The economics of digital currencies

By Robleh Ali of the Bank's Financial Market Infrastructure Directorate, John Barrdear of the Bank's Monetary Assessment and Strategy Division, and Roger Clews and James Southgate of the Bank's Markets Directorate.[1]

- Although digital currencies could, in theory, serve as money for anybody with an internet-enabled device, at present they act as money only to a limited extent and only for relatively few people.
- The economics of the schemes as currently designed, both in terms of individuals' incentives and at a macroeconomic level, pose significant challenges to their widespread adoption.
- Digital currencies do not currently pose a material risk to monetary or financial stability in the United Kingdom. The Bank continues to monitor developments in this area.

Overview

Digital currencies represent both innovations in payment systems and a new form of currency. This article examines the economics of digital currencies and presents an initial assessment of the risks that they may, in time, pose to the Bank of England's objectives for monetary and financial stability. A **companion piece provides an introduction to digital currency schemes**, including some historical context for their development and an outline of how they work.

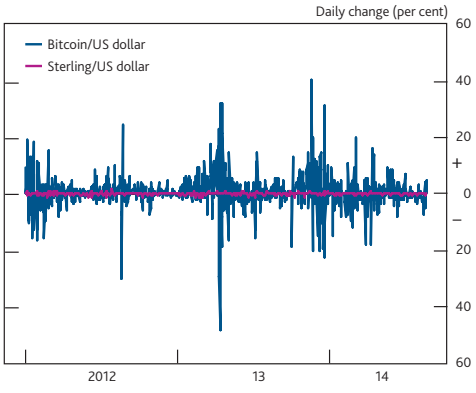
From the perspective of economic theory, whether a digital currency may be considered to be money depends on the extent to which it acts as a **store of value**, a **medium of exchange** and a **unit of account**. How far an asset serves these roles can differ, both from person to person and over time. And meeting these economic definitions does not necessarily imply that an asset will be regarded as money for legal or regulatory purposes. At present, digital currencies are used by relatively few people. For these people, data suggest that digital currencies are primarily viewed as stores of value — albeit with significant volatility in their valuations (see **summary chart**) — and are not typically used as media of exchange. At present, there is little evidence of digital currencies being used as units of account.

This article argues that the incentives embedded in the current design of digital currencies pose impediments to their widespread usage. A key attraction of such schemes at present is their low transaction fees. But these fees may need to rise as usage grows and may eventually be higher than those charged by incumbent payment systems.

Most digital currencies incorporate a pre-determined path towards a fixed eventual supply. In addition to making it extremely unlikely that a digital currency, as currently designed, will achieve widespread usage in the long run, a fixed money supply may also harm the macroeconomy: it could contribute to deflation in the prices of goods and services, and in wages. And importantly, the inability of the money supply to vary in response to demand would likely cause greater volatility in prices and real activity. It is important to note, however, that a fixed eventual supply is not an inherent requirement of digital currency schemes.

Digital currencies do not currently pose a material risk to monetary or financial stability in the United Kingdom, given the small size of such schemes. This could conceivably change, but only if they were to grow significantly. The Bank continues to monitor digital currencies and the risks they pose to its mission.

Summary chart Bitcoin price volatility



Sources: Bank of England and the BitStamp exchange, via http://bitcoincharts.com.

Click here for a short video that discusses some of the key topics from this article.

(1) The authors would like to thank Victoria Cleland, Will Abel and Danny Eckloff for their help in producing this article.

This article explores the economics of digital currencies — schemes that combine new payment systems with new currencies — and provides an initial view on the consequent implications for the Bank of England's objectives to maintain monetary and financial stability in the United Kingdom. Any potential risks to monetary or financial stability posed by digital currencies will depend on how widely they are used, both today and in the future. The article therefore begins by examining the extent to which digital currencies are currently used as a form of money. As part of evaluating the likely growth in digital currencies' usage over time, it next examines the sustainability of the low transaction fees offered by digital currencies at present.

In order to explore the macroeconomic implications of digital currencies, the article also considers a hypothetical — and extremely unlikely — scenario in which a digital currency with a fixed eventual money supply were to achieve dominant usage in an economy, supplanting the existing monetary system. The consequences of such an arrangement are examined, together with some possible responses. Finally, this article provides an initial view on current and possible future risks to monetary and financial stability that might be posed by digital currencies.(1) A short video explains some of the key topics covered in this article.(2)

Setting the context: the emergence of digital currencies

A companion piece to this article, '**Innovations in payment technologies and the emergence of digital currencies**', provides an introduction to these schemes.(3) It details the historical development of modern monetary payment systems; how digital currencies differ from these; and potential benefits of the technology underlying digital currencies beyond use as a payment system. This section offers some context by giving a brief summary of the key points from the companion piece to this article.

Evolution in payment systems and money

Money is essential to a modern economy, since it is used in virtually all the transactions that underlie economic activity. But what is accepted in payment has changed over time, and so have the ways in which payments are made. The exchange of coins made of precious metals was one early method of making payments in a number of economies, including the United Kingdom. The use of precious metals as money was gradually superseded: first by receipts for gold lodged with goldsmiths, then by banknotes redeemable in precious metals, and nowadays by banknotes whose value depends not on gold but on the monetary policy of the issuing central bank. Most money now takes the form of bank deposits, originally recorded in physical ledgers but now entered electronically onto banks' books. Payments between customers of the same bank can be settled by entries in that bank's accounts. But payments between customers of different banks are put into a central clearing system, with balances between banks settled by transferring claims on that central entity — a role typically played by the central bank of a given economy.

More recently, new schemes — 'cryptocurrencies' or 'digital currencies'(4) — have emerged that combine both new decentralised payment systems and new currencies. The first of these schemes, and still the most prominent at the time of writing, is Bitcoin. In some ways, digital currencies resemble — and are intended to resemble — earlier forms of money and of payment systems. Their creation is not controlled by central banks and they allow payments to be made directly between payer and payee without the use of any intermediaries (such as commercial banks). They do not require users to disclose which holdings of digital currency they control, thereby approaching the anonymity of banknotes for electronic payments.

The key innovation: the distributed ledger

The key innovation in this regard is the introduction of a 'distributed ledger', which allows a digital currency to be used in a decentralised payment system. Any digital record of currency opens up the possibility that it may be copied and spent more than once. With conventional bank deposits, banks hold the digital record and are trusted to ensure its validity. With digital currencies, by contrast, the ledger containing the record of all transactions by all users is publicly available to all. Rather than requiring users to have trust in special institutions, reliance is placed on the network and the rules established to reliably change the ledger.

The way in which consensus is reached regarding additions to the ledger — that is, which transactions are accepted as valid — is addressed in the companion article, but the basic process for cryptocurrencies is as follows. A user, wishing to make a payment, issues payment instructions which are disseminated across the network of other users. Standard cryptographic techniques make it possible for users to verify that the transaction is valid — that the would-be payer owns the currency in question. Special users in the network, known as 'miners', gather together blocks of transactions and compete to verify them. In return for this service, miners that successfully verify a block of transactions receive both an allocation of newly created currency and any transaction fees offered voluntarily by parties to the transactions under question.

When blocks of transactions are verified, they are added to the ledger (the 'block chain'). A key design goal of digital

(1) Other issues, such as those concerning consumer protection, taxation and money laundering, are beyond the scope of this article. Some publications from other institutions regarding some of these issues are cited at the end of the article.
(2) http://youtu.be/rGNNiTaC2xs.
(3) See Ali *et al* (2014).
(4) The two concepts are not strictly identical. There currently exist some digital currencies that do not rely on cryptographic techniques to achieve consensus (such as Ripple), but all cryptocurrencies are digital currencies.

currencies is to balance incentives carefully in order to make it more profitable to participate in the network honestly than to try to get fraudulent transactions accepted. To this end, a cost is imposed on making changes to the ledger: more concretely, miners must devote computing resources to mathematical puzzles that are hard to solve, but the answers to which are easy to check. Those contributing greater computing power will, on average (but not always), solve the puzzle first and reap the reward. So long as no one miner, or pool of miners, attains a sustained majority of computing power, those transactions that have been verified will continue to be accepted as valid.

Digital currencies as money

This section examines the extent to which digital currencies may be thought of as money. It first describes a key distinction between fiat money and digital currencies in the manner of their creation. It then considers the main functions of money and provides some analysis of the extent to which digital currencies currently serve these functions.

Digital currencies versus fiat money: how are they created?

As explained by McLeay, Radia and Thomas (2014), money in the modern economy may be thought of as a series of claims, or 'IOUs'. Deposits held at commercial banks are an IOU, being a liability for the bank and an asset for the account holder. Most money is held as bank deposits and the principal way that new money is created is through the creation of loans. Whenever a bank makes a loan, it simultaneously creates a matching deposit in the borrower's bank account, thereby creating new money.(1) Banknotes issued by a central bank are also a special form of non-convertible claim, of the physical bearer on the central bank — and are liabilities of the central bank and assets to the noteholder.

In contrast to commonly used forms of money such as banknotes or bank deposits, digital currencies are not a claim on anybody. In this respect, they can therefore be thought of as a type of commodity. But unlike physical commodities such as gold, they are also intangible assets, or *digital commodities*. Digital currencies have meaning only to the extent that participants *agree* that they have meaning. That agreement takes the form of a public ledger and a process for how changes to it are made, including the creation of new currency. Not being an IOU or liability of the central bank (or the state) does not prevent digital currencies from being used as money (see below), but it does mark an important difference between them and national currencies.

Most existing digital currencies incorporate strict rules that govern their creation, following a pre-determined path to a fixed eventual total supply.(2) For example, there are currently a little over 13 million bitcoins in circulation and that system's protocol dictates that there will be an eventual total of 21 million, which should be largely reached by around 2040.

Among most digital currencies, new currency is allocated to users that contribute computing resources to the verification of transactions on the network. In some ways — and to the extent that digital currencies serve as money — this allocation is similar to *seigniorage* (the creation of monetary value minus the cost of its creation).(3) But it differs from seigniorage in the classic sense as, rather than accruing to the government, it is an explicit payment of new currency to the private sector in return for the verification of earlier transactions.

The three functions of money

Throughout history there have been many different manifestations of money, both physical and electronic. Economic theory identifies money through the role that it plays in society, and, in particular, the extent to which it serves the following purposes:

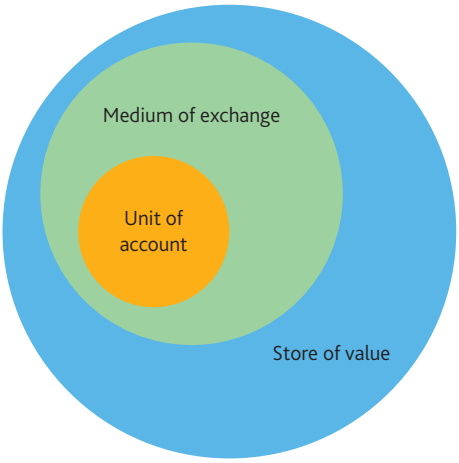
- **A store of value** with which to transfer 'purchasing power' (the ability to buy goods and services) from today to some future date.
- **A medium of exchange** with which to make payments.
- **A unit of account** with which to measure the value of any particular item that is for sale.

It is not always the case that a given asset serves, or categorically does not serve, these functions. Different assets may, at various times, play some or all of these roles. And they may offer them for some people, but not for others. For example, Radford (1945) documents that cigarettes served all three of these roles within prisoner of war camps during the Second World War. Furthermore, meeting these economic definitions does not necessarily imply that an asset will be regarded as money for legal or regulatory purposes.

The functions of money may be considered to operate in a hierarchy, as depicted in **Figure 1**. There are many assets that people view as stores of value — houses, for instance — that are not used as media of exchange. By comparison, an asset can only act as a medium of exchange if at least two people (as parties to a transaction) are prepared to treat it as a store

(1) McLeay, Radia and Thomas (2014) also explain that money creation is constrained by banks' own internal risk appetite, regulatory restrictions, the demand for credit by households and businesses, and — most importantly — the application of monetary policy by the central bank to adjust interest rates in order to achieve a specific inflation target.
(2) Some digital currencies are created entirely at their inception (such as Ripple), while a small number of existing cryptocurrency schemes, particularly among those making use of 'proof of stake' systems, may allow for permanent growth in the money supply.
(3) Note that for digital currencies the cost of having the new allocation accepted by the rest of the network (which is significant) is distinct from the cost of creation (which is approximately zero).

Figure 1 The three functions of money



of value, at least temporarily. Finally, for an asset to be considered a unit of account, it must be able — in principle, at least — to be used as a medium of exchange across a variety of transactions between several people and as such represents a form of co-ordination across society. For this reason, some economists consider the operation as a unit of account to be the most important characteristic of money. Indeed, it is commonly argued that a defining feature of monetary policy lies in central banks' control of the unit of account (Woodford (2003)).

Are digital currencies money?

The extent to which an asset serves the various roles of money varies from person to person and over time. **In theory, digital currencies could serve as money for anybody with an internet-enabled computer or device. At present, however, digital currencies fulfil the roles of money only to *some* extent and only for a small number of people. They are likely at present to regularly serve all three purposes for perhaps only a few thousand people worldwide, and even then only in parallel with users' traditional currencies**. The remainder of this section first examines how widely digital currencies are used before assessing this usage against the three functions outlined above.

How widely are digital currencies used?

It is difficult to estimate the number of people that own or use digital currencies. The largest and most widely used scheme is Bitcoin. As of 9 July 2014, there were almost 41 million addresses listed on the Bitcoin block chain, but only 1.6 million that contained a balance of more than 0.001 bitcoins (roughly £0.35). This figure will still overstate the number of users, however, as each user may possess any number of wallets and each wallet may hold any number of addresses.

Over the 30 days to 20 August 2014, almost 60% of Bitcoin trading with traditional currencies was against the Chinese renminbi, with 32% traded against the US dollar and 3% against the euro. Only 1.2% of trading was against sterling.(1) If the number of Bitcoin users in each country is proportional to the trading of that country's currency with Bitcoin, then this would suggest an upper limit of about 20,000 people in the United Kingdom that have any significant holding of bitcoins. It is further estimated that across all UK users, as few as 300 transactions may occur per day. It is important to emphasise the uncertainty about these figures, however.(2)

Assessing digital currencies against the three functions of money

An asset's worth as a **store of value** rests on people's beliefs regarding its future supply and demand. Although a constrained supply is largely assured with digital currencies, prospects for future demand are far less certain. Since digital currencies lack any intrinsic demand (for use in production or for consumption) and no central authority stands behind them, an opinion about their future demand should largely rest on (i) a belief about their future use as media of exchange and (ii) a belief that they will continue to remain in demand even further into the future.(3) A brief discussion of some other relevant considerations is provided in the box on page 280.

While the non-zero prices of digital currencies reveal that they do have value for non-trivial numbers of users, they appear to be poor *short-term* stores of value given the significant volatility in exchange rates with traditional currencies. **Chart 1** shows the daily change of the prices of bitcoins (in blue) and sterling (in magenta) — both expressed in terms of US dollars — since the start of 2012. The standard deviation of daily moves for bitcoin is roughly 17 times greater than that for sterling. The worth of bitcoin as a *medium* or *long-term* store of value, however, depends on the strength of demand over time, which will in turn depend on users' evolving beliefs about the ultimate success of the digital currency.

One measure of the extent to which a currency is being used as a **medium of exchange** is the number of retailers that are prepared to accept it in payment. At present, there are several thousand retailers worldwide (predominantly, but not exclusively, internet-based providers) that are willing to receive payment in bitcoins.

The willingness of a retailer to accept a digital currency does not by itself imply, however, that the facility is widely used. A more indicative measure of a digital currency's worth as a medium of exchange is the number of transactions carried out

(1) These figures derive from the most active exchanges listed on http://bitcoincharts.com. Note that there may be unlisted exchanges that compete with these.
(2) This calculation also assumes, for example, that transaction rates are similar between 'My Wallet' users and users in the United Kingdom in general.
(3) A willingness to hold such an asset in period T requires a belief that it will be accepted by other people in period $T+1$, which in turn requires that in period $T+1$ it will be believed that the asset will be accepted by yet other people in period $T+2$, and so on.

Some factors influencing the prices of digital currencies

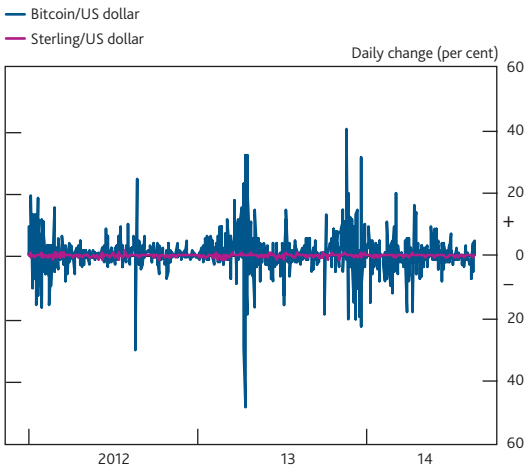
The valuation of a digital currency that is, at least in principle, able to be used as a medium of exchange needs to take a wide variety of considerations into account. These include:

- The expected real return of holding the digital currency (that is, the nominal interest rate minus expected price inflation), relative to other options.
- Any risks associated with holding the digital currency relative to other currencies, including risks of theft or fraud, and price volatility.
- The relative benefits of using the digital currency as a medium of exchange when compared to traditional systems, including availability, transaction fees and degrees of anonymity.
- Any time constraints or costs associated with switching wealth between the digital currency and more traditional assets (including sterling).
- Any non-monetary concerns, such as an ideological preference for one particular currency.
- A view on how much other people value the currency (based on the above factors) and how this is expected to change in the future.

It is not generally possible to express all of these elements in a single mathematical model. When limiting attention to only the quantifiable factors, standard economic theory suggests that, under certain conditions,(1) the expected real rates of return on any two assets that might serve as money should be equal after adjusting for risk and the costs and benefits associated with using them for spending. For example, holding all else equal, a currency with lower transaction fees may be expected to offer a lower real rate of return (since holders are also compensated via the lower fees), while one with greater price volatility should offer a higher return (to compensate holders for the extra risk).

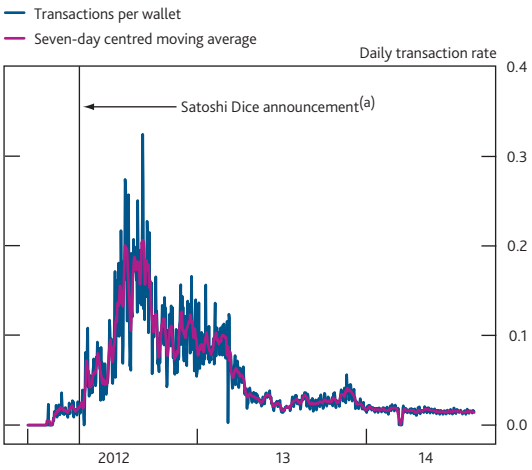
(1) For example, these conditions include a requirement that everybody have access to the same information, face the same costs in transferring their wealth between assets and are able to do so instantly.

Chart 1 Bitcoin price volatility



Sources: Bank of England and the BitStamp exchange, via http://bitcoincharts.com.

Chart 2 Daily Bitcoin transaction rate per wallet



Sources: 'My Wallet' service offered by http://blockchain.info and Bank calculations.

(a) Refers to the announcement of Satoshi Dice, a popular bitcoin-based gambling website.

by its users over a given period of time. While it is not possible to observe the transaction rate per user in any digital currency, there are some data for the transaction rate per *wallet* on the Bitcoin network. **Chart 2** presents this measure among users of 'My Wallet', a popular wallet-hosting service. Like other measures of transaction rates,(1) it rose in the first half of 2012 following the announced launch of Satoshi Dice (a popular bitcoin-based gambling website), but has since fallen to quite low levels.(2) So far in 2014, there have been, on average, fewer than 0.02 transactions per day for wallets held with 'My Wallet' (roughly one transaction per day for every 65 wallets). Most users appear to be simply holding their bitcoins rather than using them for day-to-day transactions.

There is little evidence of any digital currency being used as a **unit of account**. Although a small number of transactions between individuals will occur in which the parties negotiate and agree a price in bitcoins, these are believed to be isolated and largely unconnected. Retailers that quote prices in bitcoins appear to usually update those prices at a high frequency so as to maintain a relatively stable price when expressed in traditional currencies such as US dollars or sterling. Indeed, start-up companies seeking to offer bitcoin

(1) A similar pattern emerges when looking at transaction rates per unique address used.
(2) Although eponymous, Satoshi Dice is not thought to be associated with Bitcoin developer Satoshi Nakamoto.

payment facilities typically offer retailers the opportunity to price entirely in fiat currencies, using the digital currency only temporarily as a payment system. The Bank is not aware of any business that accepts bitcoins in payment that also maintains its accounts denominated in that digital currency.

The sustainability of digital currencies' low transaction fees

This section moves beyond the question of whether digital currencies currently serve the roles of money to consider the extent to which they may come to act as money for an increasing number of people over time. The most relevant question in this regard is the extent to which people may come to use digital currencies as a means of payment.

A significant feature of digital currencies — and the primary driver of interest from retailers in accepting them in payment — is the promise of low transaction fees. At present, digital currency payments require transaction fees that are typically lower than those needed for retail electronic payments (such as paying by credit card) and international transfers using traditional currencies (and centralised payment systems).

Why transaction fees are currently low

Importantly, fees are low for digital currency payments despite the fact that, as currently designed, the marginal cost of verifying transactions by miners is generally *higher* than that for centralised payment systems. These higher marginal costs are due to increasing returns to scale in the operation of computer servers: it would generally be more cost efficient to process all transactions centrally. Moreover, while the marginal costs for traditional payment systems may be expected to remain broadly constant over time, those incurred by digital currency miners may be expected to rise as their usage increases and — in addition to that — to increase over time because of an incentive for overinvestment in new equipment. These drivers of marginal costs are explained in more detail in the box on page 282.

Low transaction fees for digital currency payments are largely driven by a subsidy that is paid to transaction verifiers (miners) in the form of new currency. The size of this subsidy depends not only on the current price of the digital currency, but also on miners' beliefs about the future price of the digital currency. Together with the greater competition between miners than exists within centralised payment systems, this extra revenue allows miners to accept transaction fees that are considerably below the expected marginal cost of successfully verifying a block of transactions.(1)

The sustainability of low transaction fees

In the *near term*, the subsidies in the form of new currency that miners receive create an incentive for miners to promote the wider adoption of the digital currency they support, since anticipated increases in demand should help to drive up the expected value of their future revenue from new currency. A willingness to accept extremely low transaction fees today can then persist so long as miners' optimism about future increases in system usage remains.

The eventual supply of digital currencies is typically fixed, however, so that in the *long run* it will not be possible to sustain a subsidy to miners. Digital currencies with an ultimately fixed supply will then be forced to compete with other payment systems on the basis of costs. With their higher marginal costs, digital currencies will struggle to compete with centralised systems unless the number of miners falls, allowing the remaining miners to realise economies of scale. **A significant risk to digital currencies' sustained use as payment systems is therefore that they will not be able to compete on cost without degenerating — in the limiting case — to a monopoly miner, thereby defeating their original design goals and exposing them to risk of system-wide fraud**.

The macroeconomic problems of a fixed money supply: a digital currency thought experiment

Digital currencies do not currently serve a substantial role as money in society and, as shown in the previous section, face significant challenges to their widespread use over the long run. This means that it is very unlikely that a digital currency, as currently designed, would be used as the predominant form of money in any economy.(2) And as explained in this section, economic theory would suggest that social welfare would be lower in a hypothetical economy based on a current digital currency compared with a second hypothetical economy based on a fiat money system.

In most existing digital currency schemes, the future path of supply is pre-determined and governed by a protocol that ensures that the eventual total supply will be fixed. This has the effect of removing any discretion from the determination of the money supply. This would pose a number of problems for the macroeconomy: for example, it could contribute to deflation in the prices of goods and services (and wages). Importantly, the inability of the money supply to vary in response to demand would likely cause welfare-destroying volatility in prices and real activity.

(1) In particular, so long as miners expect the real marginal revenue from new currency to rise faster than their real marginal costs, there is no need for them to charge transaction fees (or, where fees are already being offered, to demand higher fees).
(2) Other current impediments to the widespread usage of digital currencies include: general unfamiliarity with the technology; the insufficient user-friendliness of applications associated with day-to-day use of the schemes; the increased need for personal security relative to deposits held with regulated institutions; and the volatility of digital currency exchange rates. Note that all of these issues are subject to ongoing investigation and development by the supporters of digital currencies.

The rising cost of mining

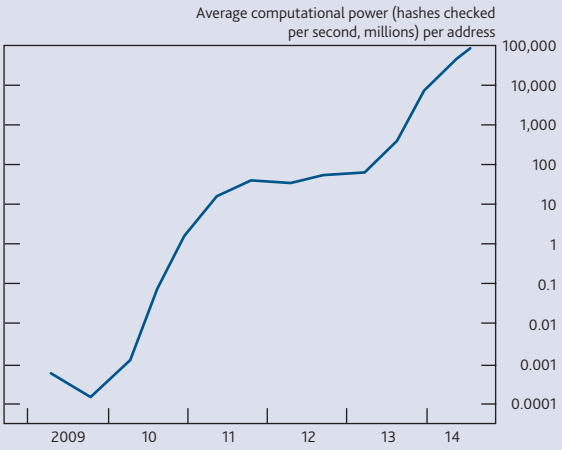
This box outlines two reasons why the underlying marginal cost of verifying a block of transactions in a digital currency may be expected to increase over time. The first relates to increases in the usage of digital currencies as media of exchange, while the second is due to an incentive for miners to collectively overinvest in computer hardware.

Digital currencies are designed to maintain a roughly constant time between transaction blocks (ten minutes in the case of Bitcoin — see the companion article for more details). As usage of the scheme rises so that the transaction rate increases, the number of transactions per block — and, hence, the size of each block — must therefore also increase.(1) This imposes both a direct cost on miners by requiring that they use more bandwidth from their internet service providers, and an indirect cost by raising the probability that the block will be 'orphaned' — that is, replaced by another block that is successfully verified at a similar time and which eventually becomes universally accepted.(2)

Moreover, to the extent that miners' expected marginal revenue exceeds their expected marginal costs, miners' costs are likely to increase over time. This should occur even if no additional people start to mine and independently from any increase in the number of transactions per block. This is because distributed systems involve a negative externality that causes overinvestment in computer hardware. The negative externality emerges because the expected marginal revenue of *individual* miners is increasing in the amount of computing power they personally deploy, but the difficulty of the problem they must each solve (and hence their marginal cost) is increasing in the total amount of computing power *across the entire network*. Individual miners do not take into account the negative effect on other miners of their investment in computing resources. Economic theory would therefore suggest that in equilibrium, all miners inefficiently overinvest in hardware but receive the same revenue as they would have without the extra investment.

It is not possible to observe the average amount of computational power per miner in any given digital currency, but it is possible to calculate the computational power per *address* in the Bitcoin network. This is shown in **Chart A** as 'hashes checked per second', referring to the number of candidate solutions checked to the puzzles repeatedly posed to miners (see the companion article for more details). So long as the number of addresses per user and the share of users that act as miners are both roughly constant over time, then changes in this measure will capture changes in the average computational power deployed per miner. The average computational power per miner has indeed increased markedly, rising by a factor of more than 200 in the year to 9 July 2014.

Chart A Computational power per address in the Bitcoin network (log scale)(a)



Sources: http://bitcoinrichlist.com, http://blockchain.info and Bank calculations.

(a) Excludes addresses with balances of less than 0.001 bitcoins. Points are taken at intervals of 25,000 blocks. Hash rates are taken as averages over the week preceding each block.

(1) This is because each time a miner broadcasts their success at verifying a block they must include a copy of all of the transactions within that block so that other miners can confirm its validity.
(2) Since the time it takes for a message to be shared across a network is increasing in the size of that message, this means that blocks with many transactions in them are transmitted more slowly, leading to a greater chance that they will be orphaned.

When the prices of goods and services are falling, households have an incentive to postpone or even abandon spending plans. Expected price deflation also raises the minimum return an entrepreneur must offer in order to raise funding for investment in physical capital. Economic theory therefore predicts both aggregate demand and potential output to fall and, if the deflation is indefinite, the unemployment rate to be permanently higher.

Although current digital currency schemes have largely fixed money supplies, there is no technical reason why they could not adopt 'smarter' rules that seek to provide ongoing subsidies to miners and remove the incentive to postpone or abandon spending. The simplest example would be a rule in which the money supply were permitted to grow at a constant rate per year, similar to that advocated by Friedman (1959, 1969). Supply would no longer be fixed, but in principle there would still be no discretionary management of the currency.(1)

(1) In the 1970s and 1980s, official policymakers in a number of countries did attempt to 'tie their own hands' by adopting targets for the growth of money. But such rules are generally suboptimal from a welfare perspective. Indeed, they were typically abandoned following difficulties in defining and observing a stable measure of demand for money and a predictable relationship between the growth of money and inflation, ultimately in favour of 'constrained discretion' in the form of inflation targets.

A second problem derives from a pre-determined supply's inability to respond to variation in demand. Aggregate demand for money is volatile, for reasons that may be seasonal (such as Christmas shopping), cyclical (such as recessions) or structural (such as from technology improvements). If the money supply cannot respond to these variations, volatility in prices will ensue, causing welfare-destroying volatility in economic activity.

In order to address a need to respond to variation in demand, a more flexible rule would be required. For example, the growth rate of the currency supply could be adjusted to respond to transaction volumes in (close to) real time. Alternatively, a decentralised voting system could be developed. Finally, variant schemes could embrace existing monetary systems by seeking to match official broad money data or to target a fixed exchange rate, although this would require the abandonment of part of the schemes' original ideology.

Monetary and financial stability

Current situation

At present, digital currencies do not pose a material risk to monetary or financial stability in the United Kingdom. Although these schemes have experienced a number of brief and very rapid periods of growth, they nevertheless remain very small. It is estimated that there is less than £60 million worth of bitcoins circulating within the UK economy, which represents less than 0.1% of sterling notes and coin and only 0.003% of broad money balances.(1) It is estimated that as few as 20,000 people in the United Kingdom currently hold any bitcoins, and that as few as 300 transactions may be conducted by those people per day.

Potential future risks

Nevertheless, it is possible to conceive of risks that may develop over time. This section provides an initial analysis of some monetary and financial stability risks that could emerge if digital currencies grew significantly and there were no mitigants implemented. Over time, although risks to financial stability are considered unlikely, they would, in general, be more likely to emerge (and sooner) than those to monetary stability. Risks to monetary stability could, in theory, emerge if a digital currency were to achieve widespread usage, but this is extremely unlikely over any foreseeable horizon under the design of current digital currencies.

Financial stability

The Bank's responsibility for financial stability is set out in the Financial Services Act 2012. The Act established an independent Financial Policy Committee (FPC), a new prudential regulator as a subsidiary of the Bank, and created new responsibilities for the supervision of financial market infrastructure.(2) This responsibility for financial stability does not entail targeting the prices of different asset classes, but a price crash in assets to which households, companies or financial institutions had large enough exposures could lead to financial distress and an impairment to the provision of critical financial services.

The prices of digital currencies can be very volatile, as illustrated in **Chart 1** for Bitcoin, and a price crash is not inconceivable. The total value of all digital currencies is too small to pose a threat in this way at present, but further increases in their prices cannot be ruled out. If marked increases in prices were to occur, it is possible that the total valuation may become large enough such that a price crash might have implications for financial stability in this manner.

The impact of any price crash would also, at present, be limited to the direct holders of the alternative currencies. But these effects could be magnified under a number of potential scenarios, such as:

- If a holder of digital currencies had increased their exposure by first borrowing money from someone else. A price crash in this scenario would have the potential to impose losses not only on the direct holders of digital currencies but also on those who had lent to them.

- If a systemically important financial institution were to have a significant unhedged exposure to a digital currency.(3)

- If a digital currency were to become entwined with financial instruments such as derivatives contracts, creating a mechanism whereby both the direct users of a digital currency and other financial market participants could hold leveraged positions against the currency. This could result in the total market exposure to digital currencies far exceeding the market value of digital currencies so that a price crash would have a magnified impact on the economy, and on a wider part of the economy than just direct participants.

A number of risks to financial stability could also emerge if digital currencies grew to a point where they played a significant role as a payment system. One new risk, specific to digital currencies, would be the possibility of system-wide fraud. If a single miner, or coalition of miners, came to control

(1) Figures are for July 2014. Note that 'broad money' refers to M4, excluding intermediate other financial corporations.
(2) The FPC is a committee of the Bank responsible for the stability of the financial system as a whole, the Prudential Regulation Authority (PRA) for the supervision of banks, building societies, credit unions, insurers and major investment firms and the Financial Market Infrastructure Directorate of the Bank for the oversight and supervision of infrastructure, including systemically important payment systems. See Murphy and Senior (2013) for more detail.
(3) Exchange rate risk with digital currencies is difficult to hedge (Yermack (2013)), which suggests that additional loss-absorbing capital may be required in that scenario.

a sustained majority of the computing power in a digital currency, that group would be able to control which payments were permitted or even to create fraudulent 'double spend' payments.(1) A related risk lies in the fact that the incentives implied by digital currencies are not yet fully understood. If a digital currency became systemically important before all incentives built into its design were completely mapped out, there would be a risk that a hitherto unrealised opportunity for disruption may be discovered and exploited.

Finally — and while not considered likely in the foreseeable future — financial stability could also be put at risk if fractional reserve banking were to emerge in an unregulated fashion above a digital currency, because of the need to protect against bank runs. Liquidity insurance would be another issue in this scenario, especially in the absence of any central bank able to create the base money for such a system in the event of a bank run. The box on page 285 considers this scenario in more detail.

Monetary stability

The greatest risk that could, in theory, be posed by digital currencies to monetary stability in the United Kingdom is an erosion of the ability of the Monetary Policy Committee (MPC) to influence aggregate demand as part of its remit to achieve 2% inflation in the consumer prices index.(2) The MPC traditionally influences aggregate demand by adjusting Bank Rate, the interest rate paid on commercial banks' reserves at the Bank of England, up and down. There are several ways in which monetary policy affects aggregate demand, but one key channel is via the transmission of changes in Bank Rate to the interest rates offered by commercial banks to savers and borrowers. The subsequent spending decisions of households and businesses then influence the aggregate amount of economic activity and inflationary pressure in the economy.

Both the extent and the distribution of usage of digital currencies are of relevance in evaluating any risk to monetary stability. If a relatively small share of payments in the United Kingdom were to be made via a digital currency such that many people conducted some transactions in that currency, but made the bulk of their purchases via traditional, sterling-based payment systems, then the MPC would retain its ability to influence the level of aggregate demand across all segments of the economy, and thus achieve its monetary stability objectives.

Alternatively, if digital currency payments were concentrated among a small number of people that sought to transact as far as possible in that currency, then that would amount to a fragmentation of the UK economy. Depending on the trade links between those people and the rest of the population, the Bank's ability to influence demand within that subset of people may potentially be reduced.(3)

The greatest hypothetical risk to monetary stability that might be posed by digital currencies is if the economy were to become, for example, 'Bitcoinised' — where everybody sought to conduct the totality of their day-to-day transactions entirely within the alternative currency and switch into sterling only when strictly necessary for interaction with the state (such as to pay taxes). This would represent a significant change. Since in this extreme scenario all payments would be conducted away from sterling as base money for essentially all of the economy, the Bank's ability to influence price-setting and real activity would be severely impaired. But such an outcome is extremely unlikely given the current impediments to the widespread adoption of current digital currency schemes imposed by their designs and is, in any event, implausible absent a severe collapse in confidence in the fiat currency. It is much more likely that, if further adopted, digital currencies will be used in a limited fashion alongside traditional currencies.

Other relevant issues

This section has focused on potential impacts on the Bank's mission to maintain monetary and financial stability within the United Kingdom. Beyond the Bank's remit, however, there are other issues concerning consumer protection, taxation, money laundering and the possible use of new payment systems and alternative currencies in financing terrorism or other crime. **No comment is made on these other issues here**. Interested readers may wish to consult publications from other authorities, such as:

- HMRC guidance on the tax treatment of digital currencies (HMRC (2014)).
- An opinion issued by the European Banking Authority (EBA (2014)), which discusses a range of possible risks related to digital currencies.
- A report by the Financial Action Task Force (FATF (2014)) on risks related to money laundering and terrorist financing.
- A speech by the Chancellor of the Exchequer (Osborne (2014)) that announced a programme of work by the UK Government to explore 'the potential of virtual currencies and digital money'.

(1) Indeed, temporary control of a majority of computing power has already occurred on a number of occasions within the Bitcoin network, although the Bank is not aware of any evidence that it was achieved with malicious intent.
(2) There are, of course, other potential risks to price stability. For example, if a systemically important payment system, no matter what form of money it transmitted, were to experience a severe outage, then that would represent a shock to which the MPC would need to respond.
(3) An important question in this latter case would be whether the digital currency was still used as a unit of account. Some economists argue that so long as a central bank retains control of the supply of the unit of account, it does not matter the extent to which it is actually used as a medium of exchange or a store of value (Woodford (2003)).

Could a banking system based on a digital currency emerge?

There are significant barriers to any digital currency, as currently designed, becoming the dominant form of money in an economy. This also presents significant challenges to the emergence of a banking system denominated in a digital currency.

Nevertheless, it is at least conceivable that a financial institution could issue IOUs to the public that were denominated in a digital currency. If an institution issuing such claims were to back them one-for-one with actual digital currencies, it would amount to a form of 'narrow banking' — the general public's holdings of assets denominated in the digital currency would not have changed.

In such a setting, and if the digital currency were somehow to achieve widespread usage, then if demand for that digital currency were to grow while its supply remained fixed, an incentive would exist for financial institutions to create extra instruments (for example, by extending loans) that were not fully backed. This would create a form of fractional reserve banking, with the digital currency playing the role of base money and the total claims on issuers the role of broad money. An important question that would then emerge is whether banks could be constrained in their creation of broad money without regulatory oversight or central bank involvement in the management of the underlying base currency.

In this vein, there are some parallels with historical episodes of free banking, in which relatively unregulated banks were able to issue their own banknotes as a form of private money. The record shows that while some free banks did act with restraint, there is a risk of uncontrolled inflation (that is, a fall in the purchasing power of the banknotes) if private issuers overuse their ability to create currency at a very low marginal cost.

Modern-day advocates of a return to free banking, like promoters of digital currencies, have been motivated in part by their disapproval of monetary management as practised by central banks. Advocates suggest that free banks should be obliged to redeem their notes at par against official currency. Any overissuance would, it is said, simply flow back to them.(1) If free banks' notes were not convertible into an official currency, banks would compete to produce the most 'useful' notes — ones that maintained their purchasing power.(2) By contrast, the safeguard offered by digital currency schemes amounts to an undertaking to issue and to recognise new currency only as indicated by an algorithm, which can be amended only with the assent of a majority of computing power on the relevant network.

The historical record shows that overissuance could occur under free banking, sometimes on a massive scale, but this was not always the case. Sometimes free banks exchanged notes with each other at par through a clearing house, as in Scotland before 1845 or in New England through the Suffolk Bank before the US Civil War. Membership of a clearing house was a valuable sign of a bank's soundness, and enabled the clearing house to exert some restraining influence over members' activities.

Although holders of free banks' notes elsewhere in the United States could, in principle, demand that they be redeemed at par, this did not always prevent overissuance. Professional 'money brokers' emerged, whose function was to take bundles of notes to the home offices of the issuing banks for redemption in specie (gold or silver). 'Wild cat banks', however, were set up in 'wild cat country' — areas that were difficult to access — in order to thwart the brokers' efforts. In other cases bank promoters were simply overoptimistic about their prospects. And convertibility was sometimes suspended.

The result was that free banks' notes by no means always traded at par. Indeed, money brokers published news sheets giving the market rate of various banks' notes in relation to specie, based partly on distance from the issuing bank but also on the probability of redemption. Many free banks were also short-lived and some holders of their notes suffered significant losses.

Historically, individual free banks faced a trade-off between overissuance for a quick gain and the benefit of low-cost funding over the long term. Promoters of existing digital currencies have no discretion to 'over issue' (relative to their algorithms). The analogy with free banking might, therefore, become more relevant if digital currencies were in future to adopt more flexible money supply rules.

(1) See, for example, Chapter 2 of Dowd (1993).
(2) See Chapters 8 and 11 of Hayek (1976).

Conclusion

Both digital currencies' status as money and the distributed ledger technology used by them have potential to develop over time. Most digital currencies, at present, deploy fixed eventual money supplies, although this is not strictly an essential feature. Usage of digital currencies is presently very low and, as currently designed, there are a variety of incentive problems that are likely to prevent their widespread adoption in the long run.

Digital currencies do not, at present, play a substantial role as money in society. But they may have the potential to come to exhibit at least some of the functions of money over time. There is little incentive for the pricing of goods and services to change from traditional currencies, however, unless these currencies were to suffer from a wholesale collapse in confidence.

Digital currencies do not currently pose a material risk to monetary or financial stability in the United Kingdom. Should they achieve limited adoption as a payment system, they are unlikely to undermine the Bank's ability to achieve monetary stability. While that could, in theory, change if sterling were abandoned in favour of an alternative currency for a significant fraction of the economy, such a scenario is considered extremely unlikely at present. A variety of potential risks to financial stability could emerge if a digital currency attained systemic status as a payment system, most of which could be addressed through regulatory supervision of relevant parties.

References

Ali, R, Barrdear, J, Clews, R and Southgate, J (2014), 'Innovations in payment technologies and the emergence of digital currencies', *Bank of England Quarterly Bulletin*, Vol. 54, No. 3, pages 262–75, available at www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q301.pdf.

Dowd, K (1993), *Laissez-faire banking*, Routledge, London.

European Banking Authority (2014), 'EBA opinion on 'virtual currencies'', EBA/Op/2014/08.

Financial Action Task Force (2014), 'Virtual currencies: key definitions and potential AML/CFT risks'.

Friedman, M (1959), *A program for monetary stability*, Fordham University Press, New York.

Friedman, M (1969), 'The optimum quantity of money', in *The optimum quantity of money and other essays*, Aldine, Chicago, pages 1–50.

Hayek, F (1976), *Denationalisation of money*, Institute of Economic Affairs, London.

HMRC (2014), 'Revenue & Customs Brief 09/14: Tax treatment of activities involving Bitcoin and other similar cryptocurrencies', available at www.hmrc.gov.uk/briefs/vat/brief0914.htm.

McLeay, M, Radia, A and Thomas, R (2014), 'Money creation in the modern economy', *Bank of England Quarterly Bulletin*, Vol. 54, No. 1, pages 14–27, available at www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q102.pdf.

Murphy, E and Senior, S (2013), 'Changes to the Bank of England', *Bank of England Quarterly Bulletin*, Vol. 53, No. 1, pages 20–28, available at www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2013/qb130102.pdf.

Osborne, G (2014), 'Chancellor on developing FinTech', available at www.gov.uk/government/speeches/chancellor-on-developing-fintech.

Radford, R A (1945), 'The economic organisation of a P.O.W. camp', *Economica*, Vol. 12, No. 48, pages 189–201.

Woodford, M (2003), *Interest and prices: foundations of a theory of monetary policy*, Princeton University Press, Princeton.

Yermack, D (2013), 'Is Bitcoin a real currency? An economic appraisal', *NBER Working Paper No. 19747*.