Kevin Jenkins

Blockchain in Aotearoa
are distributed ledgers the future for our regulators and policymakers?

Abstract

Blockchain technology has been moving beyond cryptocurrency into new areas internationally, with substantial investment from both the private sector and government, including private sector projects in Aotearoa. However, there is not yet clear evidence of successful use cases at scale. The technology offers important benefits through creating tamper-proof records of transactions, and major drawbacks of public networks like bitcoin, such as massive power consumption, do not seem to apply to regulatory uses based on private blockchain networks. But there is debate over whether the technology is as secure as its proponents claim. In exploring blockchain's potential, regulatory designers will want to carefully consider more conventional alternatives such as distributed databases.

Keywords blockchain, distributed ledger, trust, regulatory design

Kevin Jenkins is a founder of professional services firm MartinJenkins.

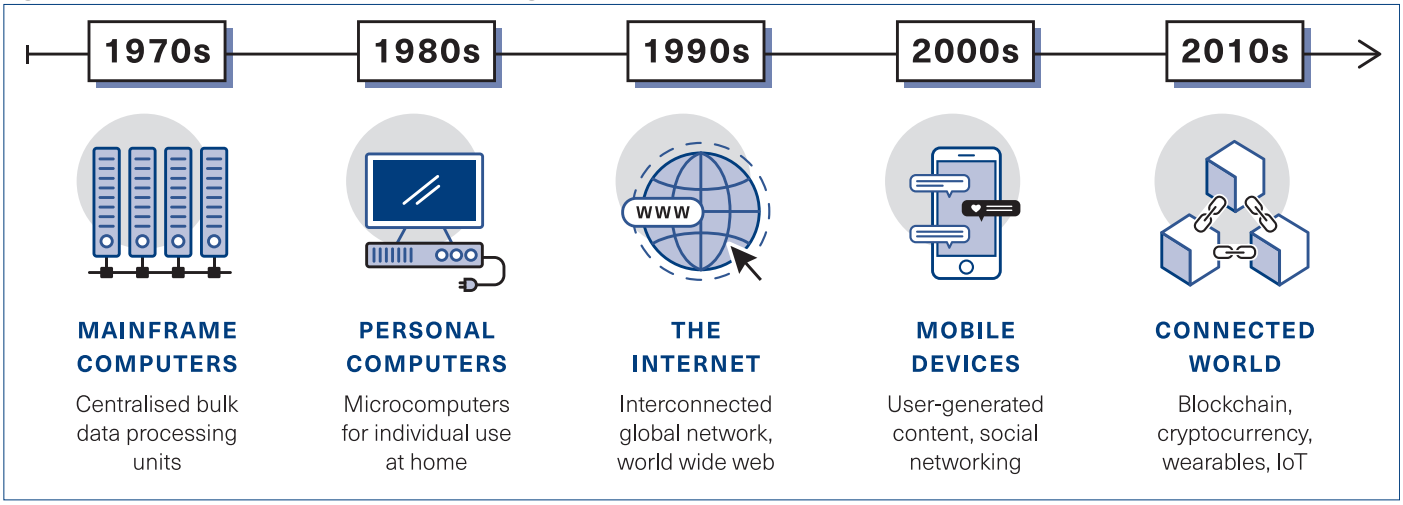
Blockchain technology – the best-known type of 'distributed ledger technology', or DLT – is a complex and very fast-moving phenomenon that has seen large investments from government and industry around the world, including in Aotearoa. There is a mass of commentary and reporting, and frequent announcements of new blockchain projects or pilots.

This article presents the results of my efforts, as a layperson interested in the interface between technological innovation and regulation, to find my bearings in the blockchain landscape, to canvass some of the often wildly diverging views, and to identify relevant questions for regulatory designers to ask in evaluating the technology's potential.

Just cryptocurrency – or a whole world of potential uses?

The OECD has recently declared that 'Blockchain technology has evolved from a niche subject to the hottest tech disruption buzzword' (Berryhill, Bourgery

Figure 1: Blockchain in the context of successive digital revolutions



Source: graphic by Lan Fu, MartinJenkins

and Hanson, 2018). But the debates and commentary in this area indicate that the blockchain industry is facing two possible futures.

One future sees blockchain technology as entwined with bitcoin, the cryptocurrency it was designed to enable, and with which the technology was packaged when it was first released into the world. Saifedean Ammous, for example, a US economics professor, scoffs at the idea of blockchain offering much beyond bitcoin:

> There is no reason, except for ignorance of its mechanics, to expect that it would be suited for other functions ... Blockchain is better understood as an integral cog in the machine that creates peer-to-peer electronic cash with predictable inflation. (Ammous, 2018, p.272)

The other camp sees cryptocurrency as simply the foundation use-case, with many more in play or shortly about to be. This camp says we are only scratching the surface of the benefits that blockchain technology can offer for business, government and citizens in general. For regulatory systems specifically, it is supposed to offer greater effectiveness in the form of better security and accuracy, and also greater efficiency and economy.

So how is this going to play out, including in Aotearoa? A recent report published by the Callaghan Institute, by Joshua Vial of Enspiral, clearly takes the second, more expansive view. Vial argues that 'Distributed ledgers and blockchains are emerging general purpose technologies that are likely to have a significant impact across all aspects of the economy' (Vial, 2018). He argues that in Aotearoa we need a more blockchain-friendly economic and regulatory environment.

Vial's strong statement suggests that this projected blockchain revolution may be as exciting and comprehensive as, say, the personal computer revolution of the 1980s, where, whatever you and your business or agency were doing, putting a computer on your desk was pretty much guaranteed to mean you'd be doing your work more quickly, more accurately or more cheaply, or all three, with significant gains in productivity.

But there have been warnings out there that that great promise is still mostly just a promise. The McKinsey consulting firm wrote at the start of 2019:

> A particular concern, given the amount of money and time spent, is that little of substance has been achieved. Of the many use cases, a large number are still at the idea stage, while others are in development but with no output. The bottom line is that despite billions of dollars of investment, and nearly as many headlines, evidence for a practical scalable use for blockchain is thin on the ground. (Higginson, Nadeau and Rajgopal, 2019)

Early moves beyond cryptocurrency: Ethereum's 'smart contracts'

Vitalik Buterin is the legendary founder of the blockchain-based platform Ethereum, usually second or third to bitcoin for cryptocurrency market cap. Some have suggested he's part-robot, but he seemed like a super-bright, driven, but still very much human entrepreneurial geek when I saw him speak in Wellington in 2017.

Ethereum is an early example of using blockchain technology for more than cryptocurrency. Descriptions can get pretty complicated quickly, but *Blockchain Revolution*, by father-and-son team Don and Alex Tapscott, and the biggest selling blockchain book so far, usefully explains the difference between the platform, the application and the currency (which is called Ether):

> Ethereum is a platform technology, designed from the outset to enable *distributed applications* (DApps) … At the core of distributed applications are smart contracts, software that mimics the logic of a business agreement. … they minimize the need for intermediaries (banks, brokers, lawyers, courts …). If Ethereum is the city grid, and the DApp is the car, then ether is the fuel. (Tapscott and Tapscott, 2016, pp.xxxii–iii)

Ethereum's 'smart contracts' offer the prospect of extending the benefits of blockchain technology beyond cryptocurrency afficionados to cover a vast range of contractual transactions in everyday commercial and personal life. They are supposed to be self-executing and self-enforcing, so that, for example, payment is triggered automatically when

certain conditions are met. A better name for them may, however, be 'dumb contracts', as they essentially just work their way through a series of binary yes–no options to reach a conclusion based on the relevant value at each option point. They have been criticised as too inflexible to handle the nuances and unforeseen circumstances that make up much of the real life of contractual arrangements and disputes (Notland, 2019). But like bitcoin and other blockchain cryptocurrencies, they offer the benefit of a tamper-proof transaction record and eliminate the need for third parties and the costs that they entail.

'Blockchain 3.0' – the next digital revolution?

Melanie Swan, discussing the pattern of the last half century of a digital revolution every decade, places blockchain and smart contracts in the 'connected world' revolution of the 2010s (Swan, 2015). She argues that blockchain represents a whole new layer of the internet that facilitates value transactions.

Swan talks of three blockchain stages. Blockchain 1.0 has been bitcoin and other cryptocurrencies. Blockchain 2.0 has been the extension of blockchain into 'smart contracts' along Ethereum lines: for example, for transactions involving land title, shares and mortgages. What's up next, she says, is Blockchain 3.0, involving the application of the technology to completely different sectors, such as government, health and art.

As the title of their *Blockchain Revolution* gives away, the Tapscotts join Melanie Swan in the broad revolutionary camp, where blockchain steamrolls into new sectors. They call blockchain the 'Internet of Value'. In their eyes what we call the internet is really just the 'Internet of Information' because all it does is move information – copies of documents, photos, audio – from person to person. They see blockchain as revolutionary because it is disruptive of at least seven domains. Financial services is familiar, but they also cite the design of firms, business models, the Internet of Things, economic inclusion, government and democracy, and the creative industries.

Putting those disruptions together, they are saying the world will be remarkably different – and better – in less than a generation because of blockchain. Key to these changes is radical decentralisation, and also a move to most transactions being between things (through the use of smart infrastructure and devices), not people.

From Estonia to Uttar Pradesh, DLT projects abound

There have been plenty of signs of movement into the Blockchain 3.0 zone, from both government and the private sector, often in partnership.

Consistent with our membership of the D9 group of advanced digital nations, which includes Estonia, the United Kingdom, South Korea, Israel and others, New Zealand has seen a lot of activity and investment in blockchain technology, though not yet any government applications.

Estonia has been an early leader in government adoption of distributed ledger technology, as it has in digital government generally, and began experimenting early on with a locally developed form of DLT called 'keyless signature infrastructure' (UK Government Chief Science Advisor, 2016). It has been making use of distributed ledger technology in a number of areas, including identity management and health records (Halim, 2019; Shen, 2016).

Dubai is another governmental leader in the use of distributed ledgers. Its Dubai Blockchain Strategy set the bold target of making Dubai 'the first city fully powered by Blockchain by 2020'. In January 2020 it reported it had succeeded in implementing 24 applicable use cases, including establishing a shared platform that government agencies could use to implement use cases rather than having to invest in individual platforms (Smart Dubai Department, 2020). Fully implemented use cases include verification of property titles, the issuing of university certificates, the licensing of healthcare specialists, and requesting a certificate of loss of passport.

It is difficult to keep up with the announcements of new blockchain or DLT projects internationally – which are, however, frequently only pilots and proof of concept exercises. Blockchain has been discussed as particularly well suited to the transactions of 'prosumers' in areas such as peer-to-peer home-generated solar power that is fed into electricity grids. At the end of 2019, a new pilot along those lines was announced for the Indian state of Uttar Pradesh, which, with just over 200 million people, is the largest sub-country political entity in the world. The pilot involves two state-owned power utilities partnering with an Australian energy blockchain company, Power Ledger. This is Power Ledger's second such pilot in India, adding to a project in New Delhi, but the new project is significant in that Uttar Pradesh would be the first Indian state to amend its regulatory framework to allow peer-to-peer energy trading (India Times, 2019; Lewis, 2019).

… and on to Christchurch

Consistent with our membership of the D9 group of advanced digital nations, which includes Estonia, the United Kingdom, South Korea, Israel and others, New Zealand has seen a lot of activity and investment in blockchain technology, though not yet any government applications.

Centrality (https://centrality.ai/) is a marketplace for decentralised apps (dApps) for software developers that is incubating

blockchain companies. TrackBack, for example, completed a proof of concept to track mānuka honey from New Zealand to Shanghai. TrackBack worked with AsureQuality, New Zealand Post and a producer to tackle the fake mānuka honey trade.

Techemy (https://techemy.co/) is a New Zealand-based community of blockchain companies that invests, owns and develops companies 'at every stage of the blockchain value chain'. Joshua Vial's New Zealand report tells how Amazon's Alexa uses data supplied by Brave New Coin (https://bravenewcoin.com/), launched by Techemy, to answer questions about the price of bitcoin. Another Techemy investment is Sphere Identity (www.sphereidentity.com), which is working to offer self-sovereign identity so we consumers can control our own personal data, while removing the painful issues around online forms and abandonment rates. Other companies working on sovereign identity in New Zealand include SingleSource (www.mysinglesource.io), which partnered with Auckland company Delta Insurance (https://deltainsurance.co.nz/) to provide a decentralised blockchain identity system.

Joshua Vial cites other examples of blockchain start-ups in Aotearoa. Axia Labs is a global blockchain company founded in Christchurch in 2017 by political science and philosophy graduate James Waugh. In 2013 he learnt to use cryptocurrency to avoid PayPal charges when he sold in-game items for real-world money, leading him to focus on blockchain and cryptocurrency in almost all of his free time since.

Axia Labs is focused on 'building a more equitable economy' and, in practice, they provide top-down advice and help leaders and innovators connect more deeply with the blockchain ecosystem. Axia has worked with a wide range of international clients, including institutional corporations, universities, enterprise companies and numerous tokenisation projects. Zeroing in on token economics, decentralised architecture and industry best practices, a large portion of Axia's time has been spent in Silicon Valley and London, focusing on the global market.

We are attracting blockchain entrepreneurs from overseas too. Here's Vial again:

> They include the co-founder of Coinbase (the first billion dollar blockchain company), the co-founder of Augur (one of the first Ethereum initial coin offerings) and the head of innovation at UNICEF who has launched an impact-driven blockchain investment fund.

His report also talks about how Stronghold (https://stronghold.co), an exchange focused on the Stellar platform (www.stellar.org), was attracted to Aotearoa because we have a single regulator (the Financial Markets Authority) 'with a high degree of literacy about crypto-exchanges and a willingness to engage'.

If you're a bitcoin user-owner, no one can mess with your bitcoin because you have your own private digital key, but if you forget or lose your key then of course *you* can't mess with your bitcoin either.

Transacting securely without the need for trust: does the technology deliver on the promise?

The revolutionary content attributed to blockchain technology, and exemplified by bitcoin, is that it addresses the core problem of trust. For example, we can't safely send money through the post, so instead we work through trusted intermediaries like payment companies, banks and governments. Blockchain allows value – either digital cash or other digital artefacts with monetary value – to be transmitted safely.

Some call it 'the trust machine' (Berryhill, Bourgery and Hanson, 2018). But more accurately, as Saifedean Ammous explains, it takes the need for trust out of the equation altogether: that is, the code is transparent, and any change is also transparent and needs to be agreed by a majority of those involved (Ammous, 2018). So it's a trustless set-up, but in a completely benign way.

That said, there are some obvious limits to security without a trusted central authority. If you're a bitcoin user-owner, no one can mess with your bitcoin because you have your own private digital key, but if you forget or lose your key then of course *you* can't mess with your bitcoin either. With conventional banking, losing your bankcard or forgetting a password is likely to cost you only some time and inconvenience. But it's different with bitcoin, as John Lanchester notes:

> the unforgiving power of the public address/private key combination has also seen 7500 bitcoin lost under a landfill outside Newport in Wales, when an IT worker chucked out an old hard drive on which he had stored the private keys from his 2009 bitcoin stash. Current value of loss: £2.1 million. (Lanchester, 2016)

Kai Stinchcombe represents a fairly extreme view among blockchain detractors of the downsides of removing the security offered in the form of banks and other traditional trusted intermediaries. Phrases like 'crap technology' and 'medieval hellhole' give you a flavour of his polemic. He argues that our current trust-based systems more or less work, and that the trustless bitcoin system is just what banking looked like 800 years ago in Europe:

> with weak governments unable to enforce laws and trusted counterparties few, fragile and far between – theft was rampant, safe banking was a fantasy, and personal security was at the point of the sword. This is … what it looks like to transact on the blockchain *in the*

ideal scenario. (Stinchcombe, 2018; emphasis in original)

But can I trust the technology?

Worries about lost bitcoin keys aside, there may be a more fundamental, more 'meta', objection to the claim that blockchain technology provides security without any need for human trust.

The blockchain evangelists argue that the beauty of the technology is that it provides security without the need to trust in the honesty or integrity of any humans or social institutions. But of course you do need to trust in the integrity of the technology itself. And so what if you can't? Or more precisely – how do you know if you can or not?

Saifedean Ammous has criticised the Ethereum platform because, he argues, it suffered a fork – a splitting of the single indisputable record into two versions. He says that, to solve their (alleged) fork problem, Ethereum developers had to create a new version of the record and carry on as if 'this inconvenient mistake never occurred'. Ammous says: 'This re-injection of subjective human management is at odds with the objective of making code into law, and questions the entire rationale of smart contracts.' Bitcoin/blockchain expert Jimmy Song generally agrees. He claims Ethereum has suffered at least five forks, and that each time 'They've bailed out bad decision making' – that is, they've exercised central authority. 'By any measure', Song concludes, 'Ethereum is centrally controlled' (Song, 2018).

When I heard Ethereum's Buterin speak in New Zealand in 2017, he denied it was a fork, and at that point the debate got too technical for me to follow. But reflecting on this later, I wondered if my inability to follow the blockchain story at this point was more than just a research problem and was in fact part of the story, with me as a representative of the non-expert billions.

As a layperson, what am I to do when the experts disagree about whether one or other blockchain platform has suffered a fork, which is nothing less than a disastrous breakdown of the whole system? Which expert do I listen to on this? Do I ask which institution they might be attached to, and then ask about that institution's reputation and credibility? In other words, which expert do I … trust?

It's interesting that in practice most bitcoin users access this market through intermediaries anyway – cryptocurrency exchanges – although perhaps more for convenience than security. Rather than working out how to download the platform software and establish themselves as a blockchain node (all quite doable, depending on your digital competence and access to a suitable computer, but of course most likely time-consuming), the typical bitcoin transactor chooses to go through an exchange and buy or sell bitcoin through them.

So there seem to me to be questions about how successfully blockchain technology replaces trust with clever software. Put another way, and to refashion a story popularised by Stephen Hawking, do we really have a trustless pile of turtles all the way down, or do we inevitably find there's an inter-human trust relationship at the bottom holding the whole edifice up?

As much electricity as a small country

Shift perspective now to that of a regulator or policymaker, rather than a cryptocurrency user. An early question I had about blockchain's potential relevance for government was how the cryptocurrency network architecture would translate to the world of public sector regulation. The short answer appears to be that much of it does not, and doesn't need to, including several negative features that might alarm regulatory designers.

… the bitcoin system is very slow at processing transactions: about seven per second is the best it can do, whereas Visa, for example, handles more than 1,500 per second …

Needless to say, one of your first questions in deciding to approach a cryptocurrency exchange will be which of these intermediaries you should trust. It's not an unimportant question, as shown by the hack of the Japan-based Mt Gox exchange in 2014. Mt Gox was, by 2013, the biggest and most well-known exchange handling bitcoin, dealing with 70% of all transactions. In early 2014 the exchange shut down after losing 850,000 bitcoin to hackers, a loss valued at US$450 million at the time, but at US$8.5 billion by 2019 (Baydakova, 2019).

Mt Gox is not an isolated story. According to Reuters,

> There have been at least three dozen heists of cryptocurrency exchanges since 2011; many of the hacked exchanges later shut down. More than 980,000 bitcoins have been stolen, which today [September 2017] would be worth about $4 billion.

It described cryptocurrency exchanges as having become 'magnets for fraud and mires of technological dysfunction' (Stecklow et al., 2017).

For one thing, the bitcoin system is very slow at processing transactions: about seven per second is the best it can do, whereas Visa, for example, handles more than 1,500 per second (Berryhill, Bourgery and Hanson, 2018, p.33). This is because of the time it takes to record transactions to a new block and then write the new block to the blockchain. So, as a platform like bitcoin gets more and more popular and the transactions increase, it faces problems scaling up.

The bitcoin network also uses a truly horrendous amount of power – in 2018 reportedly about as much as Ireland (Economist, 2018). So there's an unsettling disconnect between bitcoin's clean, digital vibe and all that very real-world energy going in to power the banks of bitcoin-mining computers and the air-conditioning needed to stop them overheating. In this time of Greta Thunberg and potential global

catastrophe, you can't help asking: can the way ahead – the fully unfolded fourth industrial revolution – really look like *this*?

The good news is that both those problems – slow processing and massive energy use – are inherent to bitcoin's public, permissionless network model, but not inherent to blockchain applications generally. It's all because the computing tasks involved in recording and storing the data in this open DLT system are *deliberately* made hard. Satoshi Nakamoto – the he, she, they or it who designed blockchain and bitcoin – set up the writing and storing of the blocks that way, using a 'proof of work' model where bitcoin 'miners' expend massive computing power to solve artificial computing tasks (see Box 1).

By contrast, in a private – or 'permissioned' – blockchain network, access is controlled and permission to write transaction data to the blockchain depends not on proof of work, but simply on proof of authority. We can assume that all the public sector use cases that have been implemented or piloted internationally involve private, permissioned blockchain networks. Translated to regulatory use, writing data in a blockchain network established by a government agency would depend simply on permission from that agency.

Here, of course, we're back in the world of trusted central authorities underwriting the whole system, but still with the advantages of a distributed ledger – along with faster processing and much lower energy consumption. Using a proof of authority model, different levels of permission are possible, including, for example, permission to access and read the information, permission to enter data and transactions on the system, and top-level authority to edit and control access to the network.

Most important, perhaps, government ownership of the network also effectively solves the 'fork' problem that can arise in public networks. The possibility of a fork exists precisely because of the open democracy of a system like bitcoin, where all nodes are equal.

Blockchain in the public sector – what is it good for?

There are detractors, like Kai Stinchcombe,

BOX 1 Bitcoin and blockchain: how it works

Blockchain cryptocurrency technology is a classic example of the coming together of several existing technologies to produce something revolutionary and disruptive: cryptography, online payment processes, game theory and software coding.

It's good to get it straight at the outset that 'blockchain' is the underlying technology and 'bitcoin' is a specific platform or use case. Blockchain is 'a digital distributed ledger system that acts as an open, shared and trusted record of transactions among parties that is not stored by a central authority' (Berryhill, Bourgery and Hanson, 2018). Blockchain is not the only type of distributed ledger technology, or DLT, but it's the best known.

Distribution is key here. All the different users – or 'nodes' – on the network, such as bitcoin owners:

> hold identical 'ledgers' of transactions that are rapidly updated any time a new set of transactions is added. This enables a key feature of the Blockchain architecture: consensus models where nodes in the system confirm the validity of transactions that occur on the platform, and flag inappropriate dealings when necessary. (ibid.)

Joshua Vial of Enspiral puts it this way:

> A distributed ledger is a set of data replicated across many networked computers. … [It] uses protocols so changes are consistently replicated to each computer and the data converges to an agreed known state. (Vial, 2018)

So it's not that each node – each bitcoin user-owner – holds a copy of the ledger, with the accompanying uncertainty that a copy might be altered, deliberately or accidentally, and diverge from the original. Rather, they all hold the same ledger.

Disintermediation

Bitcoin is a *public* distributed ledger system. A buzzword used to describe the effect of such a distributed ledger is 'disintermediation' – that is, the removal of the need for a central authority to act as a trusted intermediary and validator when thousands of individuals who don't know each other and have no particular reason to trust each other want to transact with each other. Or, as Berryhill et al. put it, disintermediation refers to 'The potential to reduce or eliminate the friction and costs of current intermediaries' (Berryhill, Bourgery and Hanson, 2018).

So there's no central authority – some large, stable, possibly government-backed institution – at the core of the system. But it's also more than merely decentralisation. The point is that everyone in the network, every node, is connected to every other node at the same time.

That distinction between decentralisation and distribution was key to Paul Baran's model – now more than half a century old – for communications networks, which was immensely influential in the design of the internet (see Figure 2).

Two steps: validation plus storage

There are two critical steps to the bitcoin-blockchain system. First, transactions are validated, and here the distributed nature of the ledger is key. Validation depends on a majority of all users (or rather their automated software) agreeing that a bitcoin transaction is valid. (The potential for a nefarious 51% vote to agree to validate an invalid transaction is another story.)

It's the next step – writing and storing the record of the validated transaction – where the blockchain itself is key. A 'block' is an encrypted and unique set of validated transactions. Blocks are linked in a 'chain' in a way that means the information is accessible but cannot be tampered with – that is, it's essentially

who would presumably reply, 'Absolutely nothing' here. However, as we have seen from the international examples, a lot of respectable and presumably careful institutions are putting significant resources into exploring the potential in that 'Blockchain 3.0' space projected by Melanie Swan, where both private sector and governmental actors take blockchain's benefits into completely new fields.

So, using a proof of authority network model under government control, in principle what kind of specific regulatory uses does it seem blockchain technology would be best suited to?

The OECD report emphasises that the technology is useful for validating and recording *transactions*, not for general data storage (Berryhill, Bourgery and Hanson, 2018). This suggests a range of potential use cases, such as motor vehicle sales and records of land title. In line with that transaction focus, the OECD also suggests a potential use for smart contracts in providing an automated process for determining eligibility for government services, such as welfare benefits.

A number of countries have in fact already established, or are establishing, new land title systems based on blockchain networks, including Bermuda, Brazil, the UK, Sweden, Russia, Georgia, Ghana and Rwanda. The absence of reliable records of land ownership is a particularly significant problem in developing countries (Kriticos, 2019; Kshetri, 2018). Fragile paper-based systems are often incomplete, and are particularly open to error, forgery and official corruption. This is a barrier to economic development, as without clear title it is difficult to obtain finance, and the risk of expropriation through fraud and corruption discourages owners from developing the land in any case. Blockchain solutions can provide certainty of title, protect against tampering by corrupt officials, and facilitate transfers and development, with lower transaction costs.

There are some significant barriers, however. First, digitising an old paper-based system is a major undertaking, requiring significant investment. Further, there are some problems that a blockchain

Figure 2: Centralised, decentralised and distributed networks

Source: graphic by Lan Fu, MartinJenkins

a list of transactions to which information can only be added. That's why it's called a chain: the blocks are related to each other in a linear sequential order.

Bitcoin mining: the 'proof of work' model

All of the nodes on the bitcoin network are involved in validating transactions, but only some of them – called 'miner' nodes – are involved in storing the transaction records in the blockchain.

The miners – or rather their large banks of computers, often located in cool northern climates to cut down on air-conditioning costs – compete among each other for the right to publish the next block in the blockchain by racing to complete complex mathematical tasks. Winning the race gets you a substantial amount of bitcoin. The system is even designed to make these tasks progressively harder as computing power increases.

This mining system is referred to as the 'proof of work' consensus model. The model is specific to the public – or 'permissionless' – blockchain model that bitcoin represents, where anyone can download the software and join the network and where users can operate pseudonymously – that is, they have an account with a name (or multiple accounts), but it doesn't need to be their real name. Alternative proof models include 'proof of stake', where the blockchain writer must show they have some kind of credentials, like a record of valid transactions.

A private, permissioned blockchain network – the type relevant for regulatory designers – is constructed quite differently, using a 'proof of authority' model. Here, the identifiable parties who set up the network – say, one or more government agencies – or who have been authorised by those who set it up, have the credentials to write to the blockchain.

network obviously can't solve: for example, it can create an authoritative, tamper-proof record of land title and thereby help prevent future disputes, but where there are numerous outstanding disputes as to ownership a blockchain solution isn't itself a means of resolving them.

Sebastian Kriticos notes these problems:

> As many governments, particularly in developing countries, continue to grapple with land governance and administration challenges, including the digitisation of their registries, blockchain is still a long way from being implemented at scale. However, there may already be potential to pilot initiatives in smaller sub-areas where governments have been able to establish a strong record of land titles. (Kriticos, 2019)

The transaction data in a blockchain system can only be as valid and accurate as the input data; as they say in the computer world, 'garbage in, garbage out'.

The limits of blockchain validation?

That problem of pre-existing uncertainty also points to a broader limitation of blockchain technology as a 'validator' of transactions.

A proof of concept exercise by US Customs and Border Protection trialled a blockchain network for receiving and verifying data on origin of goods (US Customs and Border Protection, 2018). Here, it appears, the technology was able to successfully verify the place and producer/supplier of origin, as the identity of the producer/supplier was 'anchored' in the blockchain data. In this case, the identity of the transactor was itself a key element of the input data.

But in other cases blockchain systems may often be of little help as a verifier of real-world facts. If a grower has entered data in a supply chain management system to the effect that a certain batch of produce is organic, blockchain technology can tell you whether anyone has later tampered with that data entry, but it can't tell you whether the grower was lying in the first place and had in fact used pesticides.

So blockchain 'validation' of transactions may often need to be understood in a very qualified sense. Verifying the accuracy and integrity of data will often require another layer of human intervention from testers and inspectors. The transaction data in a blockchain system can only be as valid and accurate as the input data; as they say in the computer world, 'garbage in, garbage out'.

Avoiding the single point of failure problem

Proponents of blockchain solutions in areas such as land governance or identity management in developing countries emphasise the considerable benefits to be gained from moving to these new digital solutions from fragile, incomplete paper-based systems (if a system exists at all). But it should also be emphasised that these are digital solutions of which blockchain technology is just one component.

For example, in advocating for blockchain's ability to solve a number of key problems for governments and citizens in the areas of identity management and government records and services, Joshua Woods presents the advantages of a package of three elements: digital systems rather than paper-based; authentication of identity by biometric information; and blockchain (Woods, 2018). But regulators most likely won't take much selling on the advantages of components one and two: we have been living in the world of mainstreamed digital solutions since the 1980s, and of large-scale applications for biometrics since the 2000s. Two decades into the 21st century we of course don't need bitcoin's Satoshi Nakamoto to tell us of the advantages that those two groundbreaking innovations provide.

So what are the particular capabilities and advantages of blockchain technology compared with *other* technological solutions that would also involve digital-plus-biometric components? Woods, discussing identity management, argues that a distributed ledger provides a secure, 'immutable' record that can't be altered by corrupt officials or hackers:

> even if a unified digital identity were to exist, centralized data storage would provide a major target for hackers who could then breach, steal, and/or change citizen information, voting results, or tax records. Ransomware attacks, for example, on these data types would be devastating. Since all of these breaches would have a high degree of societal impact, data storage systems must be ultra-secure and not built with single points of failure inherent in centralized design.

The Ethereum website similarly emphasises security as a key element:

> Governments and public sector organizations leverage blockchain technology to move away from siloed and inefficient centralized systems. Current systems are inherently insecure and costly, while blockchain networks offer more secure, agile, and cost-effective structures.

So blockchain networks are supposed to provide immutable, tamper-proof records in ways that alternative technologies cannot, particularly through eliminating the single point of failure risk.

We should remember, though, that the strengths of a technology are always context-specific. Immutability won't be a strength if you want to be able to modify the contents of the record in line with changes to the real-world facts it reflects.

Security now and in ten years' time

As we saw, depending on who you listen to there appears to be a question mark over how vulnerable the technology is to forks

and hacks. With a private network the fork problem appears to be eliminated, but, even so, regulatory designers will naturally want to ask very searching questions about the level of security provided by blockchain solutions against hacking. Not only would they want to be confident that the technology is sufficiently secure right now, public sector regulators looking to make major future-proofed investments in new technology would also want to be confident the technology will still be secure in ten years' time. Even if blockchain is as secure as its proponents claim, regulatory designers might well ask: could this turn out to be a case of blockchain being unhackable until it wasn't unhackable any more? Quantum computing, for example, may be just around the corner in mainstream applications. It's a world where the binary language foundation of modern computing, where any given bit is either a 1 or a zero, is upended by the possibility of a bit being both a 1 and a zero at the same time.

In October 2019, Google announced a successful trial of its new quantum computer, claiming that it had taken seconds to solve a problem that would have taken the most powerful supercomputer thousands of years (CNBC, 2019). Critics pushed back, saying Google had exaggerated its achievement: IBM, the main quantum computing rival, said a supercomputer with some more storage could solve the same problem in several days, rather than several millennia (ibid.).

But overselling from Google or no, we could be forgiven for imagining that by 2025, quantum computing – and solutions to previously unsolvable computing problems – might be a newly established part of our world, much as Uber and the new disruptive digital platforms are today, and with qualitatively new potential for hackers to breach systems like blockchain.

Considering the alternatives

In evaluating the potential of blockchain solutions, it will be important for regulatory agencies investing in new technology to think hard about their specific need and context; to ask exactly what problem they want to solve and what their current pain points are. As well as considering whether blockchain technology will solve that problem, they will also need to ask whether blockchain will do it better and more cost-effectively than alternatives.

Apart from non-blockchain DLT systems, alternatives include distributed databases of the more conventional type. All distributed databases are designed to appear to the user as if they were accessing a centralised database stored at a single physical site. However, compared with a centralised database, distributed databases can provide superior rates of reliability and availability and speed of processing requests, although at the cost of greater complexity. Regulators may find that the level of security and functionality a distributed database provides is sufficient for their needs. The cost of designing and implementing it may also be relatively low.

Different types of distributed database offer different packages of pros and cons. A 'replicated' distributed database includes complete copies of the database at each site and so, like blockchain, provides protection against single point of failure risk (as well as allowing parallel processing of user requests). However, it also creates the need to constantly update all sites and to manage concurrent access by users, to avoid inconsistency between copies (the fork problem again). With 'fragmented' distributed databases, the data is divided up and held at different sites, to make up a single copy of the one logical database. This doesn't provide redundancy protection, but there's also no risk of inconsistency.

Regulatory designers will need to consider the size and make-up of their particular network, including whether or not it will include private sector actors, such as with a supply chain management network. We have seen that beyond cryptocurrency blockchain technology may be well suited for other networks that involve a very large number of user-nodes, in the hundreds or thousands: for example, peer-to-peer electricity networks involving 'prosumers', where there is a need for recording many transactions and where prices can shift rapidly from transaction to transaction. By contrast, the needs of a regulatory system involving just a handful of nodes – perhaps different agencies or sub-agencies – may well be met by a more conventional distributed system.

As a foundation for cryptocurrencies, blockchain has already changed some of the international financial services landscape, and it is clearly appropriate that the Reserve Bank of New Zealand is exploring the technology's potential.

Guarding against unreasonable expectations

As a foundation for cryptocurrencies, blockchain has already changed some of the international financial services landscape, and it is clearly appropriate that the Reserve Bank of New Zealand is exploring the technology's potential. But it's also appropriate to warn against having unreasonable expectations for widespread blockchain use cases, particularly in the near future.

Blockchain technology may well revolutionise large parts of our lives over the next generation. However, that will require first a shared, well-founded understanding of exactly what the technology is suited to, and a clear track record of successful scalable uses.

Acknowledgements

The author thanks Jonathan Boston, an anonymous reviewer, Olga Batura and Marcus Pawson for their insightful comments on drafts of the article, which led to a number of improvements.

References

Ammous, S. (2018) *The Bitcoin Standard: the decentralized alternative to central banking*, Hoboken: Wiley

Baydakova, A. (2019) '$2 billion lost in Mt Gox Bitcoin hack can be recovered, lawyer claims', 13 September, https://www.coindesk.com/2-billion-lost-in-mt-gox-bitcoin-hack-can-be-recovered-lawyer-claims

Berryhill, J., T. Bourgery and A. Hanson (2018) *Blockchains Unchained: blockchain technology and its use in the public sector*, OECD working paper on public governance 28, Paris: OECD Publishing, http://dx.doi.org/10.1787/3c32c429-en

CNBC (2019) 'Google claims its quantum computer solved a 10,000-year problem in seconds', 23 October, www.cnbc.com/2019/10/23/google-claims-successful-test-of-its-quantum-computer.html

Economist (2018) 'Why bitcoin uses so much energy', *Economist*, 9 July, www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy

Halim, S. (2019) 'Learning from the Estonian e-health system', Health.europa.co., 11 January, https://www.healtheuropa.eu/estonian-e-health-system/89750/

Higginson, M., M-C. Nadeau and K. Rajgopal (2019) 'Blockchain's Occam problem', www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem

India Times (2019) 'Uttar Pradesh to become first state to launch blockchain-enabled solar power trading', *India Times,* 29 November, https://energy.economictimes.indiatimes.com/news/renewable/uttar-pradesh-to-become-first-state-to-launch-blockchain-enabled-solar-power-trading/72291409

Kriticos, S. (2019) 'Keeping it clean: can blockchain change the nature of land registry in developing countries?', World Bank 'Let's talk technology' blog post, 29 March, https://blogs.worldbank.org/developmenttalk/keeping-it-clean-can-blockchain-change-nature-land-registry-developing-countries

Kshetri, N. (2018) 'Blockchain-based property registries may help lift poor people out of poverty', 28 June, https://www.govtech.com/computing/Blockchain-Based-Property-Registries-May-Help-Lift-Poor-People-Out-of-Poverty.html

Lanchester, J. (2016) 'When bitcoin grows up', *London Review of Books*, 38 (8), 21 April, https://www.lrb.co.uk/the-paper/v38/n08/john-lanchester/when-bitcoin-grows-up

Notland, J. (2019) 'Smart contract history and law', *Medium*, 27 June, https://medium.com/@jrgensvenneviknotland/smart-contract-history-and-law-9b2f3331d1a

Shen, J. (2016) 'e-Estonia: the power of digital identity', 20 December, https://blogs.thomsonreuters.com/answerson/e-estonia-power-potential-digital-identity/

Smart Dubai Department (2020) *Dubai Blockchain Strategy 2020 Achievements Report*, https://www.smartdubai.ae/knowledge-hub/publications/dubai-blockchain-strategy-2020-achievements-report

Song, J. (2018) 'Why bitcoin is different', *Medium*, 3 April, https://medium.com/@jimmysong/why-bitcoin-is-different-e17b813fd947

Stecklow, S., A. Harney, A. Irrera and J. Kelly (2017) 'Chaos and hackers stalk investors on cryptocurrency exchanges', Reuters, 29 September, https://www.reuters.com/article/us-bitcoin-exchanges-risks-special-repor/special-report-chaos-and-hackers-stalk-investors-on-cryptocurrency-exchanges-idUSKCN1C41AU

Stinchcombe, K. (2018) 'Blockchain is not only crappy technology but a bad vision for the future', *Medium*, 6 April, https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-c1ca122efdec

Swan, M. (2015) *Blockchain: blueprint for a new economy*, Sebastopol: O'Reilly Media

Tapscott, D. and A. (2016) *Bitcoin Revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world*, New York: Portfolio/Penguin

UK Government Chief Science Advisor (2016) *Distributed Ledger Technology: beyond blockchain*, London: Government Office for Science, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

US Customs and Border Protection (2018) *NAFTA/CAFTA Proof of Concept: overview and results*, 28 November, www.cbp.gov/sites/default/files/assets/documents/2019-Oct/Final-NAFTA-CAFTA-Report.pdf

Vial, J. (2018) *Distributed Ledgers and Blockchains: opportunities for Aotearoa New Zealand*, Callaghan Innovation

Woods, J. (2018) 'Blockchain: public sector use cases', *Crypto Oracle*, https://medium.com/crypto-oracle/blockchain-public-sector-use-cases-49a2d74ad946