Cutting out the middlemen (e.g. banks, escrow agents and brokers)
- Increased security - these systems may arguably be harder to cheat as multiple computers are involved in maintaining the blockchain and transactions can be set up to require the use of multi-signature addresses.

However, some practical issues which are barriers to the general acceptance of smart contracts are:

- **Coding Contracts**: Most smart contracts are short, only involve around 500 lines of code and tend to rely on very binary triggers. It may be difficult to convey a complex contractual arrangement in brief terms and where triggers are defined by non-binary measures such as reasonableness. Further, the programming language 'Solidity' (which is the language used by the Ethereum platform, the most common blockchain protocol used for smart contracts) is arguably a difficult coding language, which some commentators have suggested means that there are greater opportunities for the contract to have bugs or not be coded as intended
- **Smart Contract Payments**: Without the widespread acceptance of some form of cryptocurrency (or a digital version of a fiat currency), smart contracts in New Zealand will be reliant on contractual payments being made through traditional banking channels. Until a connection into the traditional banking channels can be achieved, smart contracts will not be truly automated (New Zealand banks do not currently have open APIs).

There are also a number of enforcement challenges which may affect the uptake of smart contracts, including:

- **Resolving Disputes**: Disputes could emerge because a party refuses to recognise the validity of a smart contract or argues that the automated system has worked incorrectly or was incorrectly programmed. The forum for resolving disputes may be unclear, especially for smart contracts on a permissionless blockchain (like Ethereum) where the blockchain operates across borders and may have no clear governing law. Even where a governing law is clear, the contract is 'in the code' and courts are likely to need assistance to interpret the code and what was meant by it.

- **Redress and Immutability**: If there has been duress, a contract is with a minor or a contract is for some reason illegal or in breach of regulatory requirements and redress can be obtained against the other party, traditional remedies may not be available because it simply may not be possible to unwind the transaction (again a problem that is likely to be a much bigger issue in permissionless blockchains where 51% of the nodes would have to agree to unwind a transaction and those nodes may be in different jurisdictions).
- **Causation and Liability**: With a distributed ledger system, it could be difficult to work out where a problem happened and who caused it given that all of the computers across the distributed ledger have essentially given effect to the transaction. As such, case law on causation and contribution may be difficult to apply (assuming you could even find the parties to bring an action against).

What could blockchains do?

Despite the fact that there are a number of tricky legal issues that will need to be resolved, billions of dollars have recently been invested into (mainly permissioned) blockchain networks to develop meaningful commercial applications.

The financial sector seems to be the most exposed to disruption from blockchain technology due to the number of services that are offered that are trust-based intermediary services. Applications currently being tested relate to:

- Securities trading - for example, the ASX is likely to replace its equity clearing and settling system with a distributed ledger solution soon
- Cross border remittances - cryptocurrency solutions to remittances are being explored to decrease costs by avoiding sending remittances via the comparatively expensive SWIFT network
- Trade finance - where solutions are being explored that use GPS tracking and self-executing smart contracts to release goods and documents at ports
- Escrow arrangements - where solutions to streamline software escrow arrangements that reduce the amount of human intervention required are being explored
- Insurance - for example, entrepreneurs are experimenting with blockchains to facilitate peer to peer insurance and insurance companies are testing how a blockchain solution could be used to simplify the claims process when a major event like an earthquake occurs
- Derivatives - for example, Barclays in the UK has developed a blockchain based platform for ISDA agreements.

Applications of blockchain technology outside of financial services have also been considered for:

- Healthcare - for example, developers in the US are experimenting with blockchain technology to create a record of which medical institutions are holding a patient's data
- Property - for example, Sweden and a number of other countries have started projects to develop blockchain based land registries
- Energy - with the proliferation self-generated electricity through solar and wind, blockchain applications have been explored to facilitate the peer to peer sale of excess self-generated power to neighbours.

We expect to see more and more novel applications of blockchain technology which have the potential to revolutionise the way a number of industries and markets work.

Auckland

PwC Tower
188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659