June 2018

Blockchain technology

by Chris Angus

Over the past few years there has been considerable media and investor attention in Bitcoin and other cryptocurrencies.[1] Generally the challenges of cryptocurrencies are within the purview of the Commonwealth Government: for example, its tax treatment[2] or the development of a digital Australian currency.[3] However, the technology that underpins this and other emerging digital currencies—the 'blockchain'—may become of importance to State Parliaments in the future. Nevertheless, there remains considerable confusion and misunderstanding around blockchain technology. This Snapshot aims to demystify the blockchain and outline its potential uses.

1. What is the blockchain?

In essence, a blockchain is a type of ledger; namely, something that is used to record transactions such as money and property. Ledgers have formed the heart of commerce since ancient times.[4] Currently, ledgers are used for accounting, land title and patent registers.[5] However, the blockchain is a 'distributed ledger', an asset database that is shareable across a network of multiple sites, geographies and institutions.[6]

The Harvard Business Review has argued that blockchain should be viewed as a foundational technology—akin to the TCP/IP architecture that underpins the internet—rather than an innovation in its own right.[7] Separately, the US Congressional Research Service reported that the blockchain is less a single technology and is more a novel way of using existing technologies to enable transactions.[8] Whatever the exact definition, as a base for subsequent technological developments, blockchain technology will require broad coordination and ongoing long term planning for it to realise its full potential.[9]

The terms blockchain and distributed ledger technology (DLT) are often used interchangeably by analysts, although this is not strictly accurate. The difference between the terms are outlined by law firm Allens Linklaters in the box to the right. For the purposes of this Research Snapshot the term 'blockchain' will be used to refer to both blockchain (and associated technology) and DLT.

Distributed Ledger Technology

A digital record (or ledger) of transactions, shared instantaneously across a network of participants.

Blockchain

A technical component of the digital ledger, which refers to the chain of transactions that comprise the ledger.

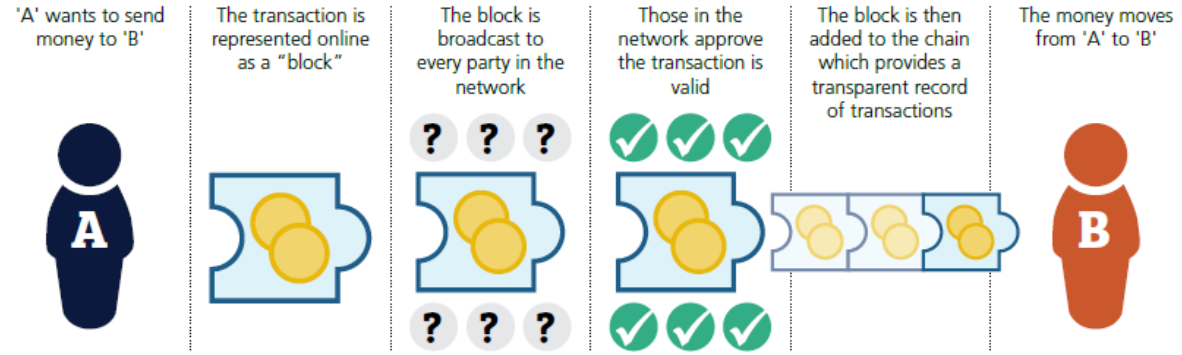
2. How does the blockchain work?

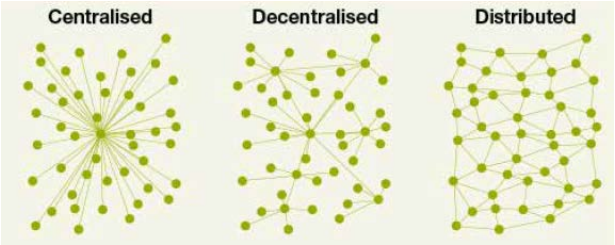
According to the United States' National Association of State Chief Information Officers (NASCIO):

> Blockchain is a shared, global, incorruptible and therefore trusted ledger of economic transactions. It is controlled equally by all who wish to participate and transparent, yet private. Think of it as a steadily growing spreadsheet of records or "blocks" that create an immutable record where each

block is "chained" or linked to the previous block using state-of-the-art cryptography. Each entry recorded is validated and reconciled by all participants in the network to ensure its consistent integrity.[10]

How blockchain works[11]





Unlike centralised or decentralised ledgers (see right)—both of which are maintained by a central authority, such as a government agency—blockchain uses a distributed ledger, with a group of peers responsible for maintaining the integrity of the ledger.[12] This means that a distributed ledger, when combined with cryptographic processes to verify transactions, does not need a 'trusted third party' to oversee and maintain a single version of a blockchain.[13] Zetzsche et al outlined the benefits of distributed ledgers:

> Risks exist [in centralised and decentralised ledgers]. The ledger could be destroyed, or more likely, hacked or otherwise compromised [sic], so that the original data are held for ransom or manipulated and replaced by new (inaccurate) data. … Distributed ledgers address these problems by raising the barriers for manipulation of stored data. Rather than relying on the hub-and-spokes model of centralized ledgers, or the hubs and spokes of decentralized ledgers, in distributed ledgers many data storage points (nodes) are all connected with each other and store all data simultaneously, and together constitute the common ledger. DLT requires consensus of those nodes rather than just the confirmation by one hierarchically structured storage device, as with a centralized ledger.[14]

Blockchains are considered to be immutable—unable to be changed—or at least 'tamper evident'.[15] This is because the distributed nature of the blockchain means that there is no single point of potential failure, while attempts to enter fraudulent data in one location are able to be interpreted as an attack on integrity by other participants and rejected. These characteristics may be of benefit for data recovery and business continuity planning.[16]

Using the example of property records, NASCIO explains how the blockchains' distributed structure could replace a government agency as the 'keeper of truth' for such records:

> In this case, the purchaser of property wouldn't file a deed at the courthouse. Instead, they would commit the updated deed to a blockchain. If enough participants in the blockchain were at consensus that this constituted a valid transaction, then a sale of property and transfer of ownership would be transacted and recorded. Likewise, an interested party wouldn't need to look up a deed at the courthouse in this scenario. They would simply check the blockchain in real time.[17]

Despite this distributed structure, blockchain technology can vary in its degree of centralisation. According to the UK Government Chief Scientific Advisor, blockchains can range from 'unpermissioned' public ledgers open to anyone to more centralised 'permissioned' ledgers that only specific parties can access and modify (see overleaf).[18]

Blockchain technology by level of centralisation[19]

However, the issue of blockchain privacy remains a contested matter, and is discussed further in Part 4 of this Snapshot.

3. Current uses of blockchain technology

Private sector: Although blockchain technology remains in its infancy, a range of users have begun implementing the technology for a variety of purposes. Many of these developments are occurring in the private sector, with examples listed below:[20]

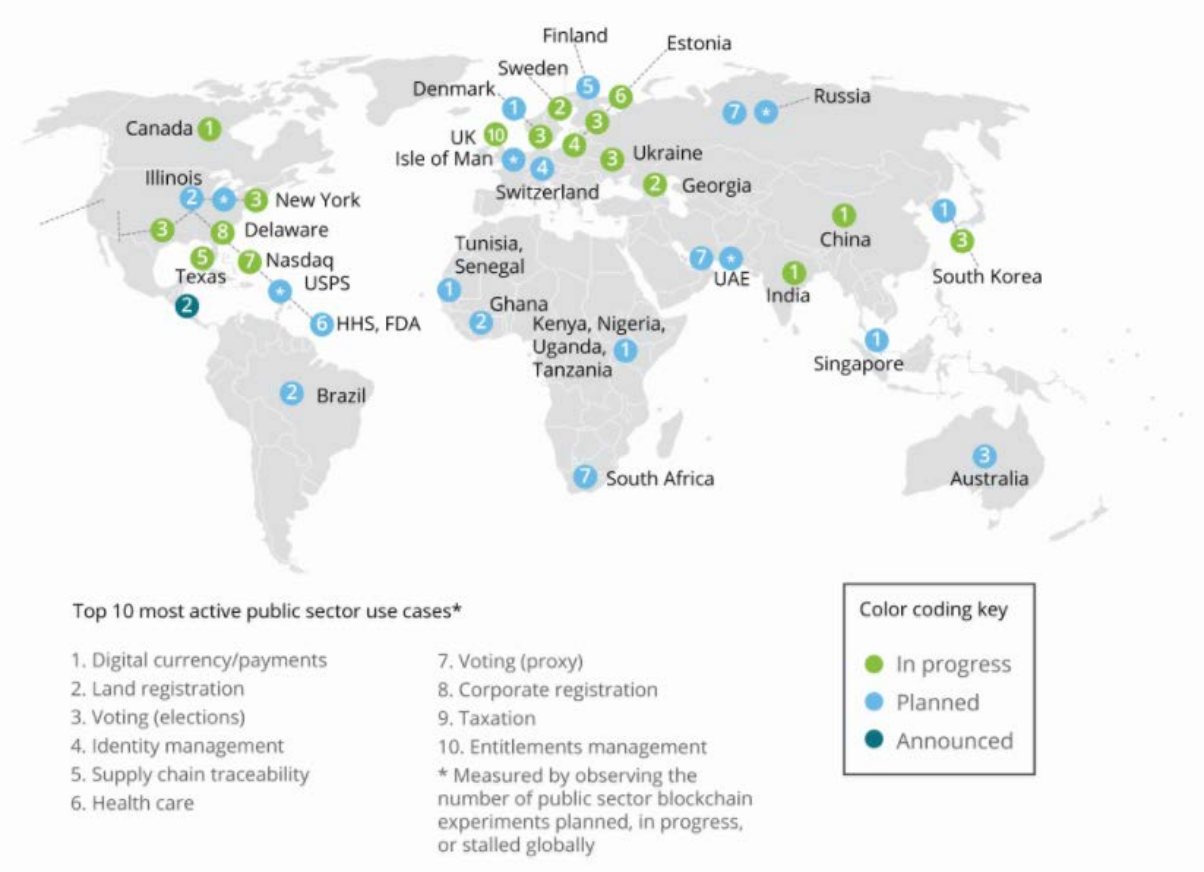
- The Australian Securities Exchange (ASX) intends to replace its Clearing House Electronic Subregister System (CHESS) shareholdings management system with a private distributed ledger;
- International food companies, Nestle, Unilever and Walmart are reportedly planning to use blockchain technology to manage supply chains with greater efficiency;
- The World Wildlife Fund has partnered with a tech innovator and a fishing and processing company to use blockchain technology to combat illegal tuna fishing; and
- A partnership between United Nations agencies and several private sector and not-for-profit companies aims to create a digital identity using a blockchain platform, helping improve citizens' access to education, healthcare, voting, banking and housing.[21]

There is also the prospect of using blockchains to create 'smart contracts'. These contracts contain computer code and can be automatically executed when certain conditions are satisfied, providing cryptographic certainty that an agreement has been honoured in the ledgers, databases or accounts of all parties to the agreement. Potential benefits include low contracting, enforcement, and compliance costs, making it economically viable to form contracts over numerous low-value transactions.[22]

Public sector: Public sector organisations are also exploring opportunities for the use of blockchain technologies, as shown overleaf. In March 2017 Standards Australia developed its *Roadmap for Blockchain Standards Report*, which is designed to identify technical issues with developing blockchains and associated international standards. The report listed key government services that could benefit from improved efficiencies and public access as a result of blockchain technology:

- Land transfers and property title registrations;
- Personal identification and passport documentation;
- Management of health records;
- Vehicle registrations;
- Welfare distribution and monitoring; and
- Public transport scheduling.

Global blockchain use in the public sector, March 2017[23]



Australian developments: The NSW Government has recently started to explore the use of blockchain technology:

- Transport for NSW's 2016 *Future Transport Technology Roadmap* noted the potential of using blockchain technology to enable secure, open loop and open platform payments;
- The NSW Treasury has released the *NSW Government Tender for Banking, Financial and Related Services*, which seeks to make the most of new technologies including blockchain;
- As part of the NSW Government's 2017 *Digital Government Strategy*, $25,000 has been committed to develop ways of authenticating the origin of food products through smart packaging and blockchain technology; and
- In August 2017 the NSW Government announced an $11.4 million agreement with the Commonwealth Government's data innovation group Data61 to address the State's top technology challenges, including how blockchain or other technology can be used to share cyber security information across agencies.

The Commonwealth Government announced in its *2016-17 Budget* that it would "encourage the exploration of Blockchain technology, including through a study and pilot testing by the CSIRO's Data61".[24] In January 2017 the Commonwealth Bank issued a 'cryptobond' for Queensland Treasury Corporation using its capital markets blockchain platform: the world's first blockchain bond issuance by a government entity. Meanwhile, the Perth Mint in Western Australia announced in January 2018 that it would use blockchain technology to trace gold from mine site to processing and end consumer.

There may be scope for creating electronic voting systems using blockchain. In its submission to the 2016 Victorian Government's *Inquiry into electronic voting*, Australia Post outlined how blockchain technology could underpin an effective, secure e-voting system:

> We envisage a vote being an electronic transaction whereby a number of voting "credits" can be "spent" by the voter to attribute preferences. Permission to vote would be secured through the use of secure digital access keys sent securely to each voter. A ballot would be cryptographically represented within the blockchain, with each vote linked to the voter through their preference choice stored within the blockchain in a way that anonymises and protects that information from being publically accessible. Once the election closes the system would simply compile the results from the database. The votes will be verifiable by candidates and voters, while preserving the secrecy of the ballot through a combination of key encryption and digital signatures implemented within the voting solution.[25]

International developments: Turning overseas, the Victorian Parliamentary Research Service has listed uses of blockchain by public entities, including a pilot program announced by the Canadian Government to use blockchain to increase transparency in recording government grants, and a Swedish government-private sector joint venture in which land ownership and sales records will be transferred to a blockchain.

There have also been a number of legislative developments to try and pre-empt possible future challenges that could arise from increasing use of the blockchain for public and private purposes, primarily in the United States. In 2015, Vermont became the first state to address blockchain in legislation when it directed a number of government agencies to report to the State's General Assembly on opportunities and risks of creating a presumption of validity for electronic facts and records that employ blockchain. The following year the Vermont General Assembly created evidentiary standards to determine the authenticity of records using blockchain technology.[26] As of 2017, four other States—Arizona, Delaware, Illinois and Nevada—have since enacted or adopted blockchain legislation, including the following:[27]

- **Arizona:** Established guidelines for electronic signatures and records using blockchain technology;
- **Delaware:** Provided statutory authority for corporations formed in Delaware to use blockchain to create and maintain corporate records;
- **Nevada:** Recognised blockchain technology as a type of electronic record for the purposes of the Uniform Electronic Transactions Act, which establishes the legal equivalence of electronic records and signatures with paper writings and manually-signed signatures.[28]

In advice to US state governments, NASCIO noted that the business and technology of blockchain will continue to evolve in time, including lessons learned, best practices, standards, legislation and regulation. With this in mind, it made the following early stage recommendations for government's use of blockchain:

1) Begin research of blockchain technology and economics now so states can begin to grow their knowledge.
2) Given this basic knowledge, begin to explore some potential use cases to better understand how blockchains may disrupt or enable your organization.
3) Consider developing a preliminary strategy on how you could adopt blockchain technology for future use.
4) Create a state stakeholder group (from both business and technology) to inform the preliminary strategy.
5) Identify relevant use cases to harvest the benefits of blockchain technology for your organization.[29]

4. Risks and shortcomings

Despite the opportunities available with blockchain, there remain uncertainties and concerns with the technology. Much of this is a result of blockchain being only a recent innovation; for example, the World Economic Forum, which although identifying blockchain as one of 12 key emerging technologies, warned that some technological risks may only become apparent once blockchain is used on a wider scale.

Privacy issues presents a key challenge for both innovators and policymakers. Zetzsche et al have commented that Bitcoin's blockchain can reveal significant information about people's profiles, allowing for re-personalisation of pseudonymous data.[30] Additionally, blockchain's immutability means that data, once stored on the ledger, cannot be erased; this could seriously affect the privacy of individuals.[31] Rountree noted possible legal tensions between Australian privacy legislation and the operation of this technology:

- Personal information may only be used and disclosed for certain purposes relating to its collection. However, in many versions of blockchain, all users can potentially access data stored across various distributed copies of the chain.
- Reasonable efforts must be taken to update inaccurate or out-of-date information. However, information which is recorded on a blockchain exists in perpetuity and is generally unalterable.
- Obligations in the Privacy Act apply to entities which 'hold' or 'collect' personal information. However, all entities who are party to a distributed ledger effectively hold a copy of the information. This raises questions as to which obligations apply to whom.[32]

It is possible that these risks could be reduced if private permissioned ledgers were used—as the ledger's owner can enforce rules on who is and is not allowed to use the system—or that newer blockchain technology could be developed with higher levels of privacy.[33] However, Zetzsche et al argue that even permissioned ledgers risk being compromised by a cyberattack,[34] while Allens Linklaters contend that any governance framework for permissioned ledgers must address correction of errors and reversing transactions in response to these risks.[35]

Another major shortcoming is the lack of knowledge about how to deal with failures in the use of blockchain systems. Data61 has reported that, to date, most existing proof of concept blockchain-based system deployments only demonstrate 'sunny day scenarios' where no error or exception occurs. The agency has recommended that future trials demonstrate responses to 'rainy day scenarios' arising from both anticipated and unanticipated problems with these systems.[36]

Specific blockchain innovations may only have limited use in practice. For example, Rountree argues in regard to smart contracts that complex or ambiguous outcomes are not suited as smart contracts, or may not even be capable of expression in software language,[37] while Data61 noted that there remains debate over whether it is possible for smart contacts to be considered legal contracts.[38] There are also questions regarding the practical benefits of blockchain technology. Allens Linklaters warned that innovation will likely require substantial upfront investment, yet may only lead to modest efficiencies.[39] Deloitte commented similarly, noting that existing systems may be preferred by stakeholders for a number of reasons:

> There are a number of scenarios where a distributed ledger appears to be superior to a central ledger. What is not clear is which of these scenarios will be economically viable. As with all technology adoption, there is a cost-benefit tradeoff to be made, and in each case it's not enough for the distributed ledger to be cheaper to build and operate than the existing central ledger, it must be cheaper than the incremental cost of improving the existing ledger. A number of these scenarios will also necessarily require multiple stakeholders to agree on the change, something that might be too challenging politically in some instances.[40]

Other commentators are even more critical, claiming that the blockchain is "one of the most overhyped technologies ever", and is slower and less energy-efficient than existing ledger technology. Currently, the extent to which blockchain may impact on the way society operates in the future is unknown. Further analysis, testing and evaluation are the only means of identifying what aspects of the technology, if any, could greatly benefit government and society.

5. Conclusion

Both the public and private sectors have a growing interest in the blockchain and its potential for greater efficiencies, security and transparency compared to existing ledger technology. Nevertheless, the adoption of blockchain technology may bring with it a range of issues, including the risk of privacy breaches, security concerns, and legal uncertainties in relation to applications such as smart contracts.

References

[1] See the following examples from the Australian media: Verrender I, Bitcoin: What the bubble tells us about ourselves, *ABC News*, 11 December 2017; Quiggin J, Bitcoin's zero-sum game, *Inside Story*, 24 January 2018; Eyers J, RBA governor Philip Lowe says bitcoin is a 'speculative mania', *Australian Financial Review*, 13 December 2017.

[2] Australian Taxation Office, *Tax treatment of cryptocurrencies*, 16 March 2018 [accessed 21 May 2018]. For a summary of the constitutional background to the issue of taxation, see Griffith G, *The Future of State Revenue: the High Court Decision in Ha and Hammond*, Briefing Paper 16/97, September 1997, NSW Parliamentary Research Service, Ch 2.

[3] Lowe P, *An eAUD?*, speech delivered at the 2017 Australian Payment Summit, Sydney, 13 December 2017; *Commonwealth of Australia Constitution Act* (Cth) s 51(xii).

[4] UK Government Chief Scientific Advisor, *Distributed Ledger Technology: beyond block chain*, 19 January 2016, p 5.

[5] Data61, *Distributed Ledgers: Scenarios for the Australian economy over the coming decades*, May 2017, p 2.

[6] UK Government Chief Scientific Advisor, note 4, p 5.

[7] Iansiti M and Lakhani K, The Truth About Blockchain, *Harvard Business Review*, January-February 2017, p 10.

[8] Jaikaran C, *Blockchain: Background and Policy Issues*, 28 February 2018, Congressional Research Service, p 11.

[9] Iansiti and Lakhani, note 7.

[10] National Association of State Chief Information Officers , *Blockchains: Moving Digital Government Forward in the States*, May 2017, p 2.

[11] Morton H, Blockchain Technology: An Emerging Public Policy Issue, *National Conference of State Legislatures*, Vol 25(44), November 2017, p 1.

[12] Evans-Greenwood P and Harper I, *Bitcoin, Blockchain, and Distributed Ledgers: What questions should we be asking?*, Deloitte Australia, p 12; UK Government Chief Scientific Advisor, note 4, p 36.

[13] Reserve Bank of Australia, *Submission to the Inquiry into Digital Currency*, Senate Economics References Committee, November 2014, p 4.

[14] Zetzsche T, Buckley R and Arner D, The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, *University of New South Wales Law Research Series*, 2017, 52, p 10-11.

[15] Data61, note 5, p 62.

[16] Ibid; Hoser T, Blockchain basics, commercial impacts and governance challenges, *Governance Directions*, 2016, 10, p 609.

[17] NASCIO, note 10, p 3.

[18] UK Government Chief Scientific Advisor, note 4, p 7, 35.

[19] Ibid p 35.

[20] Also see Graham M, Dosen I, *Cryptocurrency and blockchain explained*, Victorian Parliamentary Library & Information Service, No 2, February 2018, p 3-4.

[21] OECD, *Embracing Innovation in Government: Global Trends 2018*, p 22.

[22] UK Government Chief Scientific Advisor, note 4, p 18, 24.

[23] White M, Killmeyer J, Chew B, Will blockchain transform the public sector? Blockchain basics for government, *Deloitte Insights*, 11 September 2017.

[24] Commonwealth Government, *Budget 2016-17 Overview*, May 2016, p 12.

[25] Australia Post, *Response to Victorian Parliament's Electoral Matters Committee On Electronic Voting*, 1 July 2016, p 5.

[26] Morton, note 11, p 2.
[27] Ibid. See also: Berns J, Berns C and Civalleri J, State Lawmakers Increasing Their Focus on Virtual Currency and Blockchain Technology, *BernsWeiss LLP*, June 2017.
[28] Uniform Law Commission, *Electronic Transactions Act*, 2018 [accessed 7 May 2018].
[29] NASCIO, note 10, p 7.
[30] Zetzsche et al, note 14, p 14-15
[31] Data61, note 5, p 21.
[32] Rountree D, Technology and contracts: Navigating the blockchain and the law, *Law Society of NSW Journal*, 2016, 26, p 73.
[33] UK Government Chief Scientific Advisor, note 4, p 10, 35; NASCIO, note 10, p 5.
[34] Zetzsche et al, note 14, p 16
[35] Allens Linklaters, *Blockchain Reaction*, June 2016, p 20.
[36] Data61, *Risks and opportunities for systems using blockchain and smart contracts*, May 2017, p 38.
[37] Rountree, note 32, p 74.
[38] Data61, note 36, p 4.
[39] Allens Linklaters, note 35, p 10.
[40] Evans-Greenwood and Harper, note 8, p 45.

ISSN 1838-0204