Blockchain and Smart Contracts: The dawn of the Internet of Finance?

By Henry Davis York partner Matthew McMillan and lawyer Ken Wong

The 'blockchain phenomenon' opens up a myriad of opportunities for the financial services industry (including the evolution of smart contracts) but alongside the enormous potential a number of key legal considerations are emerging.

What makes blockchain truly disruptive, however, is not just the distributed nature of the ledger system but the ability to combine that with capabilities which go well beyond the traditional paper-based ledger. In particular, the ability to implement business rules into the blockchain or to enable smart contracts

Much has been spoken about of the 'trust asset' in recent times by participants in the financial services industry - in particular, the need to preserve and enhance customer trust in an organisation's brand to defend against displacement by digital disrupters.

This 'trust asset' is critical for trade to occur. It is the reason that third party banking institutions are often entrusted to facilitate payments and approve transactions.

But what if trust was enabled by technology itself, rather than an organisation's reputation or brand?

Blockchain aims to do just this. It facilitates transactions of value where trust is critical. And it does this by enabling transactions of value to occur over computer networks that can be verified, monitored and enforced without the need for trusted intermediaries.

WHAT IS BLOCKCHAIN?

Blockchain is the technology underlying bitcoin, which is a self-regulated cryptocurrency network operating without a central bank.

Blockchain operates as a distributed ledger system - essentially an asset database that can be shared across a network of multiple users in any location. Each user owns a full copy of the ledger, and plays an important role in automatically and continuously agreeing on the current state of the ledger and all of the transactions recorded in it.

The ledger is maintained through the use of cryptographic 'keys' which control who can do what, within the ledger. It is the data transparency between all users in the network, and underlying cryptography, that removes the need for a trusted intermediary.

Some of the key features of blockchain include:

- **Security and reliability:** The blockchain is a cryptographic technology that is highly resilient to attack. To attack the blockchain, an attacker would need to simultaneously compromise each user's copy of the distributed ledger. An attack on one copy (or network node) does not impact upon the availability and reliability of the information on the distributed ledger.
- **Single source of truth:** All transactions on the blockchain are visible to all users within the network, and each user plays a role in authenticating transactions on the distributed ledger, thereby removing the need for trusted intermediaries. This transparency renders it near impossible for changes to go undetected, and enhances trust and confidence in the information stored on the ledger.
- **Digital:** The blockchain allows for any asset - be it financial, legal, physical or electronic - to be expressed in code and recorded on the ledger. And because the blockchain is programmable, it can facilitate an enormous range of transactions involving those digital assets - many of which are only now being conceived.

These features open up huge opportunities for the financial services industry. This includes the ability to disintermediate trusted third parties from a wide array of transaction types. In the case of the bitcoin cryptocurrency, it is the removal of a central bank.

Rather ironically, however, it is the traditional participants in the financial services industry – the very ones which the bitcoin currency is designed to circumvent – that are increasingly investing in the underlying blockchain technology and converting what was once perceived as a threat into new opportunities to re-engineer back-end systems, increase settlement speeds and drastically drive down costs.

According to a 2015 report - by Spanish bank, Santander, management consultancy, Oliver Wyman, and venture capital investor, Anthemis - blockchain technology could cut banks' infrastructure costs for cross-border payments, securities trading and regulatory compliance by US$15bn-US$20bn a year from 2020.

BLOCKCHAIN TYPES

Broadly, there are two types of distributed ledger systems:

- **Permissionless systems**: such as the one on which bitcoin is based, where the blockchain is open to the public and the digital ledger is shared, transparent and operated by all of the users in the network.
- **Permissioned systems:** where the blockchain is controlled and administered by one or more entities and direct access to the network is limited to pre-defined users with known identities. There may be multiple layers of access to the permissioned blockchain including, for example, reading transactions, proposing new transactions and creating new blocks of transactions and adding them to the blockchain.

It is the latter which are increasingly gaining traction within the financial services industry. This is partly because of the anonymous nature of users in permissionless systems and the volatility and illicit activity that has plagued the bitcoin system.

Permissioned systems, on the other hand, more closely resemble today's financial systems and, for that reason, can more easily integrate into the mainstream economy and existing regulatory frameworks.

INVESTMENT LEVELS ARE UP

The level of investment being directed into blockchain technology by financial services organisations cannot be underestimated.

Recent examples include:

- The formation of the R3 consortium of 42 global banks to define protocols and build a platform to standardise the use of blockchain technology across relevant parts of the banking industry;
- Commonwealth Bank of Australia partnering with Ripple to facilitate blockchain-enabled payments between subsidiaries;
- Westpac's venture capital fund, Reinventure Group's, investment into Coinbase;
- Citigroup's creation of a new digital currency known as Citicoin;
- UBS' investigations into blockchain-enabled bond trading and the creation of its own digital currency in collaboration with the start-up community; and
- The ASX partnering within Digital Asset Holding to build a blockchain to run in parallel to - and, perhaps, even replace - the existing CHESS system.

BEYOND BLOCKCHAIN: THE EVOLUTION OF SMART CONTRACTS

What makes blockchain truly disruptive, however, is not just the distributed nature of the ledger system but the ability to combine that with capabilities which go well beyond the traditional paper-based ledger. In particular, the ability to implement business rules into the blockchain or to enable smart contracts.

It is at this application level (i.e. applications on top of the blockchain) that the real potential of the technology lies.

Smart contracts are self-executing contracts which are written in computer code and programmed into the blockchain. They are essentially computer protocols that facilitate, verify, execute and enforce the terms of a contract. This removes the need for human intervention as far as monitoring compliance and enforcement of the contract are concerned.

A smart contract could, for example, have code written to only allow a transaction (such as a trade) to execute at a certain time or upon the fulfilment of certain conditions. Or code which automatically deactivates the digital keys of a leased car, and prevents the car from being operated, upon a lease payment being missed. Or it could even be a set of programmed computer protocols which automate the execution of steps required to effect a real estate property settlement and enable the transfer of title.

The self-monitoring and self-enforcing nature of smart contracts has huge appeal in that it enables two parties to contract at arms' length, without the usual counterparty risk and without incurring the costs of administering and enforcing the contract.

LEGAL CONSIDERATIONS

Whilst the potential uses, benefits and risks of smart contracts are only starting to be emerge, they do give rise to some interesting and challenging legal issues. These include:

- **Formation of contracts.** To be an enforceable contract at law, the elements of contract formation will still need to be satisfied; that is, there needs to be an offer, acceptance of the offer, consideration and an intention to enter into the contract. This is not to say, however, that a smart contract is not capable of being a contract at law.
- **Interpretation and uncertainty.** Smart contracts are written in computer code, readable only by a computer system. How do the parties to the contract, a judge or a regulator interpret the terms of the smart contract?
- **Bugs and errors.** Computer code, by its nature, will often contain some form of defect. What are the potential consequences on the rights and obligations of the parties if there is a defect in the code which causes an error in the execution of the contract?
- **Ability to unwind contracts.** How does the self-executing nature of smart contracts sit with a party's rights at common law to void a contract under legal doctrines such as mistake or unconscionable conduct? Can a transaction on the block-

chain be unwound? How would this be achieved? And what would be the downstream impact for other transactions on the blockchain?

- **Confidentiality and security.** Distributed ledger systems, and smart contracts, result in massive repositories of data. To what extent is this information capable of unauthorised access or interception? Whilst cryptographic code may be difficult to break, it may nevertheless be bypassed - either through the inadvertent disclosure of cryptographic keys or 'back doors' in the software code.
- **Privacy.** An essential feature of distributed ledger systems is the public nature of the data and the ability for transactions, including smart contracts, to be publicly viewable in the ledger. This raises privacy concerns, particularly where transactions involving individuals are able to be tracked and analysed.
- **Systemic risk.** If each copy of the ledger is simultaneously attacked, or there is a distributed denial of service attack brought about by the network being overwhelmed with service requests, this could have dire consequences for the financial service industry at large. Whilst centralised ledger systems can act as shock absorbers, decentralised ledger systems cannot.
- **Jurisdiction.** Smart contracts operating in a distributed ledger system consist of a network of users from various locations. They are not specific to any one location. In the absence of an express stipulation of the governing jurisdiction in the smart contract, which jurisdiction would govern the smart contract?
- **Adjudication.** The self-executing nature of smart contracts may remove the need for legal enforcement actions. However, they don't necessarily remove the need for adjudication on other issues, such as liability arising from the execution of the contract or the need to resolve disputes.
- **Evidentiary matters.** As smart contracts will be subject to examination, there will be a need for new types of cryptography experts and forensics experts to verify software code and to translate the code into human-readable form.
- **Regulatory settings.** Smart contracts are enabling financial services to be provided in ways which disintermediate banks and other trusted intermediaries. This may not sit easily with existing regulatory and policy settings, which will need to be considered in greater detail as the technology and its applications evolve. How are regulators to police smart contracts? And what opportunities exist for parties to use blockchain-enabled smart contracts to potentially side-step the law by hiding the identity of the parties and the governing jurisdiction of the contract? How are cross-jurisdictional issues of taxation, national security and anti-money laundering to be managed?
- **Regulatory compliance.** On the flip side, smart contracts enabled by blockchain can be used to enhance transparency and auditability and facilitate better regulatory compliance. A market exchange, for example, could write rules into a smart contract requiring the rules to be met before the contract can be executed by market participants. For regulators, regulatory goals could be achieved through a mix of both laws and technical code.
- **Governance.** The nature of permissioned distributed ledger systems, and the use of smart contracts, means that there is still a need for rules and structures to be put in place for network users to adhere to. This can be challenging in a distributed network environment.
- **Decentralised organisations**. More complex smart contracts may lead to the creation of decentralised organisations, where rights are distributed and managed by the blockchain itself and ultimate responsibility may be difficult to pinpoint. Where does accountability lie? Is it the users of the distributed ledger system, the code creators or the system itself? And to what extent can existing corporations law concepts and frameworks be applied to decentralised organisations?

These issues warrant further detailed consideration as blockchain technology and the use of smart contracts evolve.

Care must also be taken to ensure that any future regulation of the technology maintains the integrity and security of the financial system without compromising the very real potential of the technology to transform the industry. This requires regulators to have a rich understanding of the technology itself, to tread softly and to exercise restraint so as not to stifle the opportunities it presents.

SAVE THE DATE

Wednesday 19 October 2016

CAMLA YOUNG LAWYERS SPEED MENTORING EVENING

See Page 39 for more details