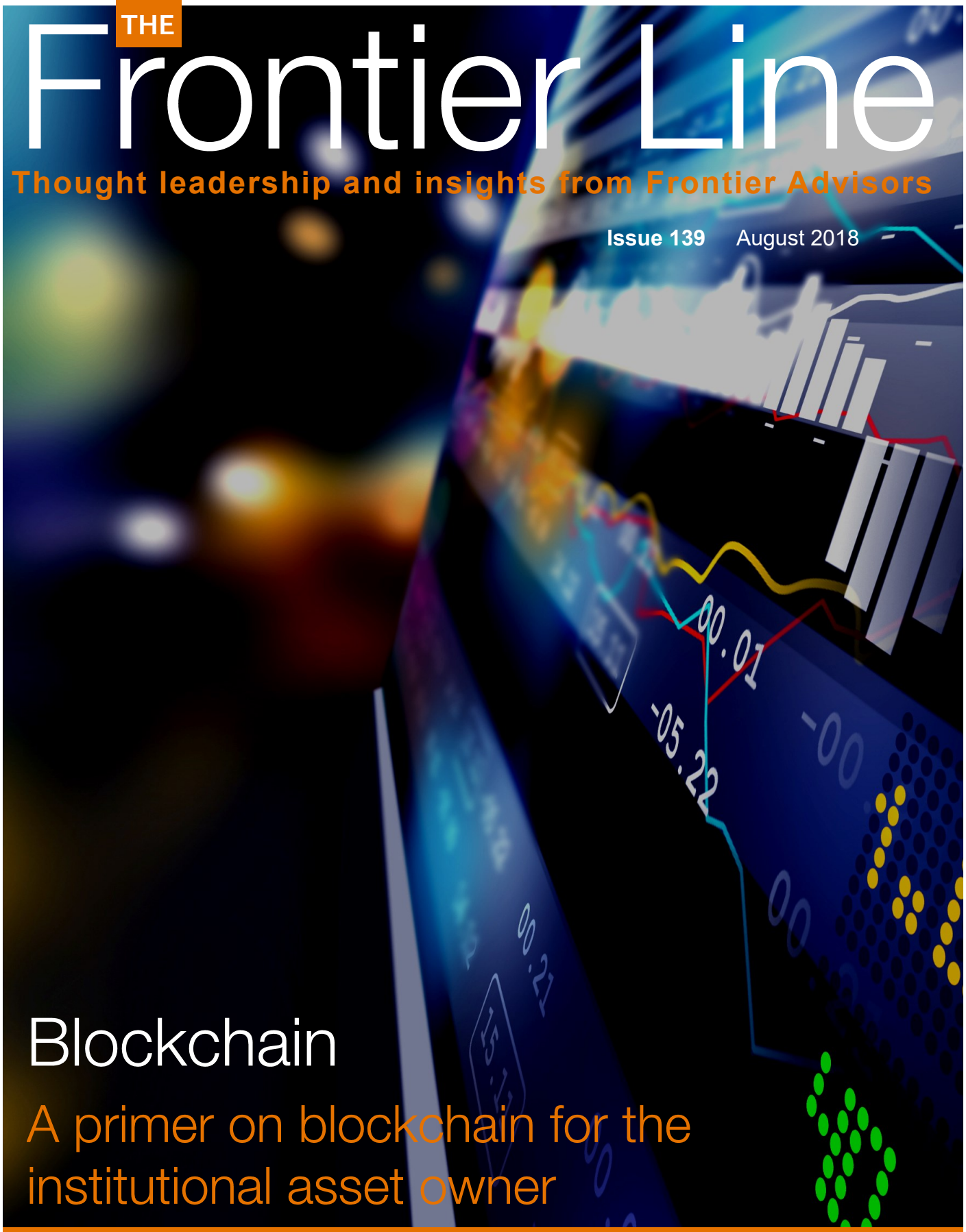
THE Frontier Line

Thought leadership and insights from Frontier Advisors

Issue 139 August 2018



Blockchain

A primer on blockchain for the institutional asset owner

FRONTIER ADVISORS

Frontier Advisors

Frontier Advisors has been at the forefront of institutional investment advice in Australia for over two decades and provides advice over more than $320B in assets across the superannuation, charity, public sector and higher education sectors.

Frontier's purpose is to enable our clients to generate superior investment and business outcomes through knowledge sharing, customisation, client empowering technology and an alignment and focus unconstrained by product or manager conflict.

AUTHOR

Melinda He

Consultant

Melinda joined Frontier as an Associate in 2014, before being promoted to Consultant, and provides investment research and consulting advice to a number of clients. Melinda also undertakes manager research with a focus on both domestic and international equities. Prior to joining Frontier, Melinda was a Consultant in Financial Services Taxation at Ernst & Young, where she was responsible for assisting superannuation funds and general corporate entities with tax compliance and tax advice. Previously, Melinda worked at Credit Suisse in Equities Research and on the trading desk. Melinda graduated from Monash University with a Bachelor of Commerce/Law with Honours, majoring in Finance. Melinda has recently passed the CFA level 3 exam.

Blockchain – a primer

As part of Frontier's annual Look Forward, one of the topics identified as an area of interest was blockchain.

Whilst blockchain has received increased attention in the last two years due to the meteoric rise (and the continued volatility) of cryptocurrency prices, the technology is in fact not new. The first blockchain was launched by Satoshi Nakamoto in 2009.

In recent years, the application of blockchain has moved beyond the trading of various cryptocurrencies and into commercial, government and even social enterprise sectors.

This paper serves as a primer on blockchain technology, outlining its advantages and potential areas of disruption in institutional finance, as well as the hurdles to widescale adoption in the financial services industry.

Examples of the application of private blockchains are also explored. This edition of The Frontier Line is deliberately pitched at an introductory level —providing an overview of the technology and its applications and potential investment implications.

Difference between bitcoin and blockchain

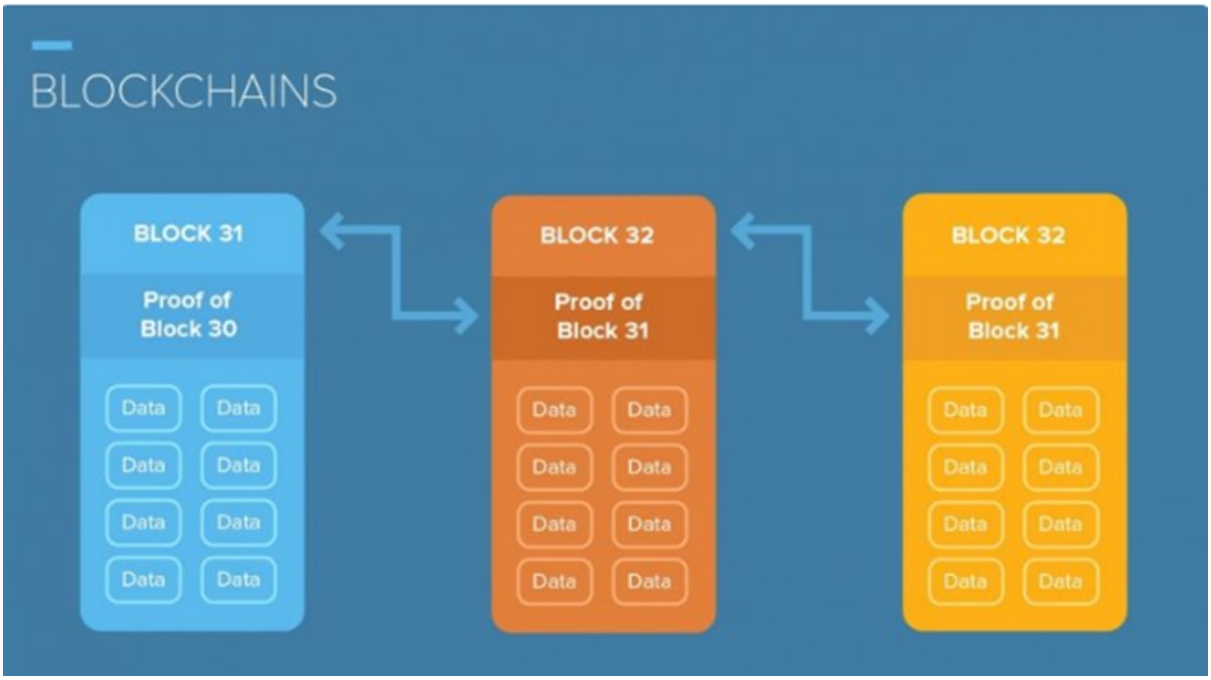
A common confusion is around the difference between bitcoin and blockchain. Blockchain is the technology that underpins bitcoin, and bitcoin was the first successful application of a blockchain.

Blockchain is also the underlying technology of other cryptocurrencies (such as etherum, litecoin and ripple), but with technical variations in the encryption process.

Blockchain has commercial applications outside the cryptocurrency realm, and this will be the focus of this primer.

Satoshi released his white paper on bitcoin in October 2008, and released the first blockchain network and the first units of the bitcoin cryptocurrency in January 2009.

What is blockchain? How does it work?



Source: Factcom University

Blockchain is essentially a type of database storage system which records data in a series of blocks, with each one attached to the previous in an ever growing chain.

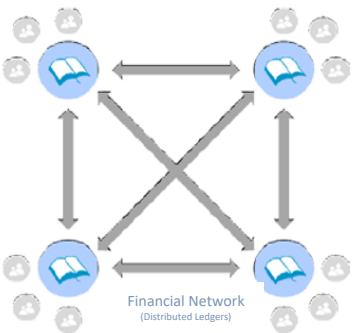
In order for transactions to be validated and a "block" to be recorded, they must undergo an encryption protocol whereby all participants agree that the transaction is true.

The idea that transactions need to be verified by all participants, instead of a central organisation, is what makes blockchain more secure. This is called Distributed Ledger Technology (DLT). Figure 1 shows a traditional database storage system, where data is maintained by a central organisation in a single place.

Figure 2 shows DLT, where data is maintained in a decentralised framework across many locations. The participants verifying these transactions are termed "nodes" (basically computer servers).

Figure 1: Traditional financial intermediaries model

Figure 2: Blockchain model



Source: Source: Citi Research

The encryption protocol for blockchain is done through a process called "Proof of Work" (PoW), whereby computers solve complex puzzles (also known as "mining", hence the expression "mining for bitcoins"). This process of mining for bitcoin requires vast amounts of computational power.

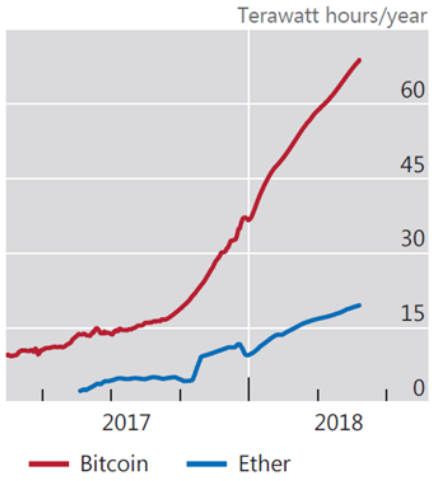
Chart 1 shows the estimated energy usage of two major cryptocurrencies, bitcoin and ether (recall that cyrpotcurrencies are an application of decentralised blockchain networks).

To put this in context, AGL Loy Yang, which produces approximately 30% of Victoria's power requirements every year, produces around 19 terawatt hours per year.

Different methods of encryption protocols (or mechanisms of validating transactions) can lead to requiring less computational power.

For example, under Proof of Stake (PoS), a transaction can be validated where one can prove a certain ownership, instead of all participants verifying a transaction (PoW, as utilised by Bitcoin). In Chart 1, one factor leading to Ether's lower energy consumption is that it switched its encryption protocol, from PoW to PoS in 2018.

Chart 1: Energy usage of select cryptocurrencies



Source: BIS Annual Economic Report 2018.

[1]Bitcoin uses the "gold standard" encryption protocols, called Proof of Work. Other encryption protocols have since been developed, such as Proof of Stake (PoS). Under the PoS method, instead of all participants verifying a transaction, a transaction can be validated where you prove a certain ownership. The advantage of PoS over PoW is that it requires much less computing power, however there is conjecture amongst the Blockchain community whether this is as secure.

What are the benefits?

The key benefits of blockchain over traditional centralised data storage systems are as follows.

Disintermediation gains

Through the process of cutting out the role of multiple intermediaries, blockchain has the potential to facilitate increased speed and reduced costs. The inherent technology is not fast itself, *but the process of disintermediation results in notable efficiencies.*

Figure 3 shows the disintermediation role that blockchain could potentially play in an interbank clearance process, clearly facilitating faster settlements.

There are reports in the media of "blockchains" being hacked, but these have tended to be related to cryptocurrencies and the distinction needs to be made between blockchain itself and the interface that sits on top of the blockchain, such as cryptocurrency wallets or cryptocurrency exchanges.

Exchanges are needed to convert cryptocurrencies (recorded by the blockchain) into fiat currency (e.g. AUD, USD). Interfaces such as cryptocurrency wallets and cryptocurrency exchanges are the most common areas where we have seen infamous hackings, but the hackings are not on the underlying blockchain itself.

For example, a hacking occurred at Mt Gox in 2013, an unregulated bitcoin exchange, where 850,000 bitcoins (amounting to around $480 million at the time) were stolen from cryptocurrency wallets. This resulted in Mt Gox filing for bankruptcy in 2014.

Immutability

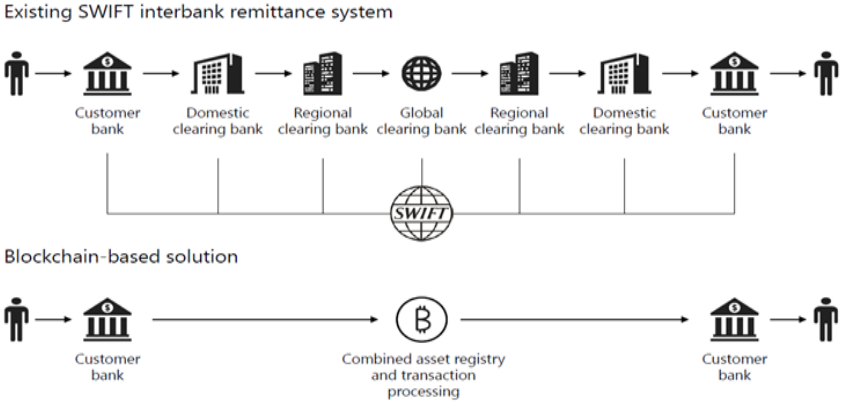
Once stored, transactions are unhackable. Nevertheless, theoretically if a user were to gain access to over 51% of the blockchain or have vastly higher "hashing" (that is, computational power), the hacker would be able to mine blocks faster than the rest of the network, and thus falsify transactions. To date, this has not yet occurred, but there have been blockchain "forks", where due to disagreement between participants, a new blockchain is intentionally created.

Programmability

Smart contracts can be programmed to take place on top of the blockchain transaction. This means that blockchain can be programmed to automatically execute transactions when certain conditions are met.

Although blockchain has attractive features, it is not the solution to every database storage problem. There are numerous database storage systems already in existence which may be more effective, particularly when weighing up the costs of designing a new system alongside an existing proven legacy system.

Figure 3: Traditional interbank clearance vs blockchain



Source: Source: Deloitte

Applications in finance

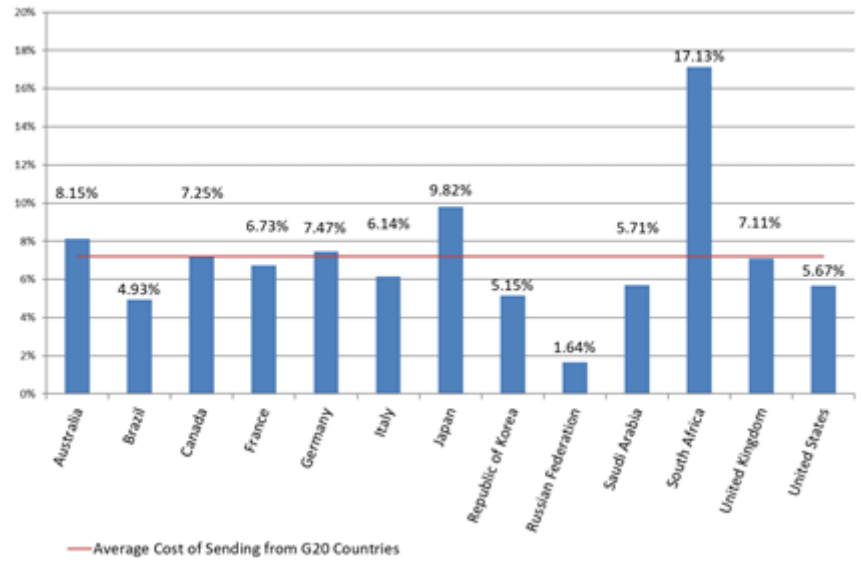
Some of the areas in the finance industry where blockchain is being applied or may be utilised in the future are as follows.

Payments

The global average cost for sending remittances was 5.2% on a weighted basis in Q1 2018. Chart 2 shows the costs of remittance of major G20 currencies in Q1 2018. Blockchain has the potential to offer faster and lower cost payments processing through savings via interbank settlements. Bitpesa, a remittance company that uses blockchain technology, facilitates payments in South African currencies, where the cost of remittance is the highest.

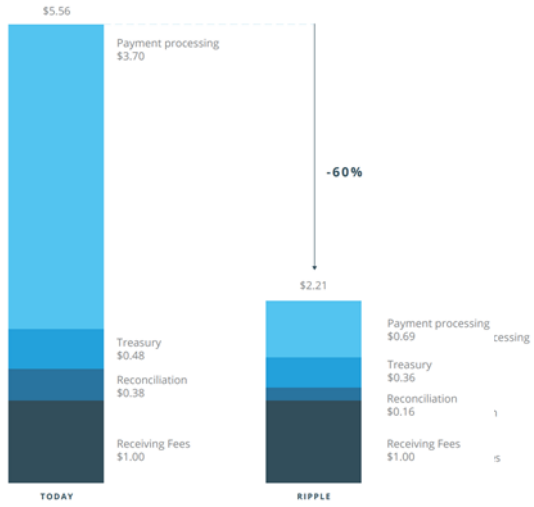
According to Bitpesa CEO, *"we lowered the cost of international payments by 75% and reduced the time to settle between currencies from 12 days to less than 2 hours".* Ripple, a currency exchange and remittance company which operates its own digital currency, also offers global payments processing, with a purported 60% reduction in cost of remittance .

Chart 2: Average cost of remittance from G20 countries



Source: World Bank

Chart 3: Traditional cost per payment vs estimated cost under ripple



Source: Ripple: Ripple Solutions Guide

Clearance and settlements

Through the disintermediation process of mid and back office functions, blockchain has the potential to fundamentally change the mid and back office settlement checks and clearances process. This could result in shortened settlement times and cost efficiencies via reduced compliance functions (as illustrated in Figure 3).

Registry and custody functions

For the same disintermediation reasons, blockchain has the potential to bypass traditional intermediary functions such as share registry and custody functions (refer to Figure 3).

Tokenisation of real assets

Whilst investors can access portions of property through REITs, asset tokenisation could expand fractional asset ownership into residential real assets or other illiquid assets such as art, antiques, vineyards etc. This expands the opportunity set for investors as it provides for more diversification of risk through owning fractions of new asset classes.

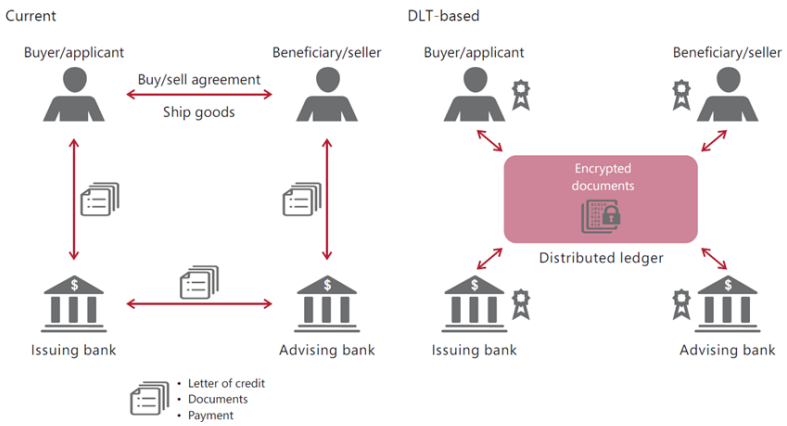
Smart contracts: real estate and trade finance

Smart contracts could be programmed to facilitate transactions in many industries. For example in real estate, the process of releasing funds from escrow, settlement, transferring title and confirming ownership could all be simplified via an automated program. This reduces human error risk, and could be particularly useful for countries without a robust land titles system.

In trade finance, smart contracts can be programmed to automatically release payment to the exporter upon the receipt of documentation of shipment (known as a "bill of lading"). Under the current system, a bank in the importer's home country issues a letter of credit guaranteeing payment to the exporter upon receipt of a bill of lading. A bank in the exporter's country may extend credit to the exporter against the guarantee and collect payment from the importer's bank to complete the transaction. Through an automated smart contract, blockchain could streamline the process of exchanging documents and releasing payment.

HSBC announced in May this year that it and Dutch bank ING had successfully completed a trade finance transaction for food and agricultural group Cargill using R3's Corda blockchain platform. CBA also reported having successfully conducted a trial in 2016 with the R3 Consortia.

Figure 4: Blockchain in trade finance



Source: BIS Annual Economic Report

Hurdles to Blockchain being a "disruptive" force

Whilst blockchain technology comes with many positive attributes – disintermediation gains, immutability and programmability, there are still several significant hurdles before it can "disrupt" the financial services sector and replace mainstream global custody services or clearinghouses. The key hurdles are as follows.

Cost

The initial investment required to develop a blockchain that is scalable and secure is hefty relative to established databases. Whilst blockhain may generate considerable cost savings, it is not necessarily the answer for all businesses especially where there are already proven technologies. Bitpesa and ripple were outlined above as examples of disruption in the global payments space. Bitpesa, for example, has taken off in countries where the existing infrastructure is not as developed or secure. In developed countries, or even other emerging countries, there already exist low cost payments systems that are relatively fast.

Legal and regulatory approval

In order for widespread adoption, the system must garner support from regulators. For example, with the tokenisation of real assets, regulations that govern how investors gain access and address issues of enforceability of property rights are needed.

Interoperability

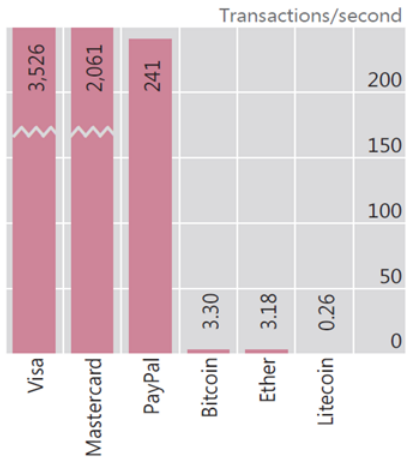
A global payments system or clearinghouse based on a blockchain network requires the participation and co-operation of multiple banks. There are some examples of banks working together, for example a consortium of banks called R3 was formed in 2014 to develop a blockchain platform, but results have been limited to date.

Scalability and speed

Blockchain requires significant computational power to verify and confirm each block of transactions, and still lacks the efficiency to be scaled for large scale operations. To date, cryptocurrency transactions underpinned by blockchain have not achieved the same level of speed as traditional payments systems (Chart 4 below).

Note that the transactions per second chart is based on 2017 data, and since then, there have already been improvements to speed, with the purported Ether speed increasing to twenty transactions per second.

Chart 4: Transaction speed of traditional payments vs major cryptocurrencies



Source: BIS Annual Economic Report 2018.

Public vs private

Whilst the decentralised nature of blockchain can be attractive as it does not rely on a central organisation, it is also one of the key features that prevents public blockchain from widespread mainstream commercial application.

The decentralised system has computational power issues mentioned above. There is also the fundamental problem of trust in an unknown online community. However, blockchain can also be utilised in a private or permissioned form instead of an open source decentralised platform. In a private blockchain, permission to read and/or verify the information is restricted to certain participants.

Private blockchains that are being developed to perform specific functions also result in less energy consumption. These private blockchains are therefore not as controversial from an environmental perspective.

Private blockchains in the finance industry

Given the hurdles to widespread commercial adoption outlined above, public blockchain do not appear to be a major threat to mainstream financial institutions in the near term.

Nevertheless, private blockchains or DLTs can generate time and savings through operating a specific function. Recall that blockchain is one specific type of DLT. Blockchain is the most secure given its decentralised nature and the fact that transactions are vetted by a vast number of participants, but this comes at the cost of speed. In a private blockchain/DLT, permission to read and/or verify the information is restricted to certain participants, hence speed is increased. To date, we have seen private blockchains/DLTs being adopted in the commercial space. This allows corporations to control the participants that can view or edit transactions, and thus protect their business.

Northern Trust has developed a private blockchain for Unigestion, one of its fund managers, to operate the fund administration process for private equity transactions (they are also giving access to their auditors to access transaction data as they occur real time). Only Unigestion, the limited partners, lawyers and regulators have access to the information. The advantage of operating on this private blockchain is to streamline a complex multi-party process of exchanging contracts with multiple revisions, and releasing funds once conditions are met.

Another example is the DTCC, which is testing a permissioned blockchain platform to centralise the storage of information regarding trades of Credit Default Swaps. Locally, the ASX has announced that it will be replacing its clearance system, CHESS with Distributed Ledger Technology in another two to three years.

The cost of building a private blockchain/DLT and replacing existing proven systems may very well outweigh the benefits in some instances. For example, the Depository Trust Clearing Company (DTCC) announced in 2017 that it had successfully tested blockchain based technology for the clearing and settlement of repurchase agreements (repos) but in March 2018 put the breaks on this project.

Private blockchains or DLTs can generate time and savings through operating a specific function.

The cost of building a private blockchain/DLT and replacing existing proven systems may very well outweigh the benefits in some instances.

Implications for institutional investors

What does this all mean for asset owners managing institutional portfolios? The key take-outs for the institutional asset owner are summarised as follows.

Awareness of the potential disruption

Blockchain has the potential to displace or greatly reduce the role of current financial organisations (such as banks, custodians, share registries and clearinghouses) due to the disintermediation effect. However, there are significant hurdles that prevent this from occurring in the immediate future. Nevertheless, asset owners should have an awareness of the ongoing technological developments and understand some of the issues that their service providers are facing. Financial institutions that have the capital to invest early, develop and successfully incorporate the technology into their business, could in fact be a disruptor themselves through efficiencies and cost cutting.

Investment implications

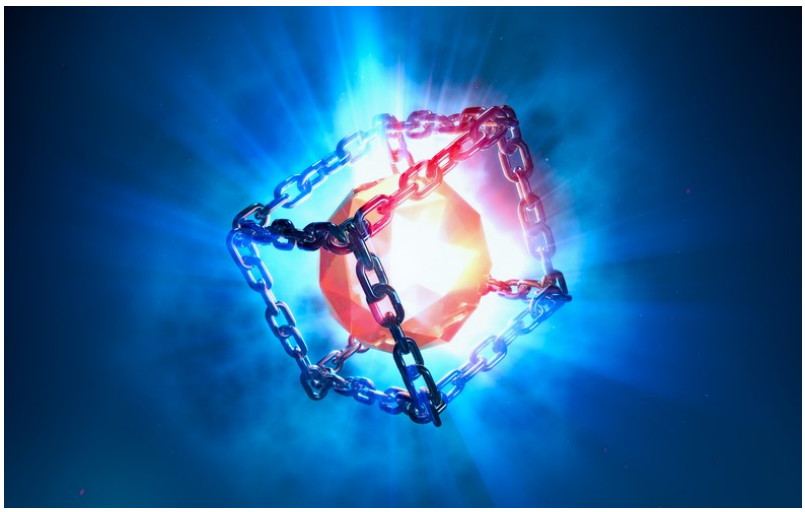
Asset owners are likely to have exposure to such financial organisations in their portfolios (through equities, loans or derivatives). As investors, understanding the potential impact of blockchain on these businesses, and whether it is a threat or opportunity is pertinent. However, caution should be applied when reading media reports on companies utilising blockchain technology. Too often, companies eagerly make bold announcements about adopting, experimenting or releasing blockchain "proof of concepts", but the subsequent adoption is not always clear.

Emerging asset classes

If the tokenisation of real assets (or other alternative asset classes such as art, antiques, vineyards etc) proves viable, this could expand the opportunity set for investment as it provides for more diversification of risk through owning fractions of new asset classes. Investing (or speculating) in cryptocurrencies is also becoming an increasingly discussed topic, and there are a few hedge funds that have done so.

The focus of this paper has been on the institutional applications of blockchain, rather than considering cryptocurrency as an asset class for potential investment. Whilst there may potentially be attractive risk adjusted returns from such investments, as with any asset class, specialist skill is required to identify the opportunities.

The cryptocurrency space is particularly rife with hype, and few are able to identify inherent fundamental value (i.e. encryption protocols that will work and gain widescale adoption), as opposed to trading or speculating in cryptocurrencies that are merely benefiting from the euphoria. To date, attempts to launch bitcoin ETFs (by Van Eck, SolidX and Winklevoss brothers) have been rejected by the SEC, but this may change in the future.



The final word…

Blockchain has many attractive features including disintermediation gains, immutability and programmability. Whilst blockchain has the potential to disrupt mainstream financial institutions, there are significant hurdles to widespread adoption. However, businesses can still greatly benefit from private blockchains/distributed Ledger technologies and this approach has underpinned most commercial applications to date. Frontier will continue to investigate advances in blockchain technology and its application as part of our ongoing research program.

Appendix - Definitions

Proof of Work (POW)	A system requiring a substantial amount of 'provable' work to be completed in order to verify the validation of transactions and deter bad participants from disrupting or misusing computational power.
Proof of Stake (POS)	A system where 'mining' is done based on the amount of ownership of a digital asset rather than the nodes computational power.
Block	A set of transactions grouped together to be added to the blockchain.
Node	A computer connected to the blockchain network working to validate blocks of transactions.
Mining/Miner	The process of validating blocks of transactions by solving mathematical puzzles.
Hash/Hash Rate	Amount of power required to keep the network operational, specifically for cryptocurrencies leveraging 'Proof of Work'. As the difficulty for mining each block increases, the higher the hash rate as power demand increases.

FRONTIER ADVISORS

About Frontier Advisors: Frontier Advisors is one of Australia's leading asset consultants. We offer a range of services and solutions to some of the nation's largest institutional investors including superannuation funds, charities, government / sovereign wealth funds and universities. Our services range from asset allocation and portfolio configuration advice, through to fund manager research and rating, investment auditing and assurance, quantitative modelling and analysis and general investment consulting advice. We have been providing investment advice to clients since 1994. Our advice is fully independent of product, manager, or broker conflicts which means our focus is firmly on tailoring optimal solutions and opportunities for our clients.

Frontier Advisors Pty Ltd ABN 21 074 287 406 AFS Licence No. 241266