RESERVE BANK OF AUSTRALIA

Speech

Cryptocurrencies and Distributed Ledger Technology

Tony Richards[*]
Head of Payments Policy Department

Australian Business Economists Briefing
Sydney – 26 June 2018

I would like to thank the Australian Business Economists for the invitation to provide a Reserve Bank perspective on cryptocurrencies and distributed ledger technology. This is a topic that is of great interest across the community. It is an area that the Bank has been watching closely for a number of years as it could have implications for us from a number of perspectives. It is also of interest to our international counterparts and so has been the subject of a lot of joint work done in the various committees that we participate in at the Bank for International Settlements.[1]

I am going to talk about cryptocurrencies by focusing on bitcoin, which is the most prominent, and will also touch on the somewhat-related issue of whether the Reserve Bank should consider issuing a new digital form of the Australian dollar. I do not claim to be speaking today as an expert on cryptography and related technical matters. Rather it is as an economist who focuses on payments issues and has been following developments in bitcoin and other cryptocurrencies since early 2013. As we at the Bank analyse new payment methods, we often try to get first-hand experience of them. So perhaps I should offer a disclosure, namely that I have had a bitcoin wallet since June 2014. It contains a small amount of bitcoin and I have used it for a few small transfers and even a retail transaction at a café that accepted bitcoin.

A Quick Primer on Bitcoin[2]

Bitcoin and similar assets have variously been called virtual currencies, digital currencies and cryptocurrencies.[3] As I will discuss shortly, the use of the term 'currency' is really not appropriate given that they share very few of the attributes of other currencies or monies. A more appropriate term for them might be 'cryptoassets'. However, because this term might also include initial coin offerings (or ICOs, which I will not cover today), I will continue to use the popular term cryptocurrencies.

Let me start with a very quick overview of bitcoin. Many of its attributes are shared with other 'first generation' cryptocurrencies, so this is useful background for any general discussion of cryptocurrencies.[4]

As is fairly well known, the protocol or computer code for bitcoin was launched in 2009, following a 2008 paper authored by an individual (or group) using the name 'Satoshi Nakamoto'.

Bitcoin was designed to electronically mimic a cash transaction: to allow quick, peer-to-peer transfers of value, without the need to know or trust the other party in the transaction or for any central body to intermediate the transaction.

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 or so, the bitcoin blockchain is updated to include a block of new 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, 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.

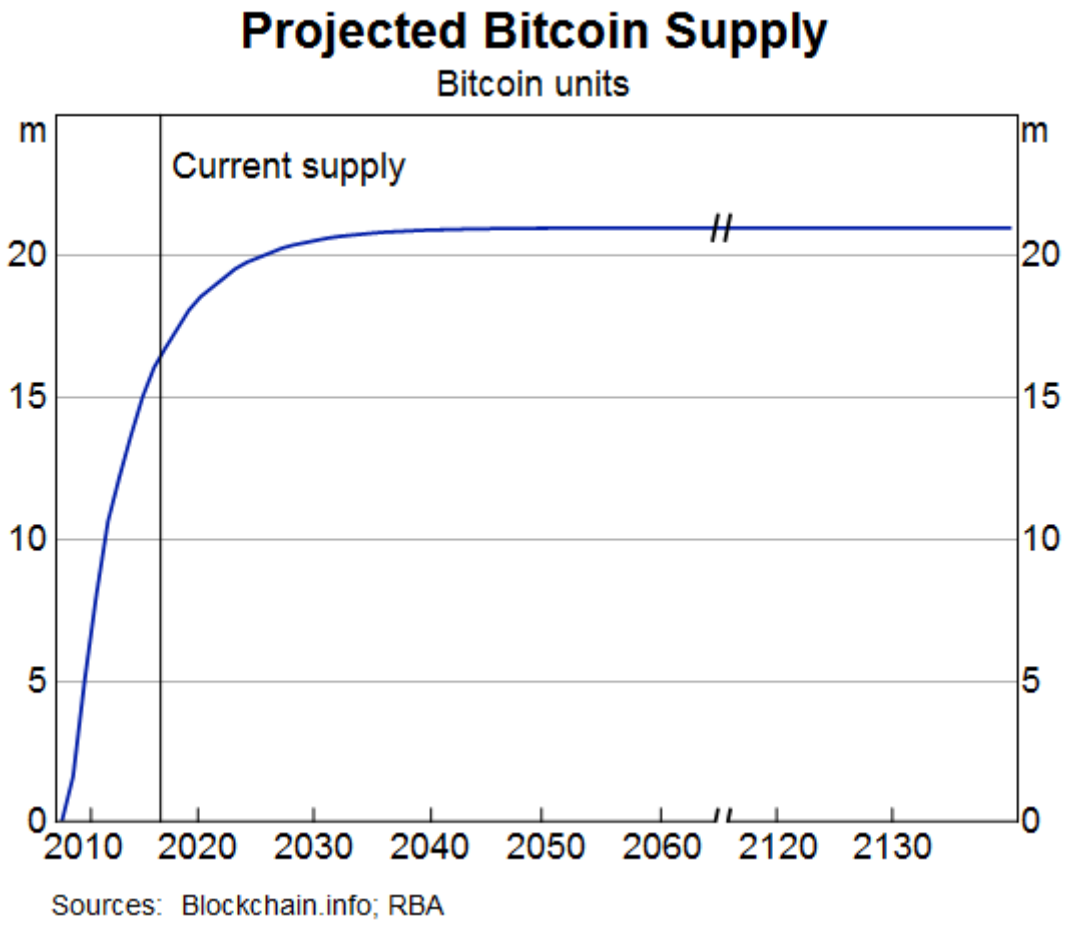
The security of the bitcoin system relies on public/private-key cryptography. The transaction verification methodology is referred to as 'proof of work'. Participants in the system (or 'miners' as they are known) compete to successfully verify (or solve the computationally intensive calculations for) a new block of transactions, with each block consisting of up to about 2,500 transactions. The first miner to do so earns a reward of newly 'mined' coins, currently set at 12½ bitcoins (worth around US$80,000). The successful miner also earns any transaction fees offered by the people initiating the transactions.

This reward leads to an arms race in bitcoin mining technology, as miners (or pool of miners) invest in faster computers to increase their chance of successfully mining a block.[5] As the computing power of the network increases, the bitcoin protocol increases the difficulty of its proof-of-work challenge to keep the rate at which new blocks are added to the blockchain broadly steady, at about one block each ten minutes.

Higher processing power obviously requires more electricity, mainly for air conditioning to cool computer servers. Currently, the majority of bitcoin mining is based in China, reflecting its low-cost electricity (and for some locations, low average temperatures). No doubt you will have seen references to the enormous energy usage of the bitcoin system – the latest estimates suggest that the annual energy consumption of the network is similar to that of entire countries such as Switzerland, the Czech Republic, Chile or Austria.[6] So it is not surprising that it has been criticised as an 'environmental disaster'.[7]

Conventional national currencies (or 'fiat' currencies) get their value in part from the fact that legislation says that they are legal tender and can be used to settle financial obligations such as taxes. However, bitcoin has no such intrinsic value. Any value that cryptocurrencies have is based on expectations that others will attribute value to them and that their supply is somehow limited. In the case of bitcoin, the protocol specifies that around 21 million bitcoins will eventually be created (with each bitcoin divisible into 100 million satoshis). There are currently just over 17 million bitcoins on issue, with additions to supply programmed to gradually decrease until 2140. As the protocol's rewards to mining decrease, the transaction fees received by miners can be expected to increase.

Graph



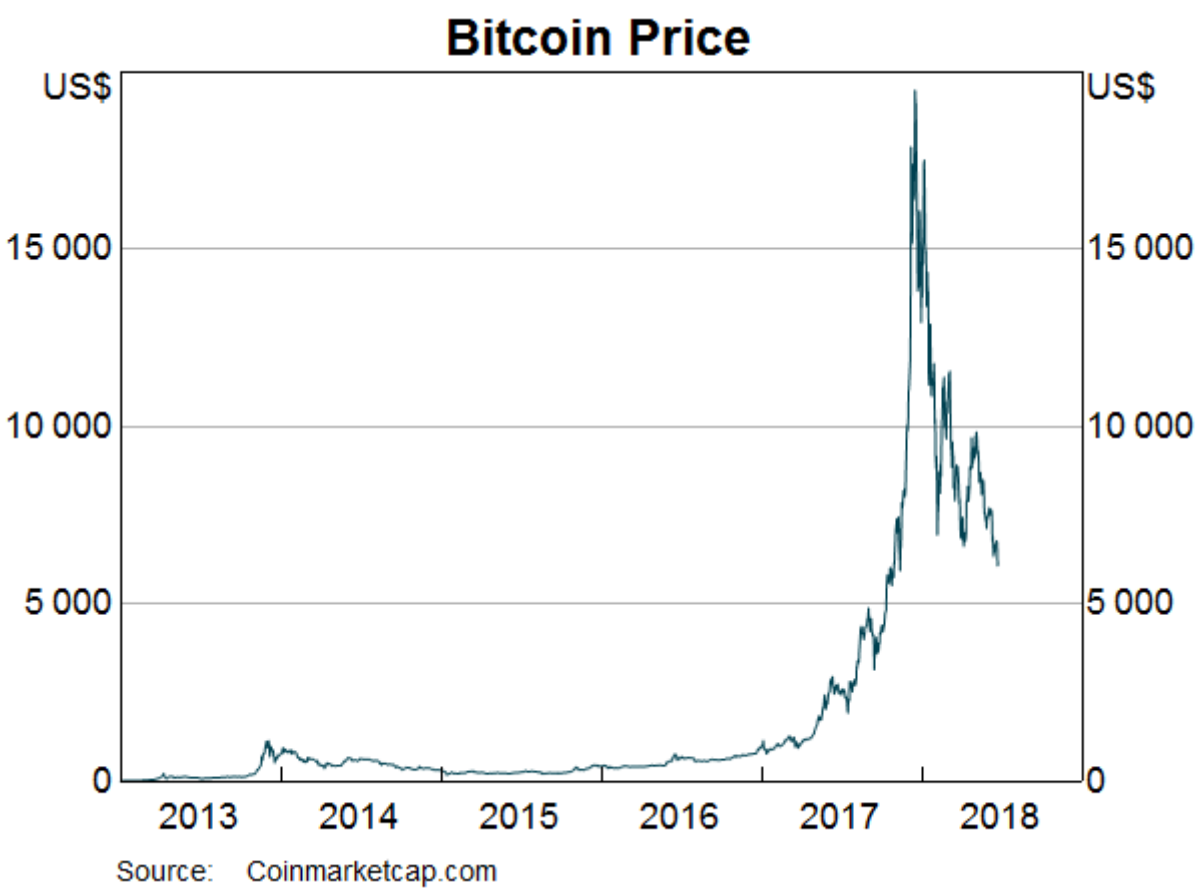
That is a quick overview of the design of the bitcoin protocol and system. My understanding is none of the various components of its design were new, but that their combination in bitcoin was. Indeed, even if one is quite sceptical of whether bitcoin will have a significant role in the economy in the future, I think it is hard to avoid some admiration for its design.

Recent Market Developments for Cryptocurrencies

I can illustrate some of the consequences of the design of the bitcoin system by looking at the sharp run-up in prices that occurred in the speculative mania seen in late 2017.

This graph shows the US dollar price of bitcoin, starting in 2013 when the price was about US$10. There are only limited data prior to that, though there is a frequently mentioned transaction back in 2010 when a programmer bought two pizzas for 10,000 bitcoin, which corresponds to a price of about 0.3 cents per bitcoin.

Graph



As we look back over bitcoin's history, I think the run-up in prices has reflected demand from a range of groups, in the following broad sequence.

Early adopters included three groups:

- those who were attracted by the innovative design and technology of the bitcoin system;
- those who were looking for anonymity in their payments (including for shadow-economy or criminal activity); and
- those who we might call 'crypto-libertarians'.

I would characterise this last group as mistrustful of the traditional banking system. Some of them 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. Of course, I

don't need to point out to this audience that, nearly 10 years after those quantitative easings, inflation in the major economies remains quite subdued.

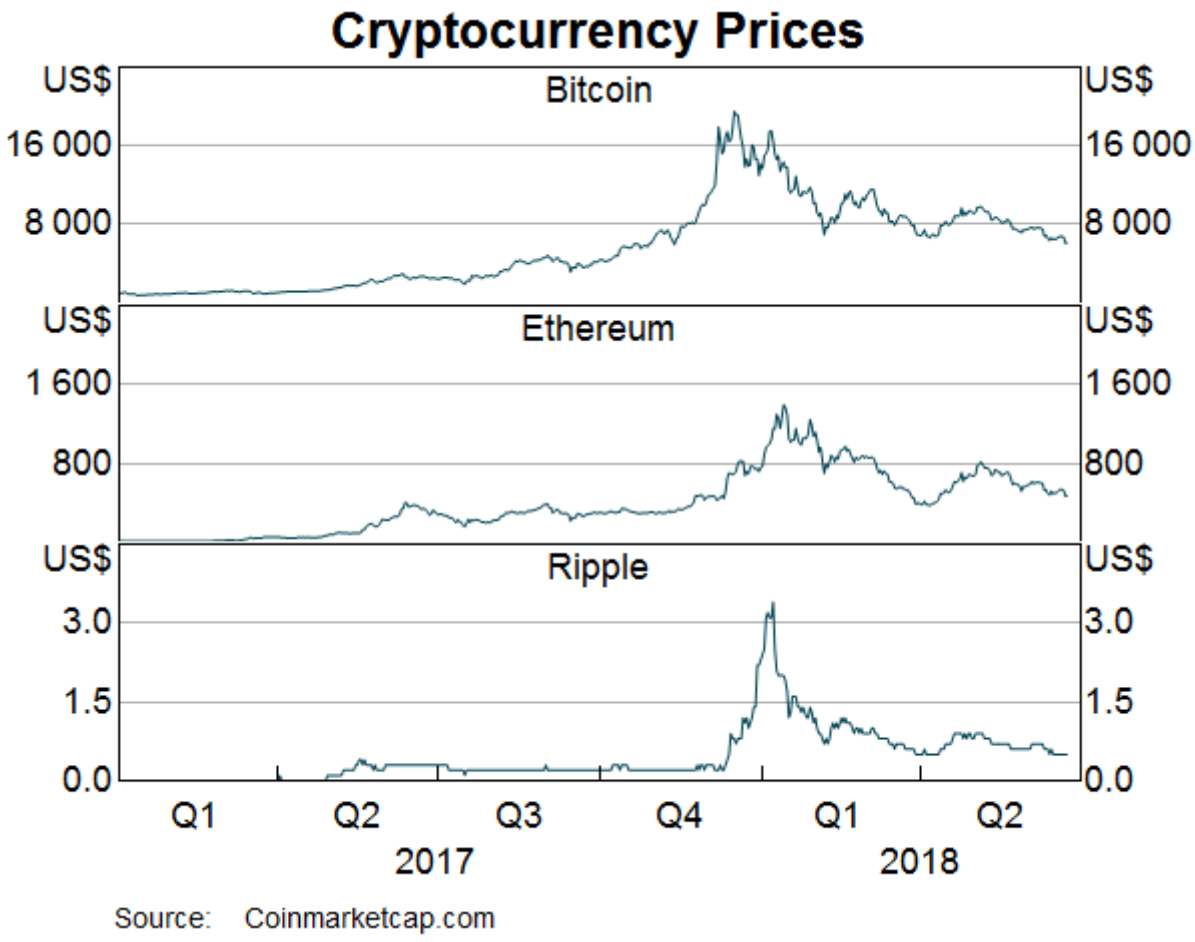
A subsequent group of adopters were those who believe that cryptocurrencies (and distributed ledger technology more broadly) could play a significant role in the economy in the future.

A further type of demand began to emerge around late 2016 and was associated with initial coin offerings.

And the final type of demand that we saw most clearly in late 2017 was conventional speculation. This is where rising prices – and media reports of price rises – encourage more buyers, regardless of the fundamental value of the speculative assets. Many of these buyers would have had very little knowledge of cryptocurrencies except what they had seen on TV or heard from acquaintances.

The sharp run-up that was seen in bitcoin in late 2017 was also seen in many other cryptocurrencies, including those from the Ethereum and Ripple systems.

Graph

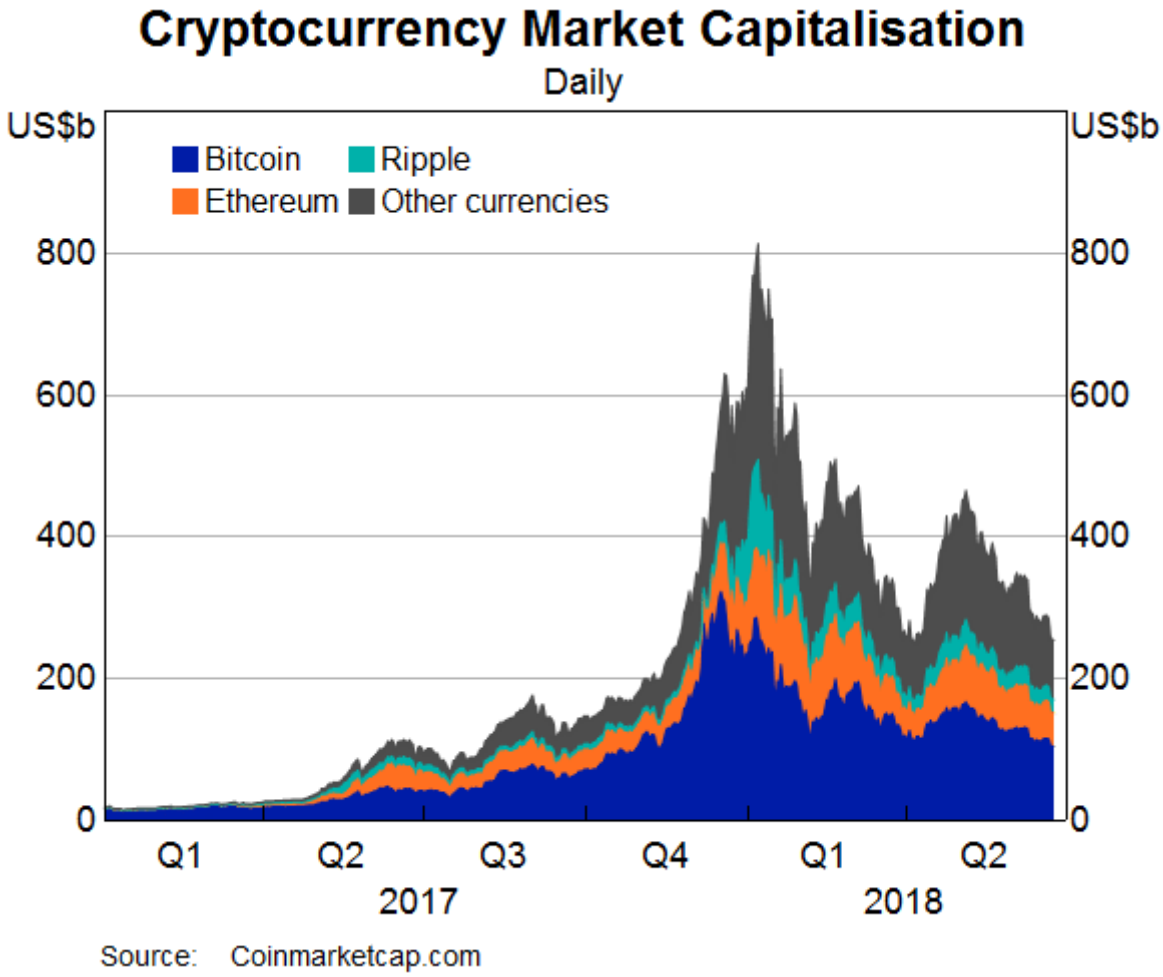


Source: Coinmarketcap.com

The price of bitcoin reached an all-time peak of over US$19,000 in mid December, around 20 times its value at the start of the year. And the total implied 'market capitalisation' of the cryptocurrency sector rose to around US$820 billion in early January this year (though that would be an overestimate because it does not account for all those holdings that are no longer accessible due to

loss of private keys). At that point, the bitcoins used to buy the two pizzas mentioned earlier would have been worth close to US$200 million.

Graph

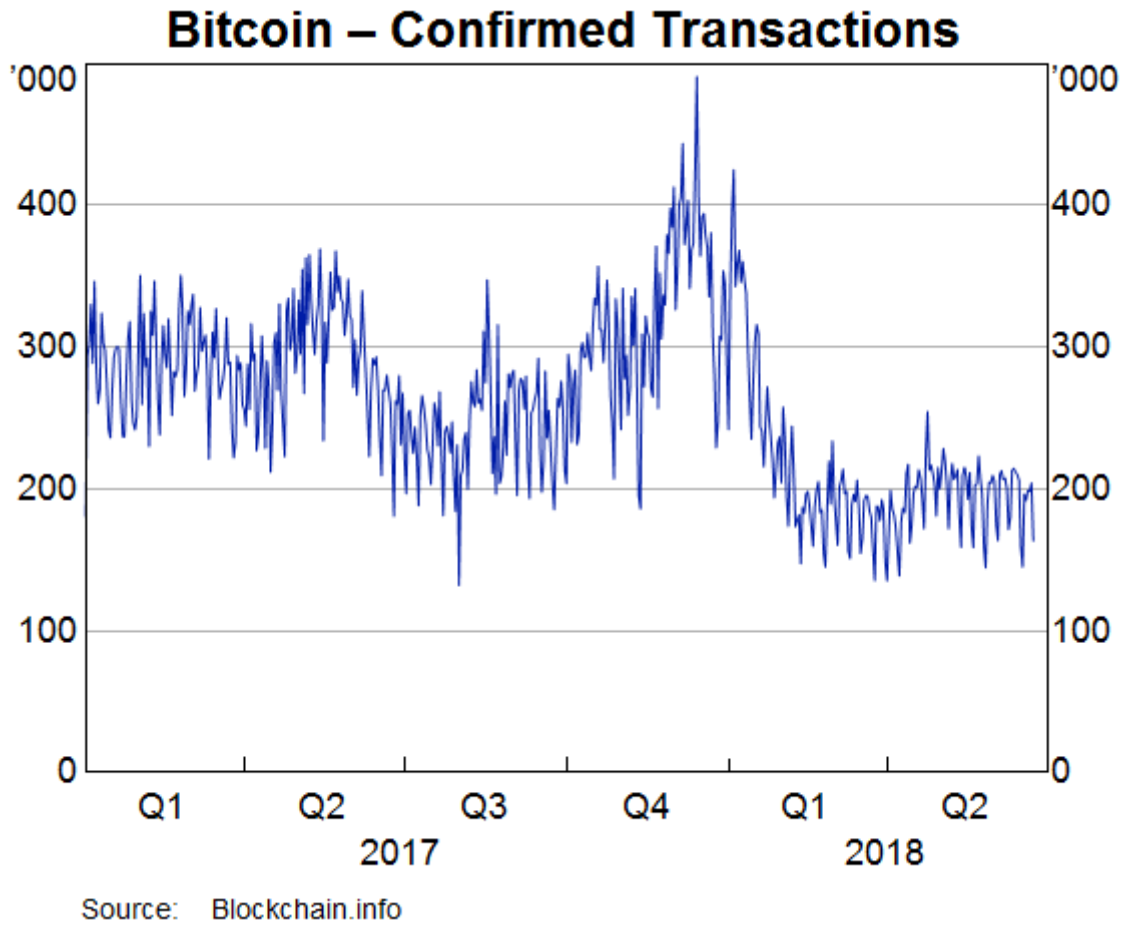


However, the price of bitcoin has fallen by nearly 70 per cent from its peak, to just over US$6,000 currently, and there have been sharp falls in most other cryptocurrencies. Much of the public frenzy seems to have calmed and the market capitalisation of the overall cryptocurrency sector has fallen back to around US$250 billion.

To put this in context, the global equity market is valued at around US$80 trillion and the global money supply is something around US$15 trillion for currency and US$90 trillion for broad money. People might reach different conclusions about the relative importance of the cryptocurrency sector from those comparisons. But I think it is clear that the market capitalisation of the sector is still at levels that we would have thought unthinkable a few years ago.

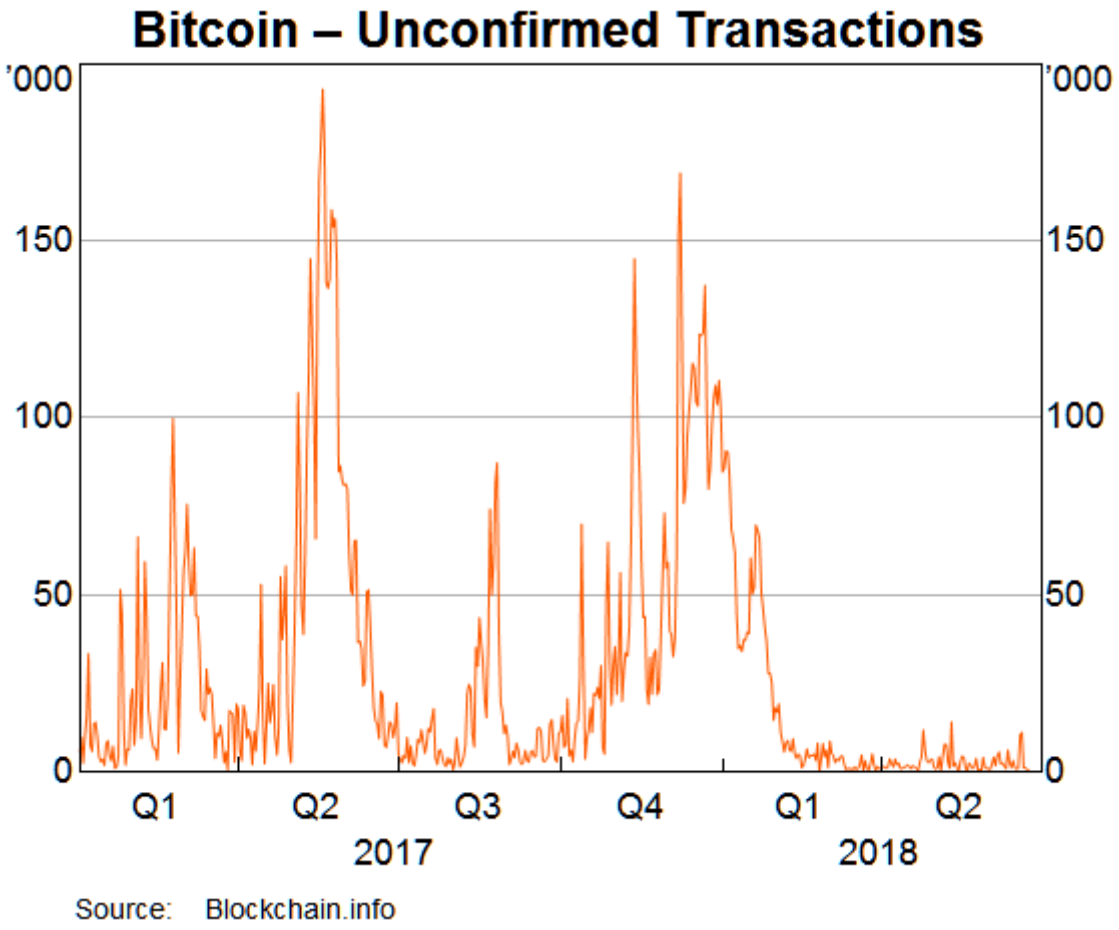
My next graph shows that the number of *confirmed* bitcoin transactions briefly got to over 400,000 per day in December when the speculative frenzy was greatest.[8] That corresponds to a peak of about 4½ transactions per second (TPS). But, to put that in context, Visa Net has a theoretical maximum of over 65,000 TPS.

Graph



However, the peak in *submitted* bitcoin transactions around this time was higher, closer to around 500,000 per day. As a result, the number of unconfirmed transactions was building up. At some points in December, there were over 100,000 transactions in the queue waiting for confirmation.

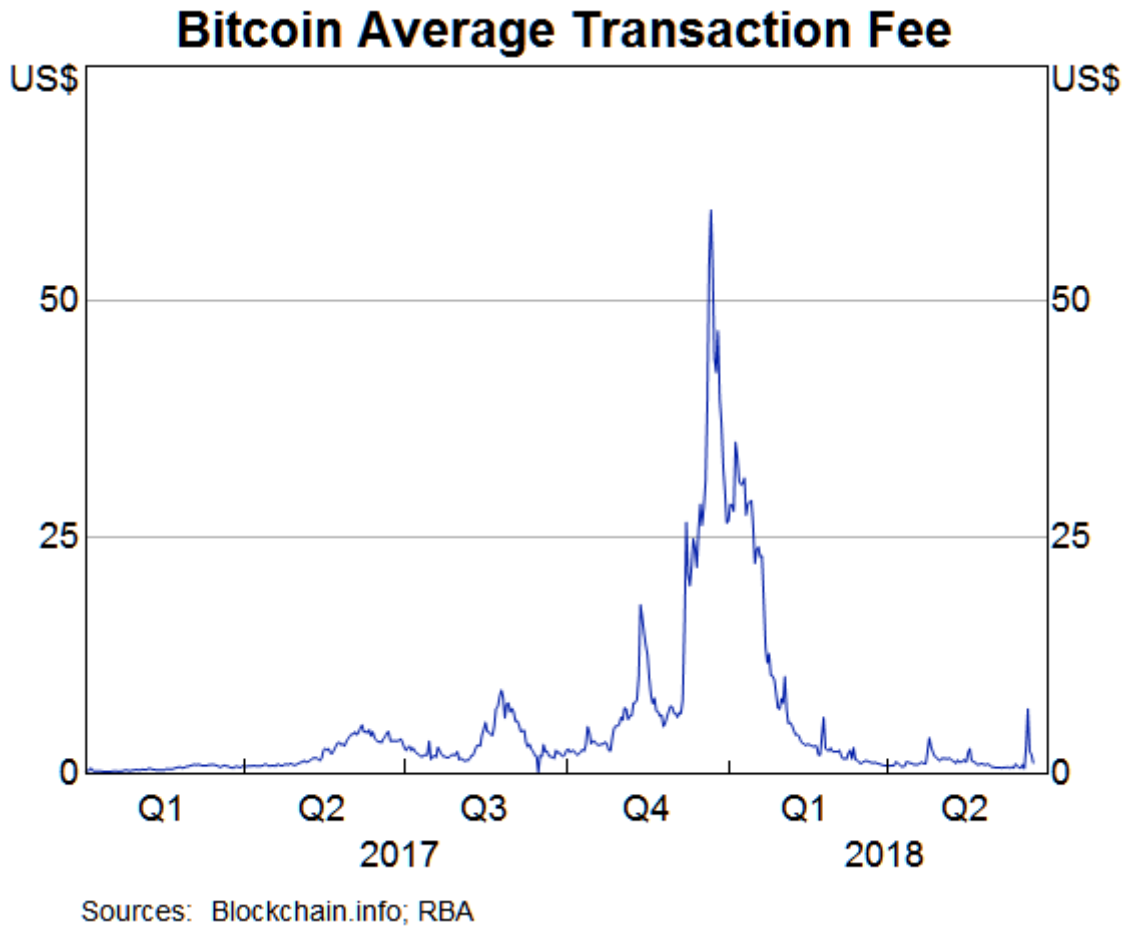
Graph



This episode points to the scalability and governance problems of the bitcoin system. Part of the attraction of bitcoin for its proponents is that there is no central governing authority. Instead, changes to the bitcoin protocol require a consensus among participants in the network. In principle, any user can propose a change to the protocol, as the code is open-source. And if enough nodes adopt the change, it becomes the new protocol. In practice, however, bitcoin's lack of a central governance structure has been a weakness in dealing with the capacity problem that results from the fact that the original protocol limits the block size to no more than 1 megabyte. There have been several proposals for changes to the protocol to deal with this scalability problem but none has yet been entirely successful.

When there is a queue of unconfirmed transactions, miners attempt to verify blocks of those transactions that offer the highest transaction fees. So as the queue lengthened in late 2017, people keen to have their transactions processed were offering to pay more. This next graph shows that at one point, average fees briefly reached over US$50 per transaction.

Graph



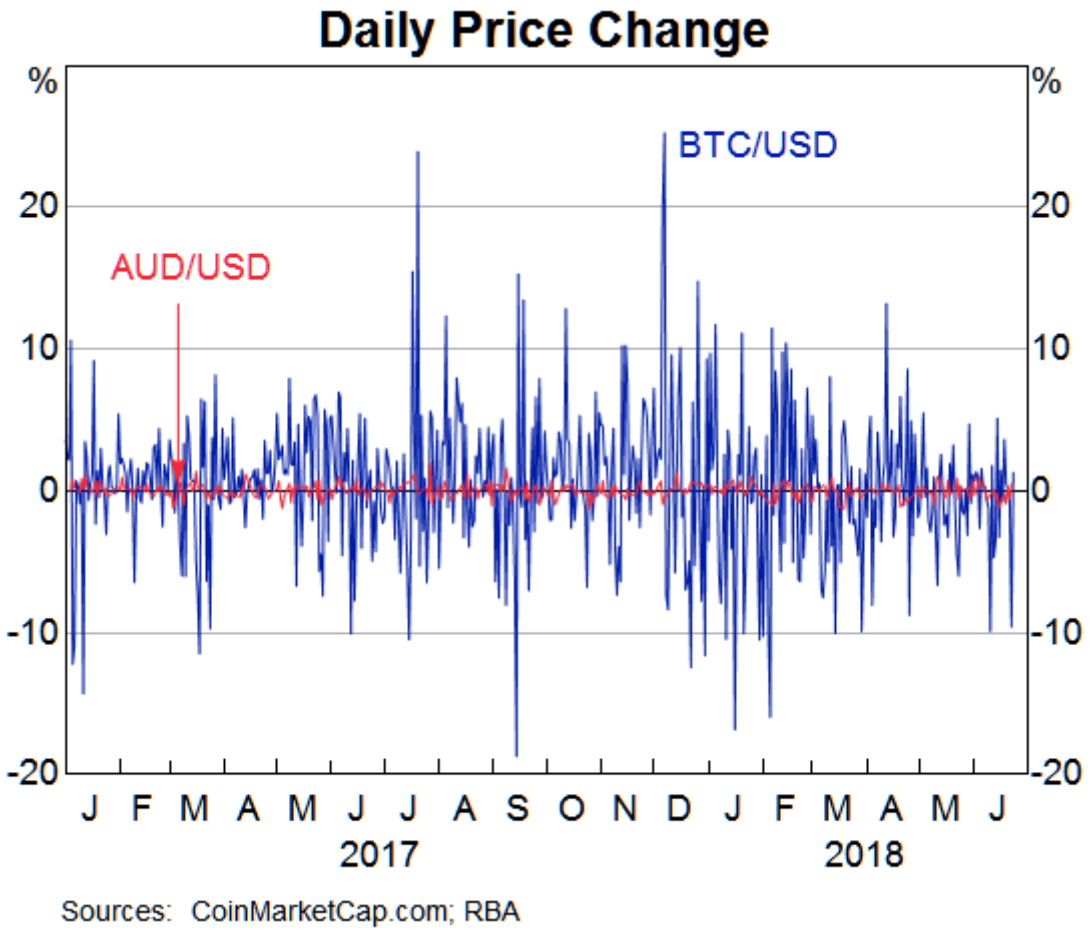
Since then, as the bitcoin price has fallen, and the mania around getting into bitcoin has eased, the volume of transactions has fallen, the queue of unconfirmed transactions has fallen, and fees for transactions have fallen. Reports suggest that some of the computing capacity put in place in late 2017 when there were high returns to mining – both from transaction fees and newly mined bitcoin – is currently uneconomic.

Are Cryptocurrencies Money?

The graphs of transaction fees and the queue of unconfirmed transactions raise the broader question of how well bitcoin (and other cryptocurrencies) perform when we look at the key attributes of money, namely that it should represent a store of value, a medium of exchange and a unit of account. Here, I think there is fairly substantial agreement.

First, bitcoin and other cryptocurrencies are yet to establish themselves as reliable stores of value. This is most obvious in a comparison of the volatility of bitcoin as opposed to national currencies like the Australian dollar. This graph illustrates the high degree of market risk in holding bitcoin.

Graph



And there have also been many hacks of cryptocurrency exchanges and wallets over the past few years. That shows there is also a lot more risk in bitcoin intermediaries than there is in the supervised banks and financial institutions in which households can hold their Australian dollars.

Bitcoin and other cryptocurrencies are also currently not very useful as a medium of exchange for everyday purchases. I have managed to find a Sydney café that accepted bitcoin for a coffee. But there are not many of them.

More broadly, although bitcoin has become more prominent over the past few years, the number of businesses accepting bitcoin may actually be falling. For example, some significant US online merchants announced a few years ago that they were accepting bitcoin, but some of these (for example, Dell) have since stopped doing so.

Of course, there are network effects in payments and ingrained habits in the behaviour of households and businesses, so observations about the current limited acceptance of bitcoin may not be surprising and may be a little unfair. However, nine years after its launch and about five years since it entered the public consciousness, bitcoin continues to have structural flaws that make it unsuitable for many uses, many of which stem from its inefficient verification process. For example, while authorisation of a debit or credit card transaction is close to immediate, bitcoin users are typically advised to wait for the creation of about six additional blocks (i.e., about 60 minutes) before relying on their transactions being final.

The third function of money is as a unit of account. Here, while a small number of businesses may accept bitcoin, their prices are posted in national currencies. Not even bitcoin conferences post their prices in bitcoin. Indeed, organisers of a high-profile US cryptocurrency conference recently apologised that they couldn't accept bitcoin as payment for attendance fees.

Many of these shortcomings of cryptocurrencies stem from their design around trustless distributed ledgers and the costly proof-of-work verification method that is required in the absence of a trusted central entity. In contrast, in situations where there are trusted central entities in well-functioning payment systems, there may be little need for cryptocurrencies.

Of course, there are payments use-cases where some form of distributed ledger might be useful. Examples that are cited include correspondent banking, international transfers, cross-border trade finance and post-trade activity in the equity market. These all involve many different parties, with existing processes that are very entrenched and where it has often been difficult to coordinate among the parties to bring about change. Discussion of the potential of distributed ledgers has highlighted inefficiencies in the current processes and is acting as a catalyst for change. However, I think the evidence to date is that trustless blockchain solutions are unlikely to be adopted. Rather, the new systems are more likely to be permissioned shared ledgers, where a central body still plays a dominant role.

Some Implications for Central Banks

Let me conclude by talking a bit about some of the policy issues that could arise for the Reserve Bank from the emergence of cryptocurrencies and distributed ledger technology more broadly.

As I indicated at the start, the Bank has been watching developments in these areas for about five years. Currently, however, cryptocurrencies do not appear to raise any major concerns for the Bank given their very low usage in Australia. For example, it is hard to make a case that they raise any significant concerns for the Bank's mandate to promote competition and efficiency and to control systemic risk in the payments system.

Nor do they currently raise any major issues for the Bank's monetary policy and financial stability mandates. There are only very limited links from cryptocurrencies to the traditional financial sector. Indeed, many financial institutions have actively sought to avoid dealing with cryptocurrencies or cryptocurrency intermediaries. So, it is unlikely that there would be significant spillovers to the broader financial system if cryptocurrency holders were to suffer valuation losses or if a cryptocurrency system or intermediary was compromised.

But given all the interest in cryptocurrencies or private digital currencies, people have inevitably asked whether central banks should consider issuing digital versions of their existing currencies. I can give you an indication of the Bank's preliminary thinking on this issue, as outlined in December by the Governor in a speech entitled ‘An eAUD?’.[9]

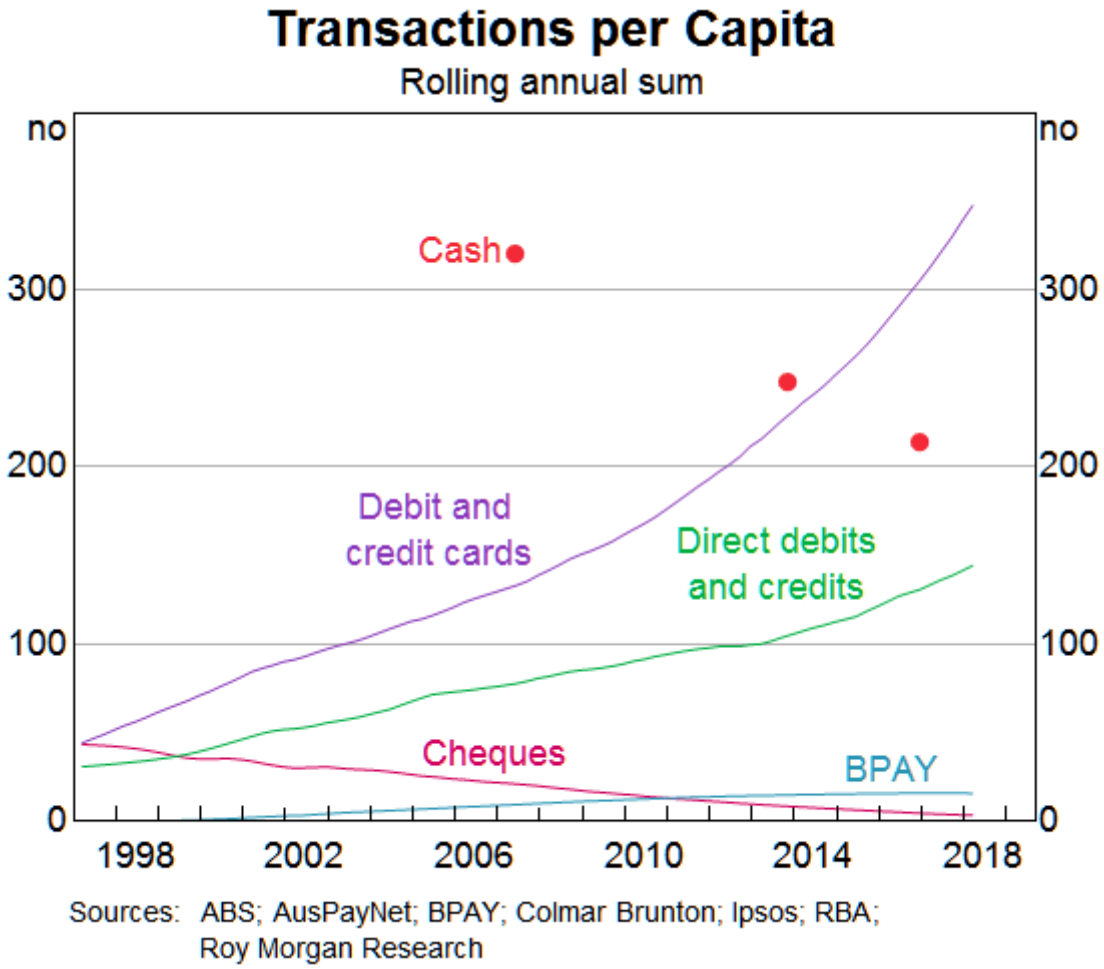
Currently if households wish to hold money, they have two choices. They can hold physical cash, which is a liability of the Reserve Bank, or they can hold deposits in a bank (or credit union or building society), which is an electronic form of money and is a liability of a commercial bank that is

covered (up to $250,000) by the Financial Claims Scheme. Both forms of money serve as a store of value and a means of payment (assuming the bank deposit is in a transaction account).

Most money is already 'digital' or electronic in form. Currency now accounts for only about 3½ per cent of what we call broad money. The remaining 96½ per cent is bank deposits, which we might call commercial bank digital money.

Furthermore, the use of cash by households in their transactions has been falling in recent years. This next graph shows there has been strong growth over an extended period in the use of cards and other forms of electronic payments. In contrast, the dots, which are from the Bank's Consumer Payments Survey, show a significant fall in the use of cash. In 2007, cash accounted for nearly 70 per cent of the number of household transactions. Nine years later, this had fallen to 37 per cent.

Graph



Clearly, some households are moving away from cash and finding that electronic payments provided by banks better meet their needs. And this trend is likely to continue as the New Payments Platform (NPP), which launched recently, allows banks to offer better services to households – namely real-time electronic payments that give immediate value to the recipient, are easily addressed, are available 24/7 and carry lots more data than currently.

So the question is: 'should the Reserve Bank introduce a new form of cash – an eAUD as the Governor called it – to give households an electronic payment instrument issued by the central bank

for their everyday payments?'

Our current thinking is that there would not necessarily be all that much demand for an additional form of money in normal times, though this would presumably depend partly on design decisions such as the interest rate (if any) that would be paid on this money.

But to the extent that there was significant demand, particularly if this occurred at times of financial uncertainty with households switching out of the banking sector, there could be significant implications for the Bank's financial stability mandate. There would also be implications for the structure of the financial sector – for example, it could result in reduced financial intermediation. We would need to think through these implications carefully.

So for the time being at least, consideration of a possible new electronic form of money provided by the Reserve Bank to households is not something that we are actively pursuing. Based on our interactions with our counterparts in other countries, it is also not front of mind for most other advanced economy central banks. An exception is Sweden, where the shift away from the use of cash is significantly more advanced than in Australia and elsewhere. Sweden's Riksbank is studying the issues regarding the possible issuance of an e-krona and expects to report by late 2019.

However, as the Governor indicated in December, there might be a stronger case for considering a new form of central bank liability for use by businesses and financial institutions.

Here it is important to remember that the Reserve Bank already offers electronic balances to financial institutions in the form of Exchange Settlement Accounts (ESAs) at the Reserve Bank. These balances can be passed between financial institutions during the banking day, with the Bank keeping the official record (or the ledger) of account balances.[10] A key function of ESAs is that they provide banks with a risk-free liquid asset for settling payment obligations through the day, to prevent the build-up of large exposures that could threaten financial stability.

However, some stakeholders in the payments area – including some fintechs – have expressed the view that the introduction of another form of central bank balances could be quite transformative. They have suggested the issuance of a new form of digital money that would be accessible to businesses and could be passed around on a distributed ledger. They argue that the availability of another form of central bank settlement instrument could reduce risk and increase efficiency in business transactions. For example, it could allow the simultaneous exchange of money and other assets on blockchains. A central bank digital currency on a blockchain could potentially also enable 'programmable money', involving smart contracts and the simultaneous execution of complex, linked transactions.

Moving in this direction would involve two major changes to current arrangements: it would involve the introduction of a new form of settlement asset and it would presumably involve broader access to central bank money for non-bank institutions. Consideration of the first aspect will require an assessment of issues relating to the technology. Consideration of the second aspect would get into some of the issues that are relevant to thinking about giving households access to electronic central bank money, namely the implications for financial stability and the structure of the financial sector.

As we think more about a model along these lines we will be considering whether the benefits could be equally well facilitated by other means. For example, could there be commercial bank money on blockchains – say Bank X tokens, Bank Y tokens, and the like, rather than RBA digital settlement tokens? Indeed, some models have been sketched out whereby commercial banks would put aside ESA balances at the central bank or would put risk-free assets into special-purpose vehicles, and then issue credit-risk-free settlement tokens for use by their customers. We will also need to think about whether the possible use-cases that have been proposed really need central bank money on a blockchain, or if they might also be possible using other real-time payment rails – perhaps the NPP. At the moment, it does not appear that a strong case has emerged for us to provide this new form of central bank money, but we have an open mind.

Conclusion

Before I finish I should note that my talk today has not explicitly addressed the merits of cryptocurrencies as investments. On this issue, I think the various risks are very well summed up by the final words on a page on ASIC's MoneySmart website: 'If you decide to trade or use virtual currencies you are taking on a lot of risk with no recourse if things go wrong.'

These risks acknowledged, cryptocurrencies and distributed ledgers are fascinating developments both from a payments and a broader economic perspective. The Reserve Bank will be continuing to study their implications and we are very interested in continuing to interact with entities, both large and small, that are active in this area.

Thank you for the invitation to speak on this topic today. I look forward to any comments or questions.

Endnotes

[*] A number of colleagues have contributed to this work, especially Jiamin Lim, Cameron Dark and David Emery.

[1] See, for example, BIS (Bank for International Settlements) (2018), 'Central bank digital currencies', report submitted by a working group established by the Committee on Payments and Market Infrastructures and the Markets Committee, No 174, March. It might also be noted there is a rather critical assessment of cryptocurrencies by the BIS in its recent Annual Report.

[2] The Bank has also published an Explainer on cryptocurrencies on our website.

[3] I will use the lower case for all references to bitcoin, though it is also possible to capitalise Bitcoin when it refers to the system and use lower case for bitcoin when referring to the currency.

[4] Some may argue that some of the flaws in bitcoin that I discuss today have been resolved in some newer cryptocurrencies. However, these others have not yet gained significant traction and bitcoin remains the largest cryptocurrency. Furthermore, a key point here is that cryptocurrency protocols are easily replicated and modified (and potentially improved on). So even if someone happens to be bullish about distributed ledgers and blockchain as general concepts, they should be aware that the value of any currently fashionable cryptocurrency could easily fall to zero in the future if it falls out of use or favour.

[5] Currently about 70 per cent of the computing power in the bitcoin system is controlled by the five largest mining pools. Concentration of mining power raises the possibility of '51 per cent attacks' whereby dishonest nodes representing a significant share of computing power attempt to subvert the system, either to take bitcoin from other users (a 'double spending' attack) or to deliberately cause a lack of confidence in the system. There are a large number of papers on this topic; for a recent contribution see Eric Budish (2018), 'The Economic Limits of Bitcoin', NBER Working Paper No 24717. While such attacks had previously been considered to be a largely theoretical risk, there was a successful attack in May on the Bitcoin Gold system (an offshoot or 'hard fork' of bitcoin) which reportedly transferred US$18 million to the perpetrators.

[6] See <https://digiconomist.net/bitcoin-energy-consumption>.

[7] For example, bitcoin has been described by the General Manager of the Bank for International Settlements as 'a combination of a bubble, a Ponzi scheme and an environmental disaster': see Agustín Carstens (2018), 'Money in the digital age: what role for central banks?', Lecture at the House of Finance, Goethe University, Frankfurt, 6 February.

[8] This measures the number of proposed transactions confirmed by the network. It may underestimate the number of underlying bitcoin transactions because some proposed transactions appear to be batch transactions conducted by intermediaries – for example, they may show a single large payment from one address and many small payments to different addresses (or vice versa).

[9] See Philip Lowe (2017), 'An eAUD?', Address to the 2017 Australian Payment Summit, Sydney, 13 December.

[10] Indeed, to support the NPP, the Bank is now providing settlement balances on a 24/7 basis, through the Fast Settlement Service.