Cryptocurrency: Ten Years On

Cameron Dark, David Emery, June Ma and Clare Noone[*]

Photo: KTSDesign/Science Photo Library – Getty Images

Abstract

Ten years on from the creation of Bitcoin, the term 'cryptocurrency' has entered the public consciousness. Despite achieving some name recognition, cryptocurrencies are not widely used for payments. This article examines why Bitcoin is unlikely to become a ubiquitous payment method in Australia, and summarises how subsequent cryptocurrencies have sought to address some of the shortcomings of Bitcoin – such as its volatility and scalability problems. It also examines the proliferation of new 'coins' and concludes that, despite the developments in cryptocurrencies, none are currently functioning as money in the economy.

Introduction

On 3 January 2009, the first bitcoins were created.[1] Ten years on the terms 'bitcoin' and 'cryptocurrency' are widely known. 'How to buy bitcoin' was the third-ranked 'How to …' search term in Google in 2017 (Google 2018), alongside significant growth in fraudulent and phishing spam mail related to cryptocurrencies (Kaspersky Lab 2018). However, neither Bitcoin nor the many thousands of cryptocurrencies that have followed have become widely used for payments. People are more likely to view cryptocurrencies as a speculative high-risk investment class than a payment system. In this article, we look back over the decade since the launch of Bitcoin. We examine how cryptocurrencies have changed over that period in an attempt to address some of the shortcomings of Bitcoin as a payment system – such as its volatility and scalability problems.[2] We also describe the development of 'programmable' cryptocurrencies. Despite these changes, we see little likelihood of a material take-up of cryptocurrencies for retail payments in Australia in the foreseeable future.[3]

What is Cryptocurrency?

One definition of cryptocurrency is that it is a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a national currency, but is designed to be accepted by some parties as a means of payment and can be transferred, stored or traded electronically.[4] Cryptocurrencies use computer software running across a network and rely on various established cryptographic techniques (hashing, digital signatures or one-way cryptographic functions) to control access and verify transactions. They use some form of 'consensus mechanism' to validate transactions; that is, a mechanism to achieve agreement across the network on whether a transaction is valid or not.

The technology underlying cryptocurrencies is often referred to as distributed ledger technology (DLT).[5] Given this, cryptocurrency is sometimes described as a 'digital token' on a distributed ledger that can be used to exchange value and thereby facilitate payments. DLT platforms vary in many ways, including: who can see and/or keep a copy of the ledger, who can update the ledger, what information is required to verify a transaction on the ledger, and how tokens are created and distributed. Another way in which DLT platforms can differ is in how the data on the platform is structured; blockchain refers to one way of structuring the data. Blockchain and alternative methods are discussed later in the article.

In recent years, other types of DLT-based digital tokens have been designed and launched. Some have characteristics that are similar in some respects to securities (such as shares or bonds) and others are tokens that can be redeemed for access to a specific product or service (that is often to be provided using DLT). These are often referred to as 'security tokens' and 'utility tokens', respectively. Together cryptocurrency, security tokens and utility tokens are commonly referred to as 'crypto-assets'. It should be noted that, while commonly used, these terms can be misleading. For example, 'currency' is often thought as being synonymous with money. However, no cryptocurrencies currently have the key attributes of money; and similarly, many crypto-assets have been found to fall well short of the definition of an asset as 'a useful thing or quality' (Macquarie Dictionary 2019).[6]

Cryptocurrencies (and crypto-assets more broadly) can enter circulation in a variety of ways. As described more fully below, in the case of Bitcoin, new bitcoins are created and paid out as a reward for participants of the system validating transactions. In other cases, new cryptocurrency units may be simply (and potentially arbitrarily) created by the controller of the protocol and sold (potentially via an initial coin offering) or given away for free (typically as a marketing exercise to broaden awareness of their coin). Cryptocurrency exchanges facilitate the buying and selling of cryptocurrencies in the secondary market. However, not all cryptocurrencies are listed on exchanges, or indeed have any market value.

The First Generation of Cryptocurrencies

Proposals for electronic versions of cash had been made and trialled at various points in the late 20th century, without success in practice.[7] Bitcoin, which launched in 2009 following the publication of a paper by an unknown author or authors in 2008, combined a series of existing technologies to provide a peer-to-peer version of electronic cash (Nakamoto 2008). Box A provides a high-level description of some of the basics of Bitcoin.

Box A
Bitcoin Basics[8]

Bitcoin has a 'blockchain' of transactions. The 'ledger', or record of changes in ownership, consists of 'blocks' of information linked together in chronological order (a 'chain'). Every 10 minutes on average, the Bitcoin blockchain is updated to include a new block of transactions. Addresses (or ownership) on the ledger are in terms of alphanumeric pseudonyms rather than legal names.

Most conventional payment methods – cash is the obvious exception – rely on some central party to keep and update the ledger or record of holdings. For example, the Reserve Bank maintains the ledger of commercial banks' Exchange Settlement Account holdings. And commercial banks maintain records of their customers' deposits. By contrast, Bitcoin and other cryptocurrencies rely on a distributed ledger. The Bitcoin ledger (the blockchain) is replicated across the 'nodes' (i.e. computers) connected to the network. The idea is that each of the nodes ends up with an identical copy of the latest version of the ledger.

If a ledger is open to participation by any party, and any party can propose changes to the ledger, it is known as a public (or 'unpermissioned' or 'trustless') ledger. Bitcoin and many other cryptocurrencies are examples of trustless distributed ledgers. The user does not need to know or trust any party on the network but, in effect, needs to trust the algorithm and the cryptography used. This allows parties who do not necessarily trust each other to transact without the need for an intermediary.

The security of the Bitcoin system relies on public/private-key cryptography. The transaction verification methodology is referred to as 'proof of work'. Participants in the system (or 'miners' as they are known) compete to successfully verify (by solving computationally intensive calculations for) a new block of transactions, with each block consisting of around 2,500 transactions at the time of writing. The first miner to do so earns a reward of newly 'mined' coins, currently set at 12½ bitcoins (currently, worth around US$100,000). The successful miner also earns any transaction fees offered by the people initiating the transactions contained in that block.

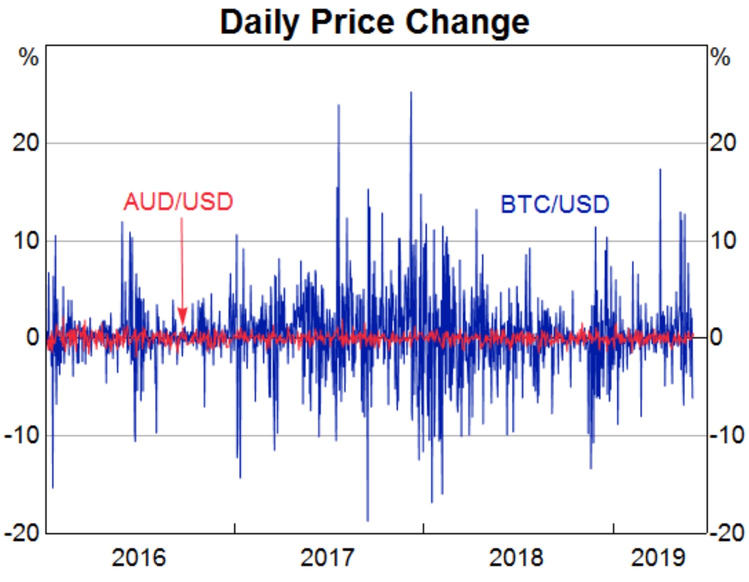
Bitcoin demonstrated that, under certain assumptions, information about transactions could be verified and relied upon without the need for a trusted central party. The possibility of transactions being recorded securely on a distributed basis led to considerable interest in Bitcoin and other potential implementations of DLT.

While Bitcoin remains the most prominent cryptocurrency, a large number of alternative cryptocurrencies and digital tokens have been created in recent years. Some are essentially replicas of Bitcoin, while others seek to introduce additional functionality or have different design features. For example, Litecoin adopts most of the features of Bitcoin but has a shorter block confirmation time of around 2½ minutes and uses an alternative hashing algorithm. Dogecoin, initially created as a novelty currency, gained use for various crowd-sourced fundraising efforts.

As identified by Nakamoto, the purpose of Bitcoin was to act as a peer-to-peer payment mechanism. In practice, its use for this function has been limited. However, it has seen significant use as a vehicle for speculation. This was particularly the case in late 2017 when there was a very considerable increase in the price of bitcoin, along with most other cryptocurrencies. Media reports of these price increases generated further speculative interest, with many buyers unlikely to have had familiarity with cryptocurrencies other than what they had heard or seen in the media or from acquaintances. Following this speculative episode, prices fell dramatically from their peaks, leaving many purchasers of cryptocurrencies with capital losses.

Economic definitions of money typically reference three key features: a means of payment, unit of account, and store of value. Assessments of whether Bitcoin and other cryptocurrencies meet this definition usually conclude that they do not (Ali *et al* 2014; RBA 2014). Bitcoin's very significant fluctuations in price mean that it is a poor store of value (Graph 1). In part reflecting this price volatility, it is not used as a unit of account: goods and services sold for bitcoin are nearly always priced in some national currency, with the amount of bitcoin required to be delivered varying as its price changes. While Bitcoin and other cryptocurrencies can act as a means of payment, they are not widely used or accepted due to a number of shortcomings.

Graph 1



Sources: Coinmarketcap.com; RBA

There are strong network effects in payments: use and acceptance of payment methods are generally self-reinforcing – as can be seen from the rapid adoption of contactless card payment by both merchants and cardholders. A failure to generate network effects can mean that payment methods become, or remain, niche. In this context, Bitcoin has a number of shortcomings that appear to have limited its suitability for widespread household and business payment use – price volatility (discussed above), lack of scalability and uncertainty around settlement finality.

The lack of scalability (see Box B) stems from the fact that Bitcoin blocks have a limit on the amount of information they can contain. This limits the number of transactions that can be validated in any individual block and restricts the system to fewer than 10 transactions per second. By contrast, the Fast Settlement Service that serves Australia's New Payments Platform is designed with the capacity of settling around 1,000 transactions per second.

Another issue with Bitcoin is that a transaction cannot be assumed to be final until sometime after it is confirmed in a block. A block is validated by the network roughly every 10 minutes. Since miners compete to nominate new transaction blocks, a transaction may be included in one miner's block but not another's. Sometimes two competing blocks are mined at approximately the same time: eventually one of these will become part of the longest chain while the other becomes an 'orphan' block. Bitcoin transactions recorded in an orphan block are likely to eventually be picked up and included in a later block in the (main) chain but, before this occurs, transactions in the orphan block cannot be treated as settled. Even after a few subsequent blocks are mined, a given block may still be part of an orphan chain: an oft-cited guide is for parties to a transaction to wait until five subsequent blocks are mined (i.e. a total of 60 minutes) before treating a transaction as final. This lack of prompt settlement finality can be a problem for users where, say, goods or services are being delivered in exchange for bitcoins.

Because Bitcoin and other first-generation cryptocurrencies rely on 'proof of work' to establish consensus on the state of the ledger, they consume considerable amounts of energy. Miners compete to solve a computationally intensive cryptographic puzzle that, when solved, verifies a new block of transactions. The successful miner earns a reward of new coins plus any transaction fees associated with a block. The chances of successfully mining a block are roughly proportional to the amount of processing power devoted to solving the cryptographic puzzle. This leads to an arms race in mining technology, as miners invest in more processing power to increase their chances of success. However, since the incentives for this additional investment apply to all miners, if all parties individually invest in faster computing power, then there is no change to their chances of successfully mining a block (Ma, Gans and Tourky 2018). At time of writing, it is estimated that the amount of energy used to power the Bitcoin consensus process is estimated to be equivalent to the energy consumption of Switzerland (Digiconomist 2019). This sizeable energy consumption is a key element of ensuring the validity of cryptocurrency ledgers, but generates large negative environmental externalities. This is likely to become an issue for policy-makers, particularly in the context of increasing concerns about climate change.[9]

While it is possible for an end user to transact in and manage their holdings of bitcoin without using a third party, most end users of cryptocurrency rely on some sort of intermediary to facilitate transactions. These include providers of cryptocurrency exchange services and cryptocurrency wallets. The roles undertaken by intermediaries effectively reinserts the need for some form of trust in a central party for most users. The central party provides services that are valuable to the end user, but also exposes the end user to risks of fraud.[10]

One perceived benefit of Bitcoin and other cryptocurrencies appears to be censorship resistance. There are two main elements to this. Once a transaction is recorded on a widely distributed blockchain, the record cannot be easily erased or altered. In addition, a user who controls their own private key can undertake transactions without a central authority (be it a government, an intermediary or any other party) preventing that user from doing so. The inability of other parties to prevent, modify or censor transactions is, for some of its adherents, a key advantage of cryptocurrency.

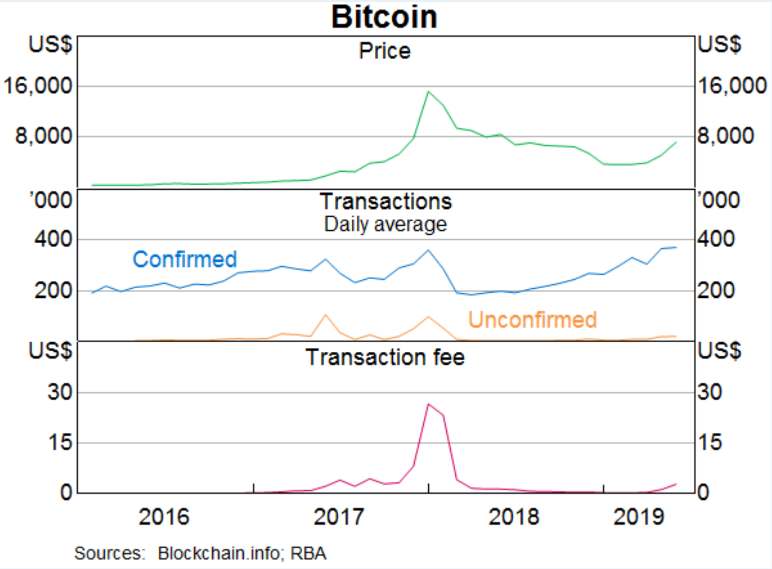
In contrast, the decentralised nature of cryptocurrencies and a lack of clarity around jurisdictional issues raises challenges for regulatory authorities, who have tended to focus not on the central protocol but rather on intermediaries providing services relating to cryptocurrencies, and on those using crypto-tokens for fundraising purposes. For example, the Australian Transaction Reports and Analysis Centre (AUSTRAC) obliges digital currency exchange providers in Australia to: register and enrol with AUSTRAC; adopt and maintain an Anti-money Laundering and Counter Terrorism Financing program that mitigates and manages the provider's money laundering and terrorism financing risks; and report suspicious matters and transactions above certain thresholds to AUSTRAC.

Box B
Bitcoin Scalability Problem

As described above, Bitcoin transactions are confirmed when miners – participants in the Bitcoin system who compete to verify transactions – include those transactions in a new block that is added to the Bitcoin blockchain. This set-up limits the number of transactions in two ways: (1) each block, which records transactions, is by construction limited in size to one megabyte; and (2) a new block is added to the blockchain approximately every 10 minutes. Thus there is a hard limit on the capacity of the Bitcoin network, and fewer than 10 transactions per second can be processed. In contrast, and as noted earlier, Australia's new Fast Settlement Service has been designed with the capacity to settle around 1,000 transactions per second. The processing capacity of the international cards schemes is even greater, being in the region of tens of thousands of transactions per second.[11]

Initially, this transaction limit was not binding, but this changed through 2017 and 2018 when bitcoin speculation became more popular and the number of transactions increased (Graph B1). In December 2017, to incentivise miners to prioritise their transaction, Bitcoin users had to pay, on average, almost US$30 per transaction (and more than US$50 on certain days).

Graph B1



Sources: Blockchain.info; RBA

Two categories of solutions have been proposed to address this scalability problem. The first, 'on-chain', seeks to change the Bitcoin protocol to allow more transactions. The second, 'off-chain', seeks to net offsetting transactions in a separate system, before settling the net flows on the main Bitcoin system.

Two main on-chain proposals have emerged: use blocks more efficiently; and/or to increase block size. In late 2017, an update to the Bitcoin code was released that, by changing the way blocks are structured, roughly doubled the transaction capacity of each block. This update was designed to be backward-compatible with the existing Bitcoin system, and gained wide adoption by Bitcoin miners. At roughly the same time, a group of miners started using new code that allowed for 8 megabyte blocks. Most Bitcoin users, however, remained with the original Bitcoin and the new system (dubbed 'Bitcoin Cash') effectively became a new, less popular, cryptocurrency. The example of Bitcoin Cash demonstrates the challenge faced by all on-chain solutions. Proposals to change the Bitcoin code must gain widespread support across the Bitcoin community (and specifically miners) to be adopted, otherwise any modifications to the code will result in a new cryptocurrency rather than an update to Bitcoin itself.

The main off-chain solution to have emerged is the so-called Lightning Network, where Bitcoin users establish bilateral 'payment channels' by transferring bitcoins to a jointly controlled address. This solution is discussed further in the section 'Iterations to address scalability'.

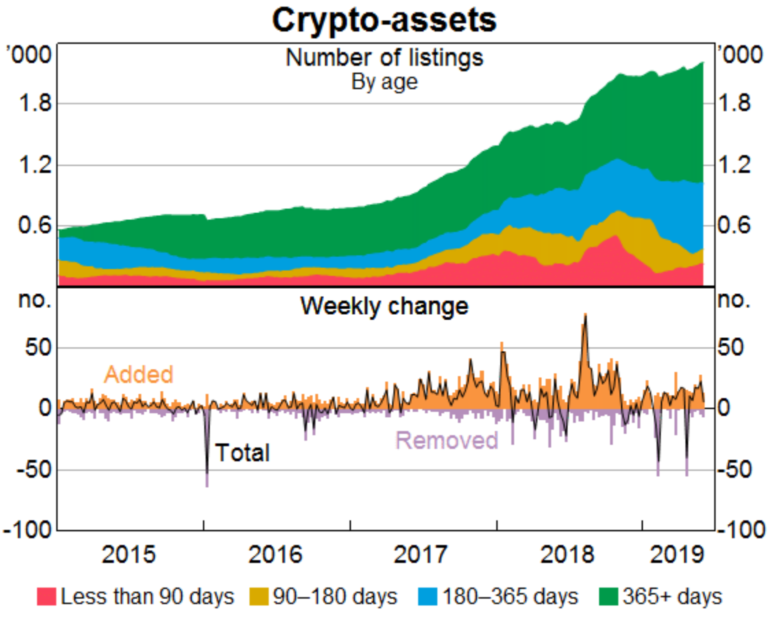
How Have Cryptocurrencies Changed?

Ten years on from its first transaction, Bitcoin remains one of the most prominent cryptocurrencies, and first generation-style coins continue to be created today (though they may not necessarily be used or traded). But there has also been innovation to address the key shortcomings of the first-generation coins and provide increased functionality. In the last two years in particular, there has been a substantial increase in the number of new crypto-assets created, some of which embody novel features or capabilities relevant for their potential use for payments. In this section we set out some prominent examples of newer coins that attempt to address the shortcomings of earlier cryptocurrencies for use in payments.

Of note, while a great many crypto-assets have been created, most are small and many do not exist for long. For example, of the more than 2,000 crypto assets included on CoinMarketCap, a crypto-asset information service with the most comprehensive publicly available list of crypto-assets, the top 50 account for more than 95 per cent of the market capitalisation of all crypto assets.[12] In addition, only around half of all crypto-assets currently included on CoinMarketCap have existed for more than one year (Graph 2), and of all the crypto assets removed from CoinMarketCap in the past four years around 40 per cent were less than a year old.

This short lifecycle of crypto-assets is not surprising. There are very few technical barriers to creating a crypto asset – as noted earlier, many are created through minor changes to the code of another crypto asset. Also, many exchanges will list new cryptocurrencies and other crypto-assets on a fee-for-service basis, without regard to their legitimacy. The short lifecycle may also partly reflect a rapid pace of technological development; with 'coins' potentially being discarded as they become 'old-tech'.

Graph 2



Sources: Coinmarketcap.com; RBA

Iterations to address price volatility

As discussed above, the price volatility of cryptocurrencies such as Bitcoin is likely to have inhibited their use as a payment method (that is, a means of exchange). If it is difficult or impossible for merchants and consumers to know what a cryptocurrency will be worth from one moment to the next, then it will be unattractive for most parties to price, or buy, goods and services in that cryptocurrency and accept payment in the cryptocurrency. Similarly, high price volatility makes cryptocurrencies a poor store of value.

In an attempt to address this, a number of so-called 'stablecoins' have emerged. Stablecoins are a type of cryptocurrency designed to minimise price volatility against some widely used unit of account (often the US dollar) or a common store of value (such as gold). Two broad approaches to achieve this currently exist: asset-backed stablecoins, and algorithmic stablecoins, with some offerings being a hybrid of the two.

Asset-backed stablecoins are cryptocurrencies that seek to gain and maintain a stable value through being – or purporting to be – a claim on real or financial assets. For stablecoins that are fully backed by assets, this means that new coins are, in theory, only issued against an inflow of assets of the same value, and that the coins can be redeemed at a fixed price by selling these assets. Stablecoins that are fully backed by assets that match the peg they are trying to maintain (e.g. money in a US dollar bank account for a USD-pegged stable coin) will, in general, be less susceptible to price volatility, while stablecoins that are not fully backed, or that are backed by more volatile assets (e.g. other cryptocurrencies) tend to be more susceptible to price volatility. Asset-backed stablecoin issuers may seek to cover costs and/or derive profit via seigniorage; that is, they earn interest on the backing assets but do not pay interest on their stablecoin liabilities.[13] These assets are typically controlled by the issuer of the cryptocurrency. However, the underlying details regarding legal recourse of stablecoin holders to those assets, and even whether the assets actually exist, is often unclear. The existence of a central entity that controls the asset backing the stablecoin runs somewhat counter to the original idea behind cryptocurrencies, which was to be a decentralised form of money not reliant on any central body.[14]

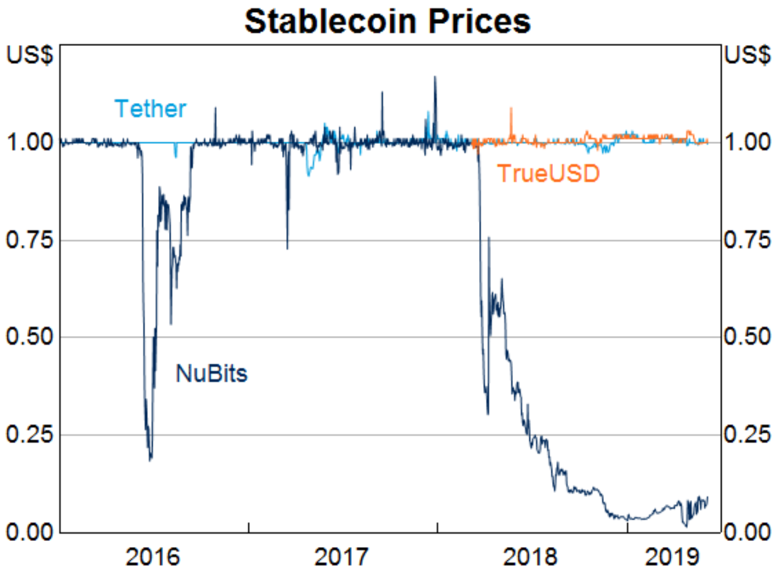
Algorithmic stablecoins attempt to gain and maintain value through a software protocol that manages the supply of the cryptocurrency to match demand, such that the market-clearing price tracks the underlying unit of account closely. Two broad approaches exist to achieving this. The first simply adds or removes coins from circulation (either directly or by changing their status to 'inactive') in order to match supply to demand. While this may succeed in maintaining the quoted stablecoin price, it does this by changing the number of active coins that users hold, such that the total value of users' holdings, being the price multiplied by the number, will still be volatile. The second approach seeks to use incentives and expectations to maintain a stable price. If supply exceeds demand, the stablecoin algorithm issues 'bonds' at a discount to face value, and uses the proceeds to purchase and destroy the surplus stablecoins. If demand exceeds supply, new stablecoins are issued to 'bondholders' to redeem the liability. If the price of the stablecoin falls but some users expect it to rise again in future, then there is an incentive for them to buy 'bonds' and profit from the temporary deviation. If, on the other hand, there are not enough such optimistic users, then the mechanism will fail and the stablecoin price may not recover.

Tether, which is one of the earliest and most prominent asset-backed stablecoins, has to date maintained a relatively tight – although imperfect – peg to the US dollar (Graph 3), despite some market participants questioning the extent to which it is indeed backed by US dollars. Of note, Tether initially claimed to be fully backed by US dollars held at an undisclosed bank. However, in February 2019, it modified its terms of service indicating that its stablecoin may be backed by other US dollar-denominated assets in addition to cash and cash equivalents. Court proceedings have since indicated that only 74 per cent of Tether tokens are backed by cash and cash equivalents (Hoegner 2019). In addition, some reserves were reportedly used by the company to invest in bitcoin and 'other assets' (Cermak 2019). In contrast, other stablecoin issuers have partnered with established financial institutions and engaged with regulators. For example, funds backing the TrueUSD stablecoin are held in escrow accounts at a number of US-based fiduciary and banking partners that the TrueUSD issuer cannot access.[15] So far, TrueUSD has maintained a tight peg to the US dollar since it launched in 2018. NuBits is one of the few algorithmic stablecoins that has launched. It uses bond-like instruments to provide users with incentives to maintain a stable price. Its price fell substantially in early 2018 and has not recovered, highlighting the role of price expectations in algorithmic stablecoin models.

In Australia, the use of stablecoins as a payment method has been very limited, as has the supply of Australian dollar-linked stablecoins. AUDRamp, the first Australian dollar-linked stablecoin to launch, went live in September 2018. However, only 137 tokens were issued and the price has fallen to zero. More recently, TrueAUD was launched in April 2019 by TrustToken, the issuers of TrueUSD, though no tokens appear to have been issued. TrueAUD is expected to operate similarly to TrueUSD.

Looking ahead, the Libra Association – whose participants include Facebook, Mastercard, Visa, PayPal and others – plans to launch a 'global cryptocurrency' in 2020 that would be fully backed by a reserve comprised of a basket of bank deposits and short-term government securities denominated in a range of national currencies. The initial description of the cryptocurrency, named Libra, notes that its value may fluctuate as it is not pegged to any given currency (Libra Association Members 2019).

Graph 3



Source: Coinmarketcap.com

Stablecoins have, in theory at least, the benefit of a stable value while retaining elements of Bitcoin's pseudonymity. However, even if the concerns about the credibility of stablecoin issuers and their coins are resolved, it is not clear that there would be material demand (at least for legitimate purposes) to pay with, or accept, stablecoins over conventional payment methods linked to deposit accounts at commercial banks. The strongest, though still niche, demand for stablecoins appears to be from holders of cryptocurrency that want to diversify into a low-volatility asset without leaving the crypto-ecosystem. Demand may also reflect a reticence to interact with the regulated banking system more generally, perhaps because of a crypto-libertarian[16] ethos, or because the cryptocurrency held may not have arisen from legitimate activities or the holder is seeking to avoid or evade taxes. It is also not obvious that all stablecoins will necessarily be attractive to crypto-libertarians. As noted above, asset-backed stablecoins rely on a central body to buy and manage the assets that back the stablecoin, which means that users have to trust that central body. This is somewhat counter to the initial idea behind cryptocurrencies, although for users who value the technical capabilities of DLT, rather than necessarily valuing the ideological aspects of Bitcoin, this may not be a problem.

Iterations to address scalability

The Bitcoin scalability problem (see Box B) highlighted one barrier to cryptocurrencies becoming widely used. At present, blockchain technology provides for transaction throughput orders of magnitude lower than what would be required for a widely used payment system in Australia, let alone a global payment system. This is unsurprising – the trade-off between decentralisation, scalability and security faced by blockchain developers often requires the throughput of the network to be a lower priority consideration. This trade off is known as the 'scalability trilemma', which claims that blockchain systems can, at most, have only two of the following three properties: (i) decentralisation, (ii) scalability and (iii) security. In practice, these trade offs are incremental; increasing the scalability of a blockchain does not require it to become entirely centralised or insecure, but *more* centralised or *less* secure. Even so, to increase throughput and not compromise on a cryptocurrency's degree of decentralisation and/or security is a difficult task. These attributes are often decided early on in a cryptocurrency's development; for a cryptocurrency to be a reliable store of value – volatility aside – security is paramount.

Increasingly, blockchain developers are implementing alternative consensus algorithms to proof of work. These algorithms include, among others, proof of stake, byzantine fault tolerance[17] and proof of authority.[18] Generally, these alternative consensus algorithms provide for a significant increase in throughput compared with computationally expensive proof-of-work mining processes. The scalability trilemma means that this is typically achieved through centralisation. For example, proof of authority requires a centrally managed *authority* node to appoint block validators; similarly, byzantine fault tolerance requires a *leader* node to propose which transactions are included in a block. Proof of stake is less centralised than these algorithms, but remains more centralised than proof of work – it concentrates the validation of blocks in nodes that hold a large volume of cryptocurrency.

Other cryptocurrencies have turned to non-blockchain solutions to address scalability. Two notable developments include off-chain 'payment channels' and non-blockchain applications of DLT. The Lightning Network is an off-chain network of bilateral payment channels that sits above a host blockchain. Users establish a payment channel by transferring cryptocurrency to a jointly controlled address on the host blockchain. Flows back and forth between any two participating users are then recorded off the blockchain ledger, and the net effect of these transactions is only settled on the blockchain ledger when the payment channel closes. This is comparable with the bilateral netting that occurs in some other payment systems. Transactions can be routed indirectly via multiple bilateral links if no direct link exists. A drawback of this system, however, is that cryptocurrency quarantined in payment channels is unable to be used elsewhere, until those channels close. Liquidity is effectively trapped in the payment channel. While the Lightning Network was first developed for Bitcoin, it has recently been implemented for Litecoin (another first-generation cryptocurrency). A similar off-chain network of payment channels is under development for the Ethereum blockchain.

One non-blockchain application of DLT used to address scalability is to replace the linear blockchain with a directed acyclic graph (DAG). Unlike a blockchain-based cryptocurrency, where transactions are bundled into blocks that form a linear chain, in a DAG-based cryptocurrency, individual transactions are linked together. Different nodes are able to confirm unrelated transactions in parallel, allowing multiple chains of transactions to co-exist and interconnect.[19] IOTA and Nano are two of the better-known cryptocurrencies using DAGs, though both have relatively low levels of activity outside of coordinated tests designed to demonstrate the capacity of each platform to process higher volumes of transactions.

Most of these solutions are not operational or are operating at a scale much smaller than intended. In May 2019, the average number of unique, active Bitcoin addresses per day was around 700,000. By contrast, the implementation of Lightning Network for Bitcoin has less than 10,000 active nodes. Alternative consensus algorithms, such as byzantine fault tolerance or proof of authority, are unlikely to be implemented in widely used public cryptocurrencies because of the centralisation needed for proposing and/or validating blocks. These algorithms may be better suited to private and permissioned blockchains where there is a degree of trust between the participants or with the entity operating the blockchain.

Iterations for functionality

One of the most pivotal innovations in cryptocurrencies since the creation of Bitcoin was the introduction of public distributed computing platforms, the most well-known of which is

Ethereum. The Ethereum platform and its native cryptocurrency, ether, were launched in 2015. The platform's key innovation is the Ethereum virtual machine, which allows the execution of 'smart contracts' that, among other things, facilitate the issuing of crypto-assets or 'tokens' and the development of distributed software applications. Ethereum operates using a proof-of-work algorithm, with ether used to pay miners to process transactions, including the execution of smart contracts. Transaction fees differ by computational complexity, bandwidth use and storage needs. As new blocks are mined, ether is created as a reward for the successful miner.[20]

Smart contracts are comprised of self-executing computer code running on a blockchain or other DLT platform.[21] The creator of a smart contract on the public Ethereum blockchain sets out the conditions under which the contract will execute and its output. As smart contracts are stored on a blockchain or other DLT platform, the conditions and associated outputs are visible to all parties to the contract and immutable. This allows parties to enter into an agreement knowing that it will be enforced without the need to trust each other. For example, a crypto-asset token can be issued using a smart contract using 'if, then' or other conditional statements. Here, the smart contract may be configured as: 'if Address A receives 1 ether from Address B, then send 10 tokens from Address A to Address B'. If the token is a cryptocurrency, it is sometimes referred to as 'programmable money'. One benefit of programmable money is that both sides of a transaction are able to settle simultaneously – a so-called 'atomic' transaction. Tokens may also have a broader array of features and characteristics, facilitating the creation of security and utility tokens. Around 1,300 of the crypto-assets listed on CoinMarketCap are created using smart contracts and around 90 per cent of these were created on the Ethereum platform. Even though smart contract code on the Ethereum blockchain is typically public, and therefore can be independently verified, fraudulent activity nonetheless occurs. In 2017, researchers estimated that as many as 10 per cent of smart contracts on the Ethereum platform were related to fraudulent activity (Bartoletti *et al* 2017).

The additional functionality offered by smart contracts does not, in itself, address the fundamental barriers – such as scalability and volatility – to cryptocurrencies becoming widely used for payments. Indeed, it may be the case that additional functionality offered by smart contracts can be integrated into centralised systems, including into some of Australia's existing payment systems. Indeed, a recent Data61-CBA proof of concept to apply 'programmable money' to National Disability Insurance Scheme payments found that a system based on a centralised database could, in theory, generate the same efficiency gains as a DLT-based approach (Royal *et al* 2018).

Are Cryptocurrencies Money Today?

Some of the evolution in cryptocurrencies in recent years has been an attempt to address some of the key shortcomings that have prevented Bitcoin from functioning as money. However, it remains the case that no cryptocurrencies currently function as money in Australia, or as widely used payment methods. Proposals to improve scalability and volatility have had varied success. Many continue to be a work in progress and they generally come at the cost of making a cryptocurrency more centralised, a feature that may not be attractive to crypto-libertarians and in any case makes them more similar to established payment systems. Developments to date have also not added sufficiently to the overall reliability, functionality and credibility of cryptocurrencies to make them an attractive alternative to established payment systems for everyday payments for the population at large.

Regardless, DLT is likely to continue to evolve, including in ways that are unrelated to cryptocurrency. For example, there are several private-sector initiatives focused on 'private permissioned' DLT systems, for example, Corda and Quorum, which – while not suitable for a widely used cryptocurrency – are being explored for use in financial market infrastructure and wholesale payments. Accordingly, the Reserve Bank will continue to study the implications of cryptocurrencies and DLT for the financial system, and the economy more broadly.

Finally, it should also be noted that innovation continues to occur in traditional centralised payment systems – the creation and launch of Australia's New Payments Platform is an example of this. As long as the Australian dollar continues to provide a reliable, low-inflation store of value, and the payments industry continues to work on the efficiency, functionality and resilience of the Australian payments system, it is difficult to envisage cryptocurrencies presenting a compelling proposition that would lead to their widespread use in Australia.

Footnotes

[*] The authors are from Payments Policy Department.

[1] We use (lower case) 'bitcoin' to refer to a unit of cryptocurrency in the Bitcoin system.

[2] In this context, scalability refers to the capacity of a system to grow to meet demand.

[3] This article focuses on privately established cryptocurrencies. It does not address issues relating to central bank digital currencies, which have been given some consideration in recent years: for a local and global perspective see Lowe (2017) and CPMI and MC (2018). Nor does this article address the potential use of distributed ledger technology in wholesale or large-value payments systems or other financial market infrastructures.

[4] This definition draws on the European Banking Authority's definition of 'virtual currencies', see European Banking Authority (2014).

[5] As described in the UK Cryptoassets Taskforce Final Report, 'DLT is a type of technology that enables the sharing and updating of records in a distributed and decentralised way. Participants can securely propose, validate, and record updates to a synchronised ledger (a form of database), that is distributed across the participants.' (HM Treasury, Financial Conduct Authority, Bank of England 2018). The term 'blockchain' is often used interchangeably with DLT, but it refers to a specific way of structuring data on a DLT platform.

[6] ASIC has issued investor warnings on both cryptocurrencies and initial coin offerings, see ASIC (2018a) and ASIC (2018b).

[7] For example, the 1990s saw trials of digicash and Mondex, early prototypes of electronic cash.

[8] This description is drawn from Richards (2018).

[9] See Debelle (2019) for a financial sector perspective on these issues.

[10] A widely known early example relates to Mt Gox, which declared bankruptcy in early 2014 following the loss of 850,000 bitcoins. More recently, customers of the Canadian exchange QuadrigaCX are reported to have lost access to crypto-assets following the death of the founder of the exchange, purportedly the only person with the cryptographic keys to access the 'cold wallets' (offline storage) of users.

[11] For example, Visa's payment network, VisaNet, processes around 1,700 transactions per second and is capable of processing more than 65,000 transactions per second.

[12] For a cryptocurrency to be included on CoinMarketCap, it must fit the definition of a cryptocurrency, be traded publicly, and actively traded on at least two exchanges. There are around 250 exchanges currently recognised by CoinMarketCap.

[13] The term seigniorage is used to describe the income earnt from the production of money. It can refer to the profit derived from the difference between the face value of the money (such as banknotes) and the cost of its production. It can also refer to the income earnt on securities acquired in exchange for the money produced, less any interest payable on the money that is outstanding (zero in the case of banknotes). Today, it is common for banknote issuing authorities, including the Bank, to derive seigniorage using the latter approach. This is because commercial banks can and do return banknotes to the central bank in exchange for fresh electronic balances at the central bank and, as such, banknotes are treated as zero-

interest liabilities. See RBA (1997) for further discussion.

[14] Outside the scope of this article, there are also, in prototype form at least, commercial bank-backed stablecoins such as JPM Coin. In such a set-up, holders are likely to be exposed to the credit risk of the commercial bank, similar to a conventional deposit account (abstracting from any government deposit guarantees).

[15] TrueUSD is registered as a money services business with the Financial Crimes Enforcement Network, which administers anti-money laundering, 'know your customer' and anti-terrorism financing regulations.

[16] Crypto-libertarians are commonly characterised as mistrustful of the traditional banking system. Richards (2018) notes that 'Some of them [crypto-libertarians] assert that the quantitative easings undertaken by major central banks in the wake of the global financial crisis have somehow debauched the value of traditional national currencies.'

[17] Byzantine fault tolerance (BFT) is a concept in distributed systems, in which the participants of a system (some of whom may be malicious) can achieve consensus on its state. Consensus algorithms such as *delegated* BFT or *practical* BFT achieve BFT by appointing a *leader* node to propose changes to the blockchain; nodes may take turns fulfilling the *leader* role. If more than a defined threshold of the other nodes agree with the *leader* node's proposed changes, the changes are committed to the blockchain.

[18] Variations on these algorithms, such as *delegated* proof-of-stake or *democratic* byzantine fault tolerance, differ mostly in how the underlying algorithm is implemented. The latter, implemented in University of Sydney and Data61's 'Red Belly Blockchain' has been shown to scale to more than thousands of transactions per second under experimental conditions.

[19] For more information, see: <https://medium.com/fantomfoundation/an-introduction-to-dags-and-how-they-differ-from-blockchains-a6f703462090>.

[20] Ethereum currently uses proof of work for mining, though it has been aiming to move to proof of stake for a long time.

[21] In this section we discuss smart contracts created on the public Ethereum blockchain. Smart contracts may also be created on private blockchain or other DLT platforms, where the intended application will inform characteristics such as privacy.

References

Ali R, J Barrdear, R Clews and J Southgate (2014), 'The Economics of Digital Currencies' *Bank of England Quarterly Bulletin*, September.

ASIC (2018a), 'Cryptocurrencies', Moneysmart site, 24 October.

ASIC (2018b), 'Initial Coin Offerings: Investment or scam?', Moneysmart site.

Bartoletti M, S Carta, T Cimoli and R Saia (2017), 'Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact', 19 July.

Cermak L (2019), 'Tether admits in court to investing some of its reserves in bitcoin', The Block site, 21 May.

CPMI (2017), 'Distributed ledger technology in payment, clearing and settlement – An analytical framework', February.

CPMI and MC (2018), 'Central bank digital currencies', 18 March.

Debelle G (2019), 'Climate Change and the Economy', Public Forum hosted by the Centre for Policy Development, Sydney, 12 March.

Digiconomist (2019), Bitcoin Energy Consumption Index site, 21 May.

Doyle M-A, C Fisher, E Tellez and A Yadav (2017), 'How Australians Pay: Evidence from the 2016 Consumer Payments Survey', RBA Research Discussion Paper No 2017-04.

European Banking Authority (2014), 'EBA Opinion on 'virtual currencies'', 4 July.

Google (2018), 'Year in Search 2017', Google Trends site.

HM Treasury, Financial Conduct Authority, Bank of England (2018), 'Cryptoassets Taskforce: final report', October.

Hoegner S (2019), 'Affidavit filed in the Matter of Letitia James, Attorney General of the State of New York v iFinex Inc., BFXNA Inv, BFXWW Inc., Tether Holdings Limited, Tether Operations Limited, Tether Limited, Tether International Limited', Scribd.com site, 30 April.

Kaspersky Lab (2018), 'Spam and phishing in 2017', 15 February.

Libra Association Members (2019), 'An Introduction to Libra', Libra site, 18 June.

Lowe P (2017), 'An eAUD?', Address to the 2017 Australian Payment Summit, Sydney, 13 December.

Ma J, JS Gans and R Tourky (2018), 'Market Structure in Bitcoin Mining', NBER Working Paper Series 24242.

Macquarie Dictionary (2019), 22 May.

Nakamoto S (2008), 'Bitcoin: A Peer-to-Peer Electronic Cash System'.

RBA (1997), 'Measuring Profits from Currency Issue', *Bulletin*, July, pp 1–4.

RBA (2014), 'Submission to the Inquiry into Digital Currency', Senate Economic References Committee Inquiry into Digital Currency, November.

Reserve Bank of Australia (2019), 'Cryptocurrencies', Reserve Bank of Australia site.

Richards T (2018), 'Cryptocurrencies and Distributed Ledger Technology', Australian Business Economists Briefing, Sydney, 26 June.

Royal D, P Rimba, M Staples, S Gilder, AB Tran, E Williams, A Ponomarev, I Weber, C Connor and N Lim (2018), 'Making Money Smart: Empowering NDIS participants with Blockchain technologies', October