



Quick Guide



Cryptocurrency and blockchain explained

No. 2, February 2018

Michael Graham
Research Assistant
Igor Dosen
Research & Inquiries Officers
Parliamentary Library & Information Service

Acknowledgments

The authors would like to thank Debra Reeves, Caley Otter, Marianne Aroozoo, Alice Petrie, Bella Lesman and Jon Breukel for their help in the preparation of this paper.

ISSN 2204-4779 (Print) 2204-4787 (Online)

Research Note: No. 2, February 2018.

© 2018 Parliamentary Library & Information Service, Parliament of Victoria

Research Notes are produced by the Parliamentary Library's Research & Inquiries service. They provide analysis on selected components of new Bills and topical issues in response to, and in anticipation of, the needs of Members of the Victorian Parliament.

This research publication is current as at the time of printing. It should not be considered a complete guide to the particular subject or legislation covered. While it is intended that all information provided is accurate, it does not represent professional legal opinion. Any views expressed are those of the author(s).

Some hyperlinks may only be accessible on the Parliament of Victoria's intranet. All links are current and available as at the time of publication.

What is cryptocurrency?

There has been significant media attention focused on cryptocurrency in recent months. In January 2018, the *Australian Financial Review* published an editorial on the link between cryptocurrency and interest rates.¹ South Korea has announced plans to regulate cryptocurrencies.² Estimates differ, but at the time of writing recent data puts the total market capitalisation of cryptocurrencies around the world at USD 507 billion (close to half of Australia's GDP in 2016).³ It is an issue that is gaining attention not only in the media, but also at the level of policy.

One of the key issues at the centre of all this attention is the question of the 'real value' of cryptocurrencies. This is another way of asking: what is cryptocurrency?

In the simplest terms, cryptocurrency is a digital token which represents value. The first cryptocurrency, Bitcoin, was assigned value which represented currency. This occurred for a range of factors, including: its underlying cryptographic technology, the way it could facilitate anonymous trades and the fact that it is purely digital (factors which are explained below). Since Bitcoin launched in 2009, many other cryptocurrencies have emerged, all of which represent and are assigned different units of value.

In the sense that cryptocurrency is a digital token, it is similar to our fiat money⁴ system in that the actual units traded have no intrinsic worth—when we trade cash for goods and services, cash represents trust in a financial

system of ascribing value which can then be traded or exchanged. Cryptocurrencies differ, however, in that fiat money is backed by governments while cryptocurrencies are not. The 'value' therefore derives from what buyers and sellers in the market are willing to pay for the cryptocurrencies, rather than the value deriving from a centralised governmental regulator.

Cryptocurrencies have different values as buyers and sellers in the marketplace buy and sell them for different prices. Some people are entering these new markets in the shared belief that cryptocurrencies will retain value in the future, allowing them to be on-sold at a profit. Other traders may enter the market hoping to use cryptocurrencies to exchange for goods and services. Inherent in the hopefulness of this activity is the idea that 'investment' in many cryptocurrencies is more akin to pure speculation.⁵ There are exceptions, however: a Melbourne man recently announced he would accept part payment in Bitcoin for a house valued at AUD 2.5 million.⁶

Observers have argued that cryptocurrency is a 'bubble', referring in particular to Bitcoin. To the extent that cryptocurrencies are speculative, these views are founded. They are also founded in the sense that Bitcoin is more accurately a token, as opposed to a 'currency'. To become a currency would require Bitcoin to be accepted as legal tender for public and

¹ (2018) 'Bitcoin fuelled by cheap money boom', *Australian Financial Review*, 17 January.

² S. Gibbs (2011) 'Bitcoin and Ethereum tumble after renewed fears of regulatory crackdown', *The Guardian*, 17 January.

³ Coinmarketcap (2018) 'Cryptocurrency Market Capitalizations', 31 January, coinmarketcap website.

⁴ Fiat money refers to a currency that is not backed by a physical commodity and thus does not have

any intrinsic value. The value of the currency comes from the backing of a government and the stability of the economy it belongs to. Almost all paper and coin currencies in use today are fiat money.

⁵ Mr Money Moustache (2017) 'So you're thinking about investing in bitcoin? Don't', *The Guardian*, 15 January.

⁶ M. Cranston (2017) 'First Victorian home ready to accept bitcoin as \$2.5m sale payment', *Australian Financial Review*, 28 November.

private debts.⁷ It would also require a mechanism which would allow for value to remain stable, so that prices for goods and services could be stable.⁸ Some industries are already taking some of these steps. In a world-first in 2015, 'titcoin' was recognised as a formally accepted unit of exchange by a major industry trade organisation (in this case, the Adult Entertainment Industry).⁹

Despite these exceptions, most cryptocurrencies in their current forms are inherently speculative. But if cryptocurrency is generally so speculative, why have people invested hundreds of billions of dollars into these markets? As above, part of the answer is most likely to do with the underlying technology, known as blockchain.

What is blockchain?

Blockchain is an open-sourced computer protocol which allows for users to transact, peer-to-peer. It decentralised, public and digital, effectively making it a 'transaction-recording database' stored on many different computers at once.¹⁰

The technology confirms the legitimacy of trades in real time, using cryptography (hence *cryptocurrency*), which authorises trades based on building 'blocks'. Blocks are built by 'mining', a process in which computers are tasked with solving complex and random cryptography.

As more miners attempt to build blocks, the faster the blocks are built and the blockchain becomes more secure. This is because to undo or alter a block, more miners would have to be

allocated to that task than the task of building new blocks.

In other words, in order to defraud the blockchain, more computing power must be allocated to defrauding the blockchain than the amount of total computing power working on the blockchain. This would be an enormous feat: in 2014, a study found that electricity consumption of the Bitcoin blockchain was roughly equivalent to that of Ireland.¹¹

Blockchains can be conceptualised as 'distributed ledgers' of trades. Each blockchain is a different ledger which has the potential to record any trade of information. The ledger is highly secure in that: it is stored on many different devices in many locations, reducing the risk of corrupting the database; it is based on complex cryptography, reducing the risk of fraud, and; it has the potential to verify trades instantaneously, leading to huge increases in efficiency in managing and storing information.

Along with being a digital token, Bitcoin refers to one ledger of over a thousand blockchains or ledgers. Bitcoin therefore describes a system of exchange. Because Bitcoin is a cryptocurrency, it also describes the monetary value which is ascribed to those exchanges. This is not always the case: while all blockchains use tokens to represent trades or information, not all tokens are used to represent currency (see below).

Returning to the blockchain, traders can be either anonymous or named, depending on the way that each particular blockchain is set up.¹² As above, the cryptography used to confirm the validity of trades means it is difficult to succeed in making fraudulent trades. This allows for users to trade even when they do not trust each other; when they do not know one another's identities, or; when they do not have

⁷ Mr Money Moustache (2017) op. cit.

⁸ Ibid.

⁹ Titcoin (2018) 'Titcoin Digital Currency: The Official Cryptocurrency [sic] of the Adult Industry', Titcoin Development Group.

¹⁰ N. Kshetri (2017) 'Can blockchain technology help poor people around the world?', *The Conversation*, 1 May.

¹¹ F. Filpo & M. Berne (2017) 'The bitcoin and blockchain: energy hogs', *The Conversation*, 17 May.

¹² For example, Monero offers 'anonymous' trading. See: Monero (2017) 'Monero: Private Digital Currency'.

the time to themselves verify the legitimacy of trades.

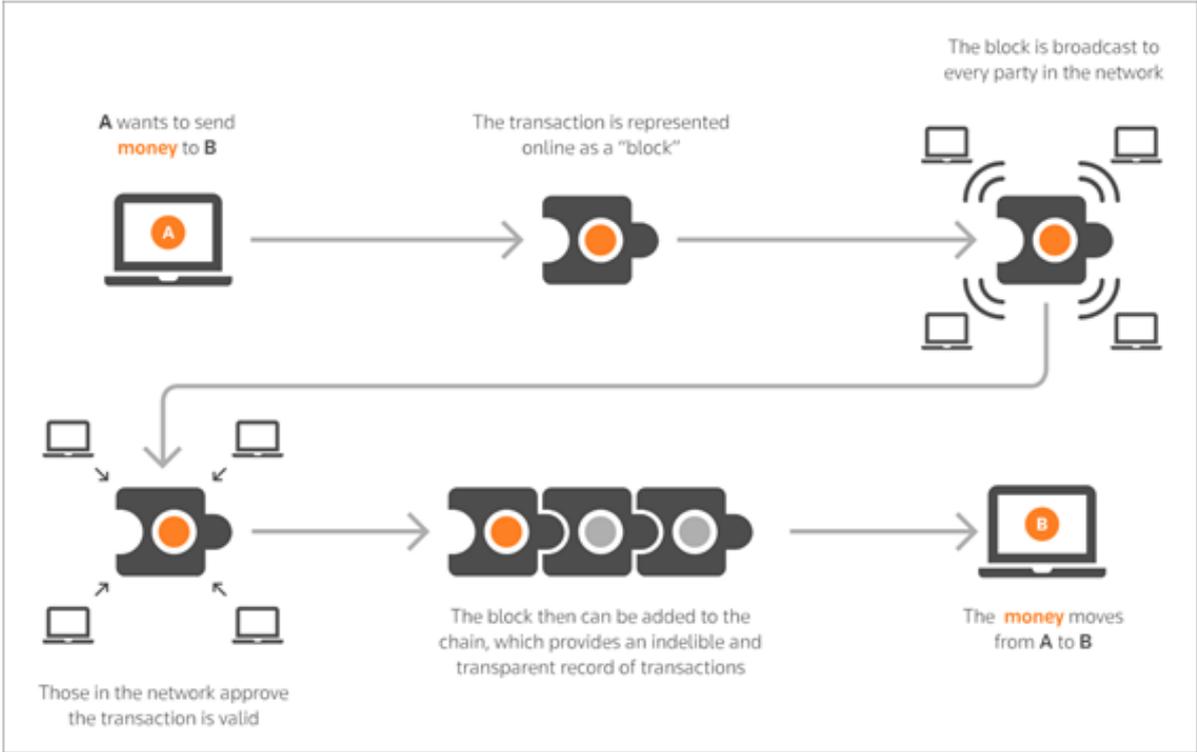
This is significant in that blockchains can be set up so that trades are completed only when certain conditions are fulfilled. These particular blockchains enable 'smart contracts', which can be used in situations such as a life insurance policy which is managed by a blockchain to pay the beneficiary only when a doctor submits a digitally signed death certificate to the blockchain.¹³ In that instance, the token used would not represent currency, but would represent the completion of the trade of information and the storage of that information on the ledger of transactions, the

used as a currency, blockchain also removes the need for a centralised authority which authorises and regulates the value of the unit of trade, like the Federal Reserves used to regulate fiat currency.

In a currency context, this offers the potential for greater efficiency and freedom for people to trade as they wish. However, third parties such as banks are leading research into the ways in which some services will still be required to be performed by third parties to make transactions.¹⁴

Figure 1 depicts the way in which blockchain could record a transaction of money:

Figure 1. How blockchain technology works



Source: Thomson Reuters, 'Blockchain'.

insurer's blockchain.

In the cryptocurrency context, the peer-to-peer nature of the technology has a libertarian application in that the blockchain removes the need for an intermediary which authorises and regulates individual trades, like a bank. When

Other businesses already utilise blockchain in data management. For example, Nestlé, IBM and Walmart have implemented blockchain in order to manage supply chains with increased

¹³ N. Kshetri (2017) op. cit.

¹⁴ S. Gilder (2017) 'Early blockchain experiments point to jobs of the future', *Commonwealth Bank of Australia*, 29 November.

efficiency and to detect and mitigate against food contamination.¹⁵

Another group in the USA is using blockchain to help low-income people to pay bail at court.¹⁶ An Australian start-up, backed by the United Nations, has announced plans to use blockchain to improve democratic processes like voting.¹⁷

Other applications are in 'responsible' journalism, which will use blockchain to create a decentralised community of writers, fact-checkers and funders to create unbiased, 100 per cent verified stories.¹⁸ Blockchain is also being used in a new pilot program which aims to combat illegal fishing of tuna.¹⁹ Commonwealth Bank of Australia has been using a blockchain to store government bonds for over a year.²⁰ These new applications are using blockchain due to its transparency and traceability.²¹ In a 2015 report, the World Economic Forum predicted that ten per cent of the world's data will be stored using blockchain technology by 2027.²²

Public entities are also turning to the technology. The Canadian Government has

recently announced a pilot which will use blockchain to increase transparency in recording government grants.²³ In 2016, a Swedish business partnered with the Swedish Land Registry to trial a pilot which seeks to put land ownership and sales onto a blockchain.²⁴ The same company is investigating the potential for applying a blockchain to government activity in Andhra Pradesh, India, to reduce fraud and data management errors.²⁵

It is difficult to estimate the market capitalisation of cryptocurrencies in Australian 'exchanges', or cryptocurrency markets. It remains to be seen as to whether any cryptocurrencies will become recognised by governments as legal tender.

The 'value' of blockchain technology is easier to approach in that the technology has real applications, some of which have been listed above. The software is interesting in that it has the potential to disrupt information management and data security systems as we know them. The applications of the technology are many and varied.

¹⁵ R. Browne (2017) 'IBM partners with Nestle, Unilever and other food giants to trace food contamination with blockchain', *CNBC*, 4 October.

¹⁶ Bail Bloc (2018) 'Bail Bloc is a cryptocurrency scheme against bail', *The New Inquiry*.

¹⁷ Horizon State (2018) 'Redesigning democracy for the 21st century', *Horizon State*.

¹⁸ Civil (2017) 'What if the news were run by the people?'; Decentralised News Network (2017) 'News by the people, for the people.'

¹⁹ C. Visser & Q. Hanich (2017) 'How blockchain is strengthening tuna traceability to combat illegal fishing', *The Conversation*, 22 January.

²⁰ J. Evers (2017) 'Commonwealth Bank puts government bonds on a blockchain', *Australian Financial Review*, 24 January.

²¹ C. Visser & Q. Hanich (2017) op. cit.

²² World Economic Forum (2015) 'Deep Shift—Technology Tipping Points and Societal Impact', September, p. 24.

²³ N. De (2018) 'Canadian Research Body Pilots Ethereum in Transparency Push', *Coindesk*, 22 January.

²⁴ ChromaWay (2017) 'Cases: Future house sales'; Lantmäteriet, ChromaWay & Kairos Future (2016) 'The Land Registry in the blockchain', July.

²⁵ ChromaWay (2017) op. cit.

References

- (2018) 'Bitcoin fuelled by cheap money boom', *Australian Financial Review*, 17 January.
- Bail Bloc (2018) 'Bail Bloc is a cryptocurrency scheme against bail', *The New Inquiry*.
- Browne, R. (2017) 'IBM partners with Nestle, Unilever and other food giants to trace food contamination with blockchain', *CNBC*, 4 October.
- ChromaWay (2017) 'Cases: Future house sales'.
- Civil (2017) 'What if the news were run by the people?'.
- Coinmarketcap (2018) 'Cryptocurrency Market Capitalizations', 31 January, coinmarketcap website.
- Cranston, M. (2017), 'First Victorian home ready to accept bitcoin as \$2.5m sale payment', *Australian Financial Review*, 28 November.
- De, N. (2018) 'Canadian Research Body Pilots Ethereum in Transparency Push', *Coindesk*, 22 January.
- Decentralised News Network (2017) 'News by the people, for the people.'
- Eyers, J. (2017) 'Commonwealth Bank puts government bonds on a blockchain', *Australian Financial Review*, 24 January.
- F. Filpo & M. Berne (2017) 'The bitcoin and blockchain: energy hogs', *The Conversation*, 17 May.
- Gibbs, S. (2011) 'Bitcoin and Ethereum tumble after renewed fears of regulatory crackdown', *The Guardian*, 17 January.
- Gilder, S. (2017) 'Early blockchain experiments point to jobs of the future', *Commonwealth Bank of Australia*, 29 November.
- Horizon State (2018) 'Redesigning democracy for the 21st century', *Horizon State*.
- Kshetri, N. (2017) 'Can blockchain technology help poor people around the world?', *The Conversation*, 1 May.
- Lantmäteriet, ChromaWay & Kairos Future (2016) 'The Land Registry in the blockchain', July.
- Mr Money Moustache (2017) 'So you're thinking about investing in bitcoin? Don't', *The Guardian*, 15 January.
- National Australia Bank Group Economics (2017) 'State Economic Handbook: October 2017', October, NAB.
- Titcoin (2018) 'Titcoin Digital Currency: The Official Cryptocurrency [sic] of the Adult Industry'.
- Visser, C. & Q. Hanich (2017) 'How blockchain is strengthening tuna traceability to combat illegal fishing', *The Conversation*, 22 January.
- World Economic Forum (2015) 'Deep Shift—Technology Tipping Points and Societal Impact', September.

Research & Inquiries Service

Research Notes are produced by the Parliamentary Library's Research & Inquiries service. They provide analysis on selected components of new Bills and topical issues in response to, and in anticipation of, the needs of Members of the Victorian Parliament.

This research publication is current as at the time of printing. It should not be considered a complete guide to the particular subject or legislation covered. While it is intended that all information provided is accurate, it does not represent professional legal opinion. Any views expressed are those of the author(s).

Some hyperlinks may only be accessible on the Parliament of Victoria's intranet. All links are current and available as at the time of publication.

Enquiries:

Jon Breukel
Coordinator, Research & Inquiries
Victorian Parliamentary Library & Information Service
Parliament House
Spring Street, Melbourne
Telephone (03) 9651 8633
www.parliament.vic.gov.au