CONFIDENTIAL

PAYMENTS SYSTEM BOARD

INFORMATION PAPER FOR THE BOARD **MAY 2013 MEETING**

7. International Developments

7.5 Bitcoin

Bitcoin – a 'virtual currency' – has received some recent media attention, driven by large price movements. In April, its traded price on the Tokyo-based Mt.Gox, the largest Bitcoin 'exchange', peaked at US$265 before falling to US$105 within hours and to US$50 within a week; the current price is around US$115.[3] By comparison, Bitcoins traded in a range between US$5 and US$15 during 2012. In addition to increased media interest, the extreme price movements have also led to a number of public enquiries made to the staff about Bank policy in this area.

As with some virtual currencies, Bitcoin is a system for transferring 'real-world' value over the internet. While Bitcoins have some attributes of a national currency (medium of exchange, store of value and unit of account), they are not issued under the authority of any government body and do not have legal tender status in any jurisdiction. Users may transfer Bitcoins among each other in exchange for real goods and services, or for national currencies at a number of Bitcoin exchanges. They can do this by instructing the network to transfer Bitcoins from one virtual 'address' to another, with each transfer verified by a 'private key' that only the owner of the sending address should know.[4] The Bitcoin system is, in essence, a ledger of all such transfers, using cryptography to maintain an accurate record of the changes to ownership of each Bitcoin.

The system has been designed (through an algorithm created in 2009 by 'Satoshi Nakamoto', an anonymous cryptographer or group of cryptographers) to fix the rate of increase in the total number of Bitcoins, which will be limited to 21 million.[5] Assuming that the volume of goods and services bought and sold with Bitcoins continues to increase, the fixed supply has deflationary implications for the system.

Unlike more traditional electronic payment systems, Bitcoin transactions are not processed by any central entity. Instead, transactions are processed and verified through a peer-to-peer network that links each user with all other users. This decentralised structure ensures – and relies on – massive computing power to maintain the integrity of the transaction 'ledger' and provides a means of allocating newly created Bitcoins, based on the computing power contributed by each user, known as Bitcoin 'mining'. Users can remain anonymous since their real-world identities are not attached to the transaction record, similar to the anonymity that can be provided by cash transactions. Indeed, this anonymity has led to Bitcoin becoming a favoured currency for black market transactions. Cross-border transfers of Bitcoins can be made relatively promptly, with relative ease and minimal fees compared with the traditional banking system.[6]

---

3 Mt.Gox accounts for over 80 per cent of all Bitcoin/national currency trades. Its name is an abbreviation of *Magic: The Gathering Online Exchange*, reflecting its background in fantasy gaming.

4 Users manage their addresses and can store their private keys using 'wallets' developed by third-party service providers.

5 At the pre-determined rate of increase, supply will be close to 21 million by around 2040. Each Bitcoin is divisible to 8 decimal places, forming the base unit of account.

6 Senders of Bitcoins may choose to pay a fee to the network to accelerate the verification of the transfer.

In short, users may find the Bitcoin system more attractive for certain transactions than traditional payment systems because of anonymity, ease of use and low transaction costs. However, the anonymous and irrevocable nature of Bitcoin transactions means that users have little or no redress in cases of fraud. The consensus among cryptographers is that the algorithm underlying Bitcoin supply transfers is highly secure, but users are vulnerable to attacks on third-party service providers and exchanges, some of which handle or store users' private keys.

Bitcoin's regulatory status has been the subject of recent consideration. In March 2013, the US Financial Crimes Enforcement Network issued 'guidance' to the effect that money transmitter regulations – with an anti-money laundering focus – apply to the exchange of any newly created virtual currencies for a national currency, and to intermediaries that accept such virtual currencies in order to transfer them to another person. Moreover, the Commodity Futures Trading Commission is reportedly considering whether derivative contracts based on Bitcoins would come under its jurisdiction. By contrast, a 2012 European Central Bank paper examined the potential risks arising from virtual currencies (including Bitcoin) and concluded that, due to their current scale, they pose little risk to the payments system as a whole but do raise some consumer protection concerns.

Risks to the payments system also appear to be limited in the Australian context at this stage. There are currently no Bitcoin exchanges located in Australia, and very few Australian merchants accept Bitcoins (or any other virtual currency) as a payment method for their goods. The volume of Bitcoins purchased with or sold for Australian dollars at Mt.Gox is also relatively small, at an average daily turnover of 1 710 Bitcoin units (around A$100 000 at the average price) during 2013; by contrast, the average daily turnover for US dollar purchase/sales is 86 000 Bitcoin units (around US$6.6 million at the average price).

Payments Policy Department
13 May 2013

INFORMATION NOTE

BITCOIN: REHASHING IDEAS OF STONE AND GOLD[1]

Bitcoin is a 'virtual currency' – essentially a transactions ledger – used to make anonymous, near-instantaneous online transactions. It was created by one or more cryptographer(s) and began operating in 2009. Unlike traditional electronic payment systems (which typically operate through a central infrastructure or administrator), Bitcoin operates through a decentralised peer-to-peer network, with participants interacting directly with each other and verifying transactions themselves; the integrity of the transactions record is protected by multiple levels of cryptography. In this note we describe how Bitcoin works and the policy issues that the system potentially raises, with a focus on its attributes as a payment system. Risks to the payments system (and the economy more generally) are currently limited since Bitcoin remains a niche product, particularly in Australia.

1. Background

Bitcoin is a virtual currency created by 'Satoshi Nakamoto', a pseudonym for either one or a group of cryptographers, in a 2008 paper (see Appendix A for more on virtual currencies).[2] It began operating in 2009 and is one of the first implementations of a decentralised 'crypto-currency', where the supply of bitcoin units and the system of transferring these are protected by cryptography instead of the rules of a central operator or administrator. In essence, the Bitcoin system is a public **ledger** (called the 'block chain') recording the bitcoin units owned by each user and a history of all transfers in the ownership of each unit, with cryptography protecting the record from corruption.[3]

The Bitcoin system is decentralised in that each user is connected to all other users; users transact with each other directly in a peer-to-peer network. Bitcoin's software is open source and is maintained by the Bitcoin Foundation.

1.1 Supply

The supply of bitcoins is modelled on that of a scarce commodity (e.g. gold) and is fixed at 21 million by the algorithm behind the system.[4] The path of growth up to that cap is also pre-determined, and around 11 million bitcoins have been created so far (Graph 1). At its current market price the 'market capitalisation' of Bitcoin is around

---

1 In this note, 'Bitcoin' is used when describing the system in which value is transferred, and 'bitcoin' for the units of value/account.

2 More on Bitcoin's history and creator(s), who 'disappeared' in 2011, can be found in Davis (2011).

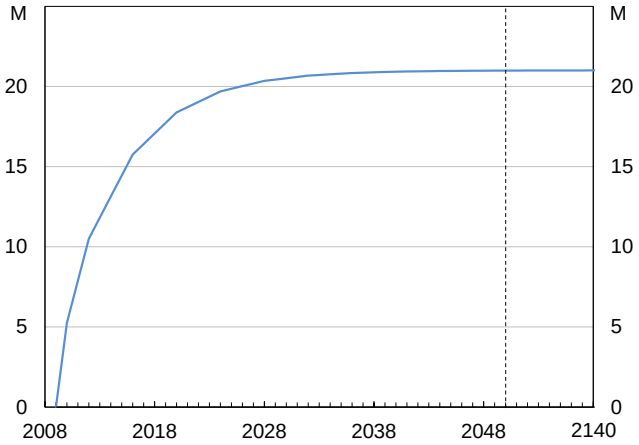
3 Indeed, Bitcoin has been compared to the stone coins of the Island of Yap. The multi-tonne coins were not physically moved; instead, changes to ownership were general knowledge, and therefore even a stone lost at sea could be used as a 'coin' – see Friedman (1991). Others have referenced Kocherlakota (1998) who argues that money is a form of memory.

4 There are two caveats: the total units of bitcoins available for transactions may diminish if private keys (see Section 3) are lost, or increase if a fractional reserve banking system develops (the latter is unlikely to accord with the intent of Bitcoin's creator(s)).

US$1.3 billion.[5] Each bitcoin is divisible to eight decimal points, which form the base unit of account (called a 'satoshi').[6]

New bitcoins are distributed to users as a reward for contributing computing power to confirm transactions within the system (bitcoin 'mining' – see Section 3.3). Since November 2012 the reward has been 25 bitcoins paid to one 'miner' every ten minutes; this reward is halved roughly every four years until around 2140, when it becomes zero.[7]

Graph 1
Projected Bitcoin Supply
Bitcoin units



Source: RBA

1.2 Demand

Demand for a currency comes from its use as a medium of exchange, as a store of value, and as a unit of account.[8] Bitcoin has some of these attributes.

Although there is no minimum demand for bitcoins as a medium of exchange since they are not legal tender in any jurisdiction, users may find bitcoins appealing when compared with more 'traditional' payment systems because (as further explained in Section 3):

- transaction fees are zero or minimal, (relative to traditional payment methods, this is a particular advantage for cross-border transfers where the user already holds bitcoins)
- transactions can be made anonymously
- value can be transferred relatively quickly, with transactions taking 10 minutes to one hour to be confirmed
- transactions are irreversible after confirmation.

Prospective and existing users may be discouraged from holding bitcoins as a store of value because of security concerns over storage (see Section 2.2), and the recent extreme volatility in its price in national currencies (Graph 2). Since 1 January 2013, bitcoin has traded between US$13 and US$266 at the Mt.Gox exchange (see Section 2.1), with an annualised volatility of over 150 per cent; the most recent closing price was US$118.21. Indeed, media reports and measures of idle bitcoins suggest that

5 Assuming that the volume of goods and services bought and sold with bitcoins continues to increase, the fixed supply clearly has deflationary implications on the Bitcoin system (even as the price of each bitcoin unit increase in national currency terms).

6 For a perspective on whether this is an economically meaningful base unit of account, the current 1.1×10^{15} satoshis in circulation compares with 2.7×10^{13} AUD cents in the M1 money supply and 3.0×10^{15} USD cents in the US monetary base.

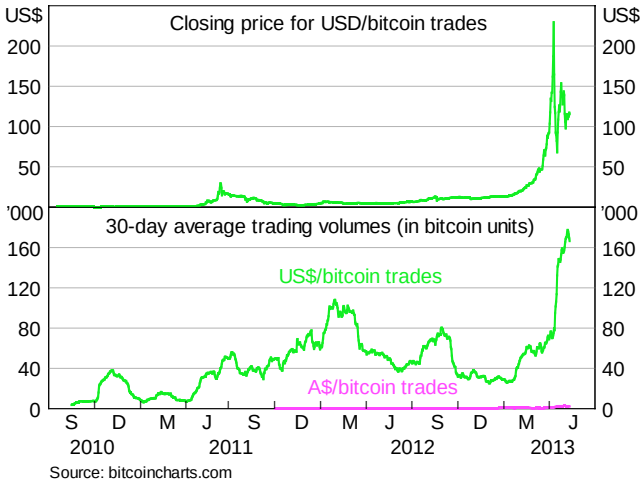
7 In the long-run new bitcoin units would be expected to be allocated proportionately to the computing power contributed by each user. From the year 2026, only one million new bitcoin units will be distributed (and only one unit in the final 35 years).

8 For example, the widespread use of a currency as a unit of account may lead to wider acceptance. Currently, few prices for legitimate goods and services are denominated solely in bitcoins. Instead, prices appear to be determined in a national currency and converted to the bitcoin equivalent, with bitcoin prices consequently moving in line with the price in national currencies.

the recent demand has been mainly for speculative purposes. Nonetheless, some commentators have suggested that bitcoins have, in some cases, been purchased as store of value in jurisdictions where users have lost confidence in the banking system.[9]

So far in 2013, around 300 000 bitcoin units are estimated to be transacted on average per day (adjusted for 'change' – see Section 3.2), including trades at Bitcoin exchanges.

Graph 2
Bitcoin Price and Volume
Trades at Mt.Gox exchange, daily



Source: bitcoincharts.com

2. Operation of the Bitcoin System

The operation of the Bitcoin system can be divided into a number of parts: entry and exit to the system; storage of bitcoins (via addresses and wallets); and the transfer of bitcoins between users (including transaction messages and the process of confirming transactions).

2.1 Entry and exit

Bitcoin 'exchanges' are the main entry and exit points to the Bitcoin system to and from the traditional payments system, with 'mining' and selling goods and services for bitcoins being less common ways for users to obtain bitcoins. Exchanges operate order books, matching buyers and sellers of bitcoins and the price (in national currencies) at which they are willing to trade. There is currently no exchange located in Australia.

Tokyo-based Mt.Gox is the largest Bitcoin exchange, accounting for over 80 per cent of all bitcoin/national currency trades.[10] It offers markets in 17 currencies, including the AUD.[11] In its USD market, 86 000 bitcoins (around US$6.6 million) are traded per day in 2013 on average, though trade has been elevated since around April; by contrast, the AUD turnover is 1 710 bitcoins (around A$0.1 million). Mt.Gox charges 25–65 basis points per transaction, with the exact fee based on the trader's transaction volume from the previous month.[12]

Users establish at least two accounts with Mt.Gox – one for bitcoins and one for each national currency they wish to trade in. Bitcoins are deposited and withdrawn from the exchange through the peer-to-peer Bitcoin network (as in any other Bitcoin transaction). The national currency account is typically funded via a transfer through the SWIFT interbank network, though domestic payment systems are also available for some currencies (sometimes for an additional fee paid to Mt.Gox or their service provider).

---

9 For example during the recent episode in Cyprus – see Bloomberg (March, 2013).

10 Mt.Gox stands for 'Magic: The Gathering Online Exchange', reflecting its origins as a marketplace for cards from the game 'Magic: The Gathering'.

11 The 17 currencies are AUD, CAD, CHF, CNY, DKK, EUR GBP, HKD, JPY, NZD, NOK, PLN, RUB, SEK, SGD, THB, USD.

12 The fee schedule for trades at Mt.Gox is available at https://mtgox.com/fee-schedule.

There are also other ways of exchanging bitcoins for national currency, including 'OTC' markets where users make bilateral trades (sometimes for physical cash), intermediaries to exchanges (where the intermediary enters into a contract to buy/sell bitcoins at a fixed price and then enters the exchange on behalf of the user), and physical machines that offer bitcoin trades ('Bitcoin ATMs').[13] These methods are typically used only when the users and the intermediary are in the same jurisdiction. In Australia, there are a number of firms operating as intermediaries, including Bit Innovate, SpendBitcoins and Omnicoins. These firms take cash payments, direct credits or BPAY transfers from a user and use those funds to enter into trades at a Bitcoin exchange.[14]

2.2 Storage – addresses and wallets

A user receiving bitcoins needs an **address**, akin to a bank account number, to which bitcoins can be assigned (and the transfer recorded in the public ledger). A Bitcoin address is a string of 27–34 alphanumeric characters to which bitcoins can be assigned. New Bitcoin addresses are easy to create and users are encouraged to create at least one new address for each transaction. Since a user's real-world identity is not linked to their addresses, this ensures that users are able to remain essentially anonymous in Bitcoin transactions.

A user's Bitcoin addresses are visible to the entire network in their capacity as the source or destination of bitcoins in a transaction. A 'private key' – another string of characters that should be known only to the owner of an address – is needed to 'sign' a Bitcoin transaction message to indicate that the true owner of the address was giving the instructions.[15] Securing the private key is therefore essential to maintaining ownership of addresses and the associated bitcoins.

Users with multiple addresses need a way to store and manage them, and to easily generate messages to transfer bitcoins from one address to another (akin to making a transfer using the user interface offered by banking websites). Both functions are performed by Bitcoin **wallets**. There are many suppliers of these wallets, and most are free to use. Some users also choose to store their private keys in a wallet.[16] It should be noted that wallets are provided by third parties and are not protected or based on the core Bitcoin code; the level of security offered and required is up to the wallet issuer and end-user.

2.3 Making transactions – Bitcoin messages

Transactions in Bitcoin are transmitted through transaction **messages**. Each message, which may contain multiple economic transactions, has two components:

---

13 For an example of such an ATM, see here.

14 Depending on the procedures to manage exposure to bitcoin price movements between entering into the contract with the user and entering into the corresponding trade at an exchange, these intermediaries may take on market risk.

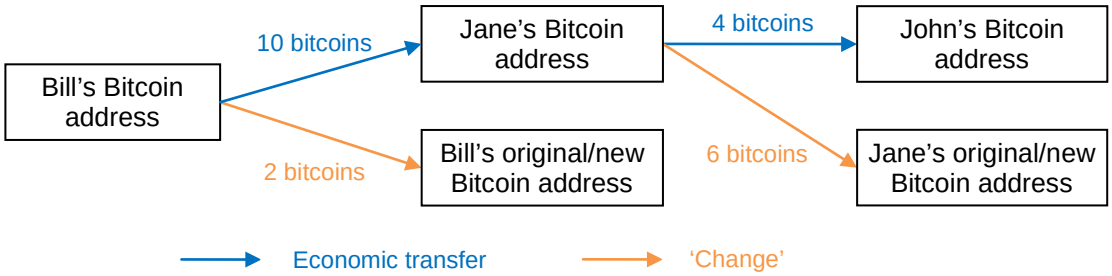
15 Each public address has only one possible private key; the mathematical link between the two is determined by public key cryptography.

16 Keeping private key within a Bitcoin wallet has proved risky due to hacking. Some users keep their private keys in data storage that is not connected to the internet, and some have recorded parts of their private keys in a physical form by minting Bitcoin 'coins'.

- *Inputs*: the source(s) of the bitcoins, which is one or more Bitcoin addresses[17]
- *Outputs*: the address(es) that the bitcoins are being sent to and the units to be sent to each addresses.

As an example, if Jane owns 10 bitcoins (received from Bill in a previous transaction) and wants to send four bitcoins to John, Jane must input 10 bitcoins into the message (Figure 1). The message will then have two outputs: four bitcoins to John's address and six bitcoins to herself (either the original or a new address created by Jane). The six bitcoins Jane sends to herself is known as 'change'. The ability to create new addresses at will makes it difficult, for anyone other than the sender, to know what is the economic value being transferred and what is 'change'.

Figure 1
Transactions in Bitcoin Messages



As noted above, the transaction message must also be signed with a private key to ensure that the sender owns the bitcoins being sent.[18] The signed message is then broadcast publicly for verification.

A transaction fee may be required by the network for complex transaction messages with many inputs and outputs (which therefore have a large data size); this fee would be paid to the miner that confirms the message (see next section). A fee may also be required for messages where each output is less than 0.01 bitcoin units – this is to prevent 'spam' attacks where the network could be destabilised by having to process a large number of transfers. In addition, a sender may choose to pay a transaction fee to prioritise the message's confirmation. These fees, whether required or voluntary, are included in the output of a transaction message.

2.4 Confirming transactions ('mining')

Confirmation is the final step in a bitcoin transaction, after which it is added to the public ledger of every bitcoin transaction (or the '**block chain**'). Confirmation, or '**mining**', seeks to ensure that the same bitcoin unit cannot be spent twice and that the ledger is not corrupted.[19] This step is necessary in a peer-to-peer network since end-

17 It should be noted that the source address is not an 'absolute' reference in the transaction message, but rather a reference to the destination address from the latest transaction that had transferred value to that address. In this way, each address acts as a link in the chain of transactions in the public ledger.

18 'Signing' adds a string of data, encrypted with Jane's private key, to the transaction message.

19 'Double-spending' has not proved to be a significant issue in traditional payment systems. Once you use a note or coin, for example, you no longer have possession of it and therefore cannot reuse it, and security features of a national currency make counterfeiting difficult. In traditional electronic payment systems, the problem is prevented by the rules and procedures of the operator/administrator of the payment system (e.g. MasterCard for MasterCard transactions, and APCA for ATM transactions).

users would typically not have complete information – namely a record of the latest transactions – to determine whether a new transaction is valid (e.g. a bitcoin has not been spent twice).

Confirmation is performed when a 'miner' (i.e. an individual user choosing to contribute computing power to confirm transactions for a possible reward) runs an algorithm that creates a new 'block' to update the ledger; on average, a new block is created every 10 minutes. A block comprises a subset of the latest transactions (i.e. those since the creation of the last block) known to the miner, as well as the previous block in 'hash' data form.[20] Miners run this algorithm many times (creating a new block each time), competing with other miners to be the first to reach a solution – namely, a block with the right (computationally correct) properties – and thus have their block accepted as the official addition to the ledger.[21] This process is computationally intensive, and miners with more computing power will tend to have more 'wins' on average.[22] Moreover, the Bitcoin system deliberately makes it increasingly difficult, and thus computationally intensive, to discover the correct block as the computing power of the network increases (as the number of miners increase).

The correct block is then broadcast to the network for verification that it is indeed a solution. As part of this process, the new block must be accepted by a majority (by computing power) of the network. Once verified, the block is added to the block chain, and miners begin searching for the next block.[23] The 'winning' miner is then rewarded with newly created bitcoins and receives any transaction fees associated with transactions that are being confirmed for the first time (each new block created re-confirms *all* bitcoin transactions included in the block chain).

Individual transactions are only confirmed when they are included in the block chain. A transaction is irreversible once confirmation is made. However, complications may arise when two 'correct' blocks are created and verified near-simultaneously, because the nature of the block chain requires that there be only block from which the next one could be generated.[24] The verified status of one of the parallel blocks would need to be

---

20 As each block contains the previous block, every block is a 'chain' stretching to the start of Bitcoin. A 'hash' is a fixed-length string of data which is mapped from an arbitrary amount of data (what we can think of as a 'long-form' ledger in the Bitcoin system) by a 'hash function'. There is only one possible hash solution for each iteration of the long-form data, and so rearranging the data within the ledger changes the equivalent hash; each hash has a number equivalent. A hash function is cryptographic when altering the hash or the long-form data without changing the other is computationally infeasible. Bitcoin uses the SHA-256 function as its cryptographic hash function. These concepts are explained in more detail at the blog self-evident.

21 The 'right' block is one whose hash, in its number-equivalent form, is lower than a number set by the network. The network changes this threshold number periodically in order to change the difficulty of finding the correct block; these adjustments, based on the amount of computing power being devoted to mining, are made to keep the frequency of a correct block being found consistent with the number of bitcoins that should be rewarded (based on the pre-determined supply path).

22 While each run of the algorithm is computationally trivial, finding the right answer can require trillions of runs. Estimates suggest miners in total consume around US$190 000 per day in electricity alone. While anyone can mine by downloading a program, mining is now considered not feasible on personal computers due to the computing power and specialised operations that other miners have dedicated to the process. Dedicated mining programs are estimated to have nearly a 30 per cent profit margin (this estimate depends heavily on the market price of bitcoins).

23 While the chain may appear to comprise a large amount of data, the size of the 235 385th block, which includes 1 170 new transactions, is only 474 kilobytes.

24 In such a case, the block that is broadcast most widely (based on computing power) would typically be the one to retain its verified status. This is because the two blocks are essentially in a race to be included in the

reversed, which would also reverse the confirmed status of transactions within this block which were not already confirmed in the other block. These transactions must then be confirmed in a subsequent block. Due to the possibility of this complication, parties to larger-value transactions sometimes wait for multiple confirmations (typically up to six, which implies a waiting time of one hour) before treating a transaction as irreversible.

It is worth noting that the cryptography behind Bitcoin has been designed to make it more profitable to confirm transactions for the network – thereby protecting the integrity of the ledger – than to attack the system.[25]

3. Policy Considerations

A number of policy areas may be affected by the operations of Bitcoin. These include the payments system, seigniorage, monetary policy, financial stability, consumer protection, taxation, anti-money laundering and counter-terrorist financing (AML/CTF) and the financing of illegal activities more generally.[26]

The discussion in this section focuses on issues relevant to a central bank, particularly payments policy issues. Due to the limited usage of Bitcoin in Australia to date (given the absence of Australia-based exchanges and that very few Australian merchants accept bitcoins or any other virtual currency), risks to the payments system appear to be limited.

3.1 Payments system issues

The process of confirming transactions appears to be an inefficient use of resources compared with other payment systems. By tying the process to the competition for new bitcoins, the unit-cost (in terms of computing power) of processing a Bitcoin transaction is likely to be higher than necessary, with many miners simultaneously confirming the same transaction.[27] By contrast, economies of scale in more traditional centralised payment systems would typically lead to lower unit-costs as the network

---

next block, which is a process determined by computing power. However, a prolonged '[fork]' occurred on 11 March 2013, when a software update meant that those running the older version were not accepting a block created on the updated software; as a result, the fork persisted for a period. This was resolved through collective action coordinated by the Bitcoin Foundation.

25 Examples of attacks include altering the block chain and duplicating address–private key pairs. In both cases, the computing power and time needed for an attack, as well as the likely collapse in the price of Bitcoins in its aftermath, makes attacks less worthwhile than to use the same computing power to run the algorithm to create a new block and be rewarded with new bitcoins. As an aside, to fraudulently alter the block chain an attacker needs to control over 50 per cent of the network's computing power. It is unclear at this stage if the incentives will remain the same when the new coin reward approaches zero.

26 To date, the most comprehensive report on virtual currencies by a policy maker is the [Virtual Currency Schemes] report, published by the European Central Bank (ECB) in October 2012. The ECB found that virtual currencies: currently pose limited risk to monetary policy or financial stability due to their low levels of use; expose users to credit, liquidity, operational and legal risks; pose a challenge to public authorities due to their use in illegal activities; may fall under central banks' responsibility for the payments system, depending on their legal mandate; and could negatively impact central bank's reputation (if an incident occurs after a system has grown substantially without central bank oversight).

27 It should be noted that the Bitcoin community has argued that the computing power used by miners is necessary to protect the system against attacks. It is, however, hypothetically feasible to have a peer-to-peer payment system that verify transactions and maintain the ledger's integrity through a set of rules and a less onerous verification process (such as in PPCoin and LiteCoin, see Appendix B).

grows since transactions are verified through a single system or set of rules and procedures. In Bitcoin, only a part of these costs are passed on to end-users (in the form of required/voluntary transaction fees to the miner who 'wins' – see Section 2.3), with no compensation paid to the 'losing' miners for their processing. This characteristic contributes to Bitcoin's appeal for end-users, who benefit from its relatively low transaction fees and fast transaction times (especially for international transfers).

Of course, the appeal of low fees and fast transaction times are not themselves sufficient for the wide adoption of Bitcoin as a payment system. From a competition perspective, network externalities mean that users are likely to continue using the more established payment systems (and indeed, national currencies).[28] These externalities make it difficult for Bitcoin to gain wide adoption. However, network externalities may also work in favour of Bitcoin in terms of competition with other prospective virtual currencies (see Appendix B): while barriers to creating a decentralised virtual currency appear to be low, new entrants may find it hard to compete against an incumbent Bitcoin.[29] This effect would only increase as the Bitcoin network grows.

This inertia to adopt a new system is likely to be compounded for payment systems that transact solely in virtual currencies, given the role that confidence plays in nascent technology. The safety of Bitcoin as a payment system is reliant on cryptography and the transaction confirmation process. Just like operational procedures and risk-related rules within traditional payment systems, deficiencies in the code containing the system's cryptography and mining process could pose some risks to the integrity of the system. This is exacerbated by the status of virtual currencies as a relatively untested means of payment. For example, if the integrity of transaction messages or the ledger is called into question (e.g. from a hack of the process of 'signing' transactions or mining, or from a significant decrease in computing power dedicated to maintaining the system's integrity), users will likely lose confidence and cease to use Bitcoin. such an outcome is likely to have a limited impact on the Australian payments system or economy given current activity levels.

The stability of Bitcoin as a payment system may also be undermined by its fixed supply. To the extent that a fixed supply encourages hoarding for speculative purposes, a bubble may develop (as may be occurring given the rapid rise in the price of bitcoins in recent months). Wide fluctuations in prices and the possibility of a 'firesale' of bitcoins are likely to reduce users' desire to hold bitcoins as a medium of exchange, and undermine their usefulness as a store of value.

As noted above, cryptographers appear to regard the possibility of the core Bitcoin code being hacked as remote. In addition, some users have also argued that the diffuse, peer-to-peer nature of Bitcoin actually makes it more operationally stable relative to systems that are reliant on a single point of control (as in traditional centralised payment systems). However, there is some agreement that third-party service providers are the weakest link in the system. When these providers' operations are compromised, the safety of the system is affected both directly, through the loss of

28 That is, Bitcoin is competing against currency networks and payment system networks simultaneously.

29 The costs of entry are mostly those relating to the development of the base code; these costs have likely declined since the advent of Bitcoin given that its code is open-source.

users' stored bitcoins (for instance), and indirectly, through a loss of confidence in the system.

There is currently limited information on how exchanges operate, and they do not appear to have any public documents on settlement risk mitigation measures. For example, while Mt.Gox requires national currency and bitcoin deposits, it is unclear what procedures (if any) are used to protect settlement. Users are also directly exposed to exchanges through the latter's holding of users' deposits, whether in bitcoin or national currency. There have been a number of examples where users have had difficulty in recovering their deposits from failed exchanges.[30]

The safety of and confidence in the system are also affected by fraud.

For instance, there have been numerous reported incidents of wallets being hacked (both of the service provider or individual users). Exchanges may also be destabilised by attacks, which may affect the market price of bitcoins and facilitate the theft of bitcoins held in exchange accounts.[31] Such incidents can clearly affect confidence in a relatively new payment system, and can ultimately lead to a decline in its use.

3.2 Other central bank issues

As discussed above, Bitcoin currently poses limited risks to the payments system, the financial system and the economy more generally. If Bitcoin (or any other virtual currency-based system) were to become widely adopted, however, central banks may face a number of issues:

- A reduced ability to implement monetary policy because of loss of control over the money and credit creation process.

- A fall in seigniorage revenue if virtual currencies begin to replace physical cash at the point of sale. However, Bitcoin and other virtual currencies appear to be used currently as substitutes for other online payment methods (PayPal, credit and debit cards), which does not directly affect seigniorage as narrowly defined.

- As with any other asset class, a rush to liquidate holdings of bitcoins or bitcoin-denominated assets may have implications for the stability of the financial system.[32] This rush to liquidate could occur for reasons affecting the financial market generally (e.g. a period of deleveraging, if investors have borrowed to buy bitcoins), or because of a loss of confidence in the core Bitcoin system or large third-party service providers.[33]

---

30 For a discussion on the 'track record' of a number of exchanges, see Moore and Cristin, 'Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk'.

31 Mt.Gox was hacked in 2011, and was the subject to a distributed denial of service (DDoS) attack in April 2013. Another example is the wallet provider Instawallet which was hacked in April 2013.

32 As an aside, there are options contracts for delivery of bitcoins and bitcoin-denominated commodity futures being sold at the MPEx Exchange. Recent news reports suggest that the Commodity and Futures Trading Commission in the US is evaluating its role in derivatives contracts that are denominated in bitcoins.

33 For example, the hacking incident at the Mt.Gox exchange in 2011 compromised the details of over 60 000 members – the price of bitcoins fell from US$17.50 to a few cents within a few hours (see here).

3.3 Other policy concerns

Internationally, Bitcoin has come under most regulatory scrutiny with regards to AML/CTF, taxation and general law enforcement issues due to its ability to facilitate illegal transactions through anonymity. For example, the US Financial Crimes Enforcement Network recently released a guidance note to the effect that money transmitter regulations – which have an anti-money laundering focus – apply to the exchange of any newly created virtual currencies for a national currency, and to intermediaries that accept such virtual currencies in order to transfer them to another person.[34] On 15 May, the US Department of Homeland Security obtained a court order seizing the deposits of Mt.Gox's US subsidiary, Mutum Sigillum LLC, that are held by Dwolla (an online payments provider with a similar model to PayPal) and Wells Fargo. The Department alleged that when applying for the Wells Fargo bank account in May 2011, Mutum Sigillum claimed that it does not deal in or exchange money for its customers, despite Mt.Gox allowing US dollars to be transferred between account holders (which the Department argues is money transmitting business).

In the UK, a one-day conference was recently held by tax and law enforcement officials; one point of discussion was reportedly establishing a regulated exchange, which would enable the authorities to monitor entry and exit from the Bitcoin system.

In Australia, AUSTRAC stated in a recent report that 'digital currencies that are not backed, either directly or indirectly, by precious metal or bullion are not regulated by the AML/CTF Act'.

Consumer protection is also an issue with Bitcoin. The potential anonymity of Bitcoin users and the irrevocability of transactions after confirmation limit consumers' (or investors') avenues for recourse against fraudulent merchants or other end-users. The conduct of intermediaries between users and exchanges may also give rise to consumer protection issues.

4. Conclusion

Bitcoin can be characterised as both an alternative to national currencies and as a payment system.[35] As a payment system, Bitcoin appears to involve an inefficient use of resources, but has some benefits for end-users that encourage its use over more established payment systems (low fees, anonymity, speed, irrevocability). The system also has the potential to pose a number of risks and concerns for policymakers. Although the international community has recently given some consideration to Bitcoin's regulatory status, the focus has been on AML/CFT and consumer protection aspects instead of issues more typically associated with central banks. Given that it has not been widely traded or adopted, risks and policy concerns are currently limited in the Australian context.

David Halperin / Payments System Efficiency / Payments Policy Department
17 May 2013

---

34 Reports suggest that some US exchanges have been refused bank accounts following the guidance note.

35 Developments since Bitcoin's establishment – in particular Ripple (see Appendix B) – show that its payment system characteristics are distinct from its role as an alternative currency or asset class.

APPENDIX A – VIRTUAL CURRENCY TYPES

Virtual currencies are essentially transaction 'ledgers' recording who has a claim to units of the currency and changes to the ownership of each currency unit. Currently, all issuers of virtual currencies are non-government entities and virtual currencies are not considered legal tender in any jurisdiction. Virtual currencies can be classified based on two aspects:

1. their interaction with 'real' national currencies and the real economy (i.e. how you obtain the currency and what you purchase with it)
2. how transactions within the virtual currency system are processed (i.e. updating and maintaining the ledger).

Interaction with national currencies and the real economy can be classified as:

a. *Closed* – where, after paying a subscription or entry fee for the primary service of the virtual currency issuer (usually a game), the user obtains and spends the virtual currency solely within the confines of the virtual ecosystem.

b. *Uni-directional* – where the virtual currency is able to be purchased with national currency, either from the virtual currency issuer or a third party. Many, but not all, of this type of currency can be used to purchase real goods and services (including digital media such as movies and music).

c. *Bi-directional* – where users can both buy and sell the virtual currency for a national currency either from the currency issuer or a third party.[36]

Transactions are processed via:

a. a central party (typically the issuer of the virtual currency), or

b. a peer-to-peer, decentralised network. This is a relatively new model.

Table A1
Examples of virtual currencies

Network	Closed	Uni-directional	Bi-directional
Centralised	World of Warcraft Gold[(a)]	Amazon Coins PlayStation Credits Ven Floorz[(b)] Beenz[(b)] Facebook Credits[(b)]	Linden Dollars
Peer-to-peer			Bitcoin Ripple PPCoin LiteCoin

(a) There is an unsanctioned market for buying and selling Gold. However, Blizzard Entertainment (the issuer) can disable accounts if they think it has been used in a transaction for national currency.
(b) The virtual currency is no longer in use.

36 Based on the classifications described in ECB (2012), Virtual Currency Schemes.

APPENDIX B: BITCOIN ALTERNATIVES

Since its establishment, a number of new virtual currencies have been developed based on the operations of Bitcoin. Three such currencies are LiteCoin and PPCoin (both essentially copies of Bitcoin with slight tweaks), and Ripple.

In LiteCoin, blocks are created every 2½ minutes to speed up confirmations. Its mining process is modified to reduce the resource burden. Eighty-four million LiteCoin units will be created to supposedly limit the effect of a limited supply (though supply is still capped, implying that deflationary implications will still exist within the system). By contrast, PPCoin has a flexible money supply and uses a simpler mining process; rewards for mining vary for each block. The developers of LiteCoin and PPCoin are not-for-profit individuals, but those contributing to mining can earn transaction fees, as in Bitcoin.

Ripple, developed by OpenCoin Inc (a for-profit entity), appears to be the Bitcoin alternative getting the most publicity although it is not yet in operation. The supply of ripple units is fixed at 100 billion – 50 billion will be given to users for no charge and the rest kept by OpenCoin Inc (to profit off an expected appreciation in ripple). While Ripple has its own virtual currency, *any* currency (and 'money' created by coordinating the chain of how much users are willing to lend to specific users) can be exchanged through the Ripple system.[37] However, users are required to own a small amount of ripples in order to pay a small fee for each transaction to protect the system from spam attacks; these ripples are then extinguished from the system. Access to Ripple will be through gateways; any entity can be a gateway, and OpenCoin appears to hope that traditional banks will be interested in becoming gateways. Ripple transactions will, on average, take 5–10 seconds to be confirmed; servers charge fees for their confirmation service.

37 For more on Ripples 'IOUs' see https://ripple.com/how-ripple-works/ or https://ripple.com/wiki/Main_Page.