



# Reserve Bank of New Zealand Analytical Notes

## Crypto-currencies – An introduction to not-so-funny moneys

AN2017/07

*Aaron Kumar and Christie Smith*

November 2017

Reserve Bank of New Zealand Analytical Note Series  
ISSN 2230-5505

Reserve Bank of New Zealand  
PO Box 2498  
Wellington  
NEW ZEALAND

[www.rbnz.govt.nz](http://www.rbnz.govt.nz)

The Analytical Note series encompasses a range of types of background papers prepared by Reserve Bank staff. Unless otherwise stated, views expressed are those of the authors, and do not necessarily represent the views of the Reserve Bank.

---

## NON-TECHNICAL SUMMARY

This paper introduces the distributed ledger technology of crypto-currencies. We aim to increase public understanding of these technologies, highlight some of the risks involved in using crypto-currencies, and discuss some of the potential implications of these technologies for consumers, financial systems, monetary policy and financial regulation.

Crypto-currencies have no physical existence, but are best thought of as electronic accounting systems that keep track of people's transactions and hence remaining purchasing power. Crypto-currencies are typically decentralised, with no central authority responsible for maintaining the ledger and no central authority responsible for maintaining the code used to implement the ledger system, unlike the ledgers maintained by commercial banks for example. As crypto-currencies are denominated in their own unit of account, they are like foreign currencies relative to traditional fiat currencies, such as dollars and pounds.

We examine the 'monetary' attributes of crypto-currencies, and describe some of the reasons they have been adopted. While crypto-currencies are clearly used for exchange, we argue that they are not yet generally accepted, and for the most part they are not used as a unit of account. Bitcoin, the most-traded crypto-currency, has been a volatile and hence imperfect store of value. In the particular case of Bitcoin, the ultimate supply of bitcoins approaches a fixed limit, which means that any fluctuation in the demand for bitcoins is reflected in substantial movements in its price. Like fiat currencies, crypto-currencies have no secondary use. Their utility as a payment mechanism stems from a *belief* that others will continue to use the corresponding ledger systems to exchange goods and services in future.

The paper discusses the mechanics of Bitcoin – the original crypto-currency – to illustrate the fundamental elements of decentralized crypto-currencies. In short, transactions are implemented as messages that debit or credit account balances in duplicate ledgers. Programming protocols ensure that ledgers are synchronized, and agents are rewarded for updating and quality-assuring the ledgers with transaction data, which accumulate in 'blocks'. Cryptography is used to secure the transaction messages and the integrity of the ledgers containing account balances.

The latter part of the article provides a high-level summary of the implications of crypto-currencies for consumers, financial systems, monetary policy, and regulatory policy. Crypto-currencies ex-

---

pand the mechanisms by which people can transact with each other, strengthening competitive pressures on payment systems providers. But, as noted by many international institutions and central banks, crypto-currencies facilitate a relatively small volume of transactions. These new payments mechanisms are unlikely to completely supplant traditional payments systems. People in different countries typically transact in their own local currency. Since most jurisdictions require tax obligations to be paid in domestic fiat currency, national currencies are likely to remain an important payment mechanism. Crypto-currencies are also unlikely to supplant financial institutions' role in providing credit. Banks and other financial institutions transform assets, manage risk, assess prospective creditors and monitor creditors' progress in meeting their obligations. Credit is largely incompatible with the (pseudo) anonymity that is a common element of crypto-currency design.

Ensuring price stability is likely to remain the pre-eminent monetary policy objective for central banks, an objective unchanged by the growth of crypto-currencies. As the 'licensed distributors' of fiat currency, central banks should remain able to set interest rates in their domestic fiat currency units. The introduction of crypto-currencies should not fundamentally disrupt central banks' use of interest rates to stabilise the inflation rates of their own fiat currencies.

Crypto-currencies also raise consumer protection, anti-money laundering, and counter-terrorism financing concerns. As niche payment systems, crypto-currencies do not currently pose material financial stability concerns, but risks could increase in materiality if crypto-currencies become more popular and/or more integrated with the activities of traditional financial institutions. Exactly how crypto-currencies should be regulated to address these various concerns remains a work in progress, given the decentralised nature of most crypto-currency systems.

Lastly, it is important for consumers to understand that crypto-currencies are extremely volatile, and there are significant risks associated with holding such assets. There is no certainty that specific crypto-currencies, such as Bitcoin, will continue to function and be valued by transactors, and there are non-trivial risks of loss and theft. Consequently, transactors should consider *carefully* what proportion of assets – if any – to hold in crypto-currencies.

## 1. Introduction

This paper provides an introduction to the distributed ledger technology of crypto-currencies.<sup>1</sup> We aim to develop greater public understanding of these technologies, highlight some of the risks involved in using crypto-currencies, and discuss some of the potential implications of these technologies for payments systems, financial institutions, markets, and regulators.

In section 2 we begin by providing a brief background discussion of payment mechanisms and describe crypto-currencies in general. We describe the growth of crypto-currencies and the proliferation of new variants. To facilitate understanding of the mechanics of crypto-currencies, we conclude the section by discussing how transactions proceed in Bitcoin, the original and most-widely transacted crypto-currency. In section 3 we examine the ‘monetary’ properties of crypto-currencies and consider some common uses (transactions). We also illustrate some scalability problems that crypto-currencies face by comparing them to the electronic transactions facilitated by traditional financial institutions. In section 4 we touch on the implications that crypto-currencies have for traditional financial systems, monetary policy, and financial regulation. In relation to these issues we draw on work by other central banks and international institutions regarding these comparatively new financial instruments. We then conclude in section 5.

## 2. Payment/exchange mechanisms

### 2.1 Background context

The central role of the financial system is to facilitate the exchange of goods and services, possibly through time. The financial system contains a diverse range of institutions and mechanisms for enabling such transactions. To provide context for our discussion of crypto-currencies, we briefly discuss three payment mechanisms: i) legal tender, ii) e-payments, and iii) e-money.<sup>2</sup>

<sup>1</sup>We would like to thank Jonathan Chiu and Thorsten Koepl for providing access to their own research on blockchain technology, which helped to improve our understanding of its implementation and the issues that arise. Helpful comments were also received from Yuong Ha, Chris Kim, Leo Krippner, Anella Munro, Cavan O’Connor-Close, Roger Perry, Jeremy Richardson, Karam Shaar, and Amber Wadsworth.

<sup>2</sup>We distinguish e-payments and e-money as per [Fung et al. \(2014\)](#). ‘Credit’, as opposed to various forms of money, will be discussed later.

---

Legal tender is a payment mechanism recognized by the legal system that can be used to extinguish debts in the same units.<sup>3</sup> Typically, the notes and coins issued by a central bank serve as legal tender, which creditors must accept in payment for an outstanding obligation denominated in the same currency. For example, a ten dollar note issued by the Reserve Bank of New Zealand represents ten New Zealand dollars and can be offered to settle a debt of the same value. Currencies established by government fiat are enduringly useful because they can be used to settle tax obligations – debts to the government.

It should be noted that legal tender does not necessarily need to be used to settle a contract: two parties may stipulate how payment is to be made as part of a contractual agreement. For example, it may be agreed that a good or service will be exchanged for some other good in a barter-type arrangement. Conversely, some firms exclude certain payment mechanisms. New Zealand dairies (corner stores), for example, routinely prohibit the use of credit cards, while nevertheless accepting debit cards.

In modern economies, most transactions are conducted via e-payments rather than physical currency. Most of these e-payments are electronic transfers from deposit and credit accounts facilitated by financial institutions such as commercial banks and credit card companies. These financial institutions use private electronic networks and private account ledgers that only they can access and amend.

E-money, the third transaction medium mentioned above, is a medium of exchange in which monetary value is stored on hardware or software, enabling people to pay for goods and services bought from third-party merchants ([Bank of Canada, 2014b](#)).<sup>4</sup> Contact-less smart cards, such as ‘Snapper’ cards in Wellington New Zealand, and ‘Octopus’ cards in Hong Kong, are examples of e-money. These cards can be variously used to pay for public transportation, taxis, tolls, and in some cases retail transactions such as fast-food, supermarket and vending machine purchases.<sup>5</sup> E-money does not usually entail a physical exchange of goods. Instead, the e-money device keeps track of a balance of funds that can be used to purchase goods and services.

---

<sup>3</sup>See [McBride \(2015\)](#) for the distinction between ‘tender’ and ‘payment’. To ‘tender’ is to make a unilateral offer to complete a payment, eg by a consumer, while ‘payment’ is a bilateral act requiring the consent of both consumer and seller.

<sup>4</sup>See also <https://www.ecb.europa.eu/stats/money/aggregates/emon/html/index.en.html>, downloaded 5 May 2017.

<sup>5</sup>See [www.snapper.co.nz](http://www.snapper.co.nz) and [octopus.com.hk](http://octopus.com.hk), downloaded 5 May 2017.

E-money can be partitioned into two distinct categories: centralised and decentralised. Centralised e-money relies on a central institution – such as Snapper or Octopus – to administer the issuance of the e-money and the facilitation of transactions. Decentralised e-money brings us to the realm of crypto-currencies. See Box 1 for a brief summary of terminology.

### Box 1 Terminology

- **Digital currencies** represent value electronically. They may or may not be denominated in legal tender.
- **Virtual currencies** are digital money but are not denominated in units of legal tender.
- **Convertible currencies** can be converted or exchanged for other currencies if a counter-party can be found.
- **Decentralised currencies** do not have a central counter-party responsible for the provision of the currency.
- **Decentralised ledger technology** refers to ledgers that are stored across multiple computers, where such computers may be controlled by different people or firms.
- **Crypto-currencies** are decentralised currencies that use cryptography to secure transactions and validate balances.
- **Permissioned ledgers** restrict the agents able to amend (and possibly view) the ledger of transactions.
- **Permissionless ledgers** are open-access; all agents can read and, under certain conditions, update such ledgers.

## 2.2 What are crypto-currencies? How do they work?

Crypto-currencies rely on cryptography to facilitate and record transactions on a set of electronic ledgers – databases of financial accounts. Crypto-currencies have no tangible existence, rather they are electronic signals and records that keep track of transactions mediated with the currency. Given their electronic representation, crypto-currencies are also referred to as ‘digital’ or ‘virtual’ currencies, though distinctions can be made between all three.<sup>6</sup> The prefix crypto, meaning ‘concealed’ or ‘secret’, is derived from the Greek word *κρυπτός* meaning hidden. While cryptography

<sup>6</sup>See [ECB \(2012\)](#) and [He et al. \(2016\)](#), and Box 1.

is used to secure both individual transactions and the ledger of individual accounts, more properly 'addresses', the ledgers that record all transactions are usually in plain view to everyone who is interested in them. Nevertheless, address owners achieve a degree of anonymity as there is no central authority, such as a bank, tying a particular address to a particular individual.

Like traditional currencies, such as dollar notes or gold coins, crypto-currencies can be used to facilitate 'peer-to-peer' transactions between individuals without the services of a specific financial intermediary. While commodity currencies such as gold have tangible alternative uses, fiat currencies, bank deposits, and crypto-currencies have no secondary, non-monetary purpose. People transacting using these modern currencies believe that other people will accept them for future transactions and that such currencies will therefore be useful as a temporary store of value. Although crypto-currencies often have no centralised issuer, they are predominantly fiduciary in the sense that they are not backed by precious metal and require *trust*.<sup>7</sup>

White (2015) refers to crypto-currencies as *competing private irredeemable monies*. Irredeemable crypto-currencies stand in contrast to redeemable private monies, such as bank deposits. With the latter, an issuing bank denominates deposits in fiat currency units and promises to convert or redeem them one-for-one for fiat currency, either on demand or at maturity. Crypto-currencies are not backed by the promises of a similar institution and they are usually denominated in their own units. Bank deposits are liabilities for commercial banks and as such have a well-established place in the accounting and auditing frameworks that banks must legally satisfy as incorporated entities.<sup>8</sup> In contrast, crypto-currencies are not a liability of any given institution, and are not subject to the same accounting scrutiny and assurance.

Crypto-currencies are a decentralised technology designed to facilitate transactions without recourse to a central institution. This decentralization is achieved through the invention of the 'blockchain' – a universal distributed ledger that enables the confirmation of transactions and makes it possible to keep track of individual crypto-currency balances. A distributed ledger is a database of financial records 'distributed' across multiple nodes of a computer network.<sup>9</sup> No

<sup>7</sup>The digital currency 'E-gold' was an exception to this generalisation: E-gold was denominated in physical quantities of gold, and was backed by a corresponding cache of gold bullion. In 2007 e-gold ran afoul of the USA Patriot Act, due to money-laundering concerns, and was eventually closed down.

<sup>8</sup>Bank notes in circulation are interpreted as central bank liabilities and are also captured in central bank financial accounts. See for example the Annual Report of the Reserve Bank of New Zealand, <https://www.rbnz.govt.nz/about-us/annual-reports>.

<sup>9</sup>In the current context a node is a computer attached to the Internet.

single entity, such as a bank, is solely responsible for maintaining the nodes and ledgers.<sup>10</sup>

The ledgers contain a list of *all* transactions previously enabled via the digital currency in the order in which they were undertaken. The ledgers implicitly record the balances of all people using the crypto-currency, ensuring that people cannot spend currency they have not previously earned or obtained. The ledgers accumulate additional 'blocks' of transaction data, which are chained together, hence the name blockchain. Mechanisms are instituted to ensure that the ledgers across different nodes are synchronized, and market participants are incentivised to ensure that the ledgers correctly record transactions.

Cryptographic techniques are used to secure two related elements. First, they are used to secure transactions, to ensure that only an appropriate authority (the 'address holder') can 'spend' the funds attributed to a particular address. Second, cryptography is used to secure the transaction ledgers of the system, ensuring that people cannot fraudulently tamper with their crypto-currency balances.

The public key cryptography commonly used in crypto-currencies can be used in two different ways: i) to encode a message and then make it possible for only an intended recipient to decode the message; and ii) to secure a message yet make it possible for everyone to verify the contents of the message. We will see below that secure messaging of the latter type is an important characteristic of crypto-currency transacting.<sup>11</sup>

## 2.3 Growth in the supply of crypto-currencies

The idea of transactions by 'blockchain' was first suggested by Satoshi Nakamoto in 2008 on a cryptography mailing list.<sup>12,13</sup> This suggestion led to the development of Bitcoin in 2009 ([Bank of Canada, 2014a](#)). The number of crypto-currencies is increasing rapidly, in part because the

<sup>10</sup>The idea of a ledger as a substitute for money is a very old one. [Lipsey \(1963, p. 404\)](#) discusses a hypothetical ledger in a government-run store in a communist society.






<sup>11</sup>These cryptographic techniques have military applications and were classified by the British government when they were first discovered. Cryptography can also be applied to secure email messages, and also underpins the 'secure socket layer' that is used to secure credit card transactions over the Internet.

<sup>12</sup>See [Nakamoto \(2008\)](#).

<sup>13</sup>Satoshi Nakamoto is a pseudonym for person or people unknown. In May 2016 an Australian called Craig Steven Wright claimed to be Nakamoto, but there is public doubt about the truth of this claim. <https://www.wired.com/2016/05/craig-wright-privately-proved-hes-bitcoins-creator/>, downloaded 21 June 2017.



Table 1: Crypto-currency capitalisations – top ten

Symbol	Cryptocurrency	Mkt cap. (m)	USD price	Supply (m)	Vol. (24h) (m)
	Bitcoin	\$40,188	\$2451.52	16.4	\$1,983.8
	Ethereum	\$32,883	\$355.43	93.5	\$2,411.2
	Ripple	\$9,905	\$0.258704	38,290	\$188.8
	NEM	\$1,737	\$0.193029	9,000	\$11.8
	Ethereum Classic	\$1,695	\$18.30	92.6	\$177.0
	Litecoin	\$1,560	\$30.27	51.6	\$310.6
	Dash	\$1,197	\$162.64	7.4	\$47.6
	IOTA	\$987	\$0.355272	2,779.5	\$10.1
	BitShares	\$870	\$0.335395	2,596.1	\$197.5
	Stratis	\$775	\$7.88	98.4	\$11.1

Mkt cap. = market capitalisation = US dollar (USD) price × supply (millions). Supply is in units of each crypto-currency. Vol. = value of transactions in 24 hours, in millions of USD.

Source: [coinmarketcap.com](http://coinmarketcap.com). Downloaded 16 June 2017.

code for Bitcoin is open source. This means that the program code can be copied and altered to create new crypto-currencies relatively easily. In 2014, there were estimated to be 500 crypto-currencies in existence (White, 2015). By 8 November 2016 [coinmarketcap.com](http://coinmarketcap.com) identified 705 crypto-currencies, which had increased further to 876 currencies as at 16 July 2017. 'Market capitalisations' in July 2017 ranged from USD40 billion, for Bitcoin, to essentially nothing. As a point of comparison, the stock of M1 in the United States in July 2017 was USD3.49 trillion, roughly 87 times larger than the USD value of Bitcoin balances. Table 1 reports the top ten currencies by market valuation as at 16 June 2017. These new crypto-currency variants are often substitutes for pre-existing crypto-currencies, nibbling away at the demand for and liquidity of the pre-existing variants.

A major challenge for currency producers is to ensure that the value of their currencies is not debased by an excessive supply. Limits in the supply of precious metals constrained the supply of currency when coins were made from gold and silver. When metallic coins were used as currency, debasement typically occurred through reductions in the quantity of gold or silver contained in coins. Because fiat money is printed on low-value pieces of paper, it is straightforward to issue more currency, providing central banks or governments with an opportunity to gain control over physical

---

goods and services. When conducted on a large scale, the excessive production of currency can lead to periods of hyper-inflation, in which the value of currency in terms of goods declines rapidly (the price level rises). Inflation targeting frameworks can be thought of as a legislative mechanism to offset this tendency. An independent agent, the central bank, is tasked with ensuring that fiat currency retains a broadly stable value in terms of goods and services, i.e. inflation is maintained at low levels.

Unlike the fiat monies produced or distributed by central banks, crypto-currencies typically have explicit programmatic rules that prevent an explosion in supply. In the crypto-currency framework exemplified by Bitcoin, 'miners' are rewarded with bitcoins for validating transactions ([Peters et al., 2015](#)). With Bitcoin, the validation of transactions is central to growth in the supply of bitcoins. But Bitcoin has a *declining* growth rate in supply – the reward for adding a new block to the blockchain halves with every additional 210,000 blocks (roughly every four years, [Velde 2013](#)). Given the programming rules that govern the ledgers, the sum of all bitcoin balances is approaching 21 million bitcoins ([Velde, 2013](#)).<sup>14</sup> Litecoin, another crypto-currency variant, has the same declining reward structure for mining blocks; the supply of Litecoins is approaching 84 million units.

These asymptotic limits ensure that these crypto-currencies will be limited in supply, preventing the infinite debasement of these currencies. In decentralised systems, such as the crypto-currency schemes described here, there is no central authority that could unilaterally alter the protocols that govern crypto-currency supply. Not all crypto-currencies have a fixed level of supply. Crypto-currencies such as Peercoin and Blackcoin have modestly positive growth rates in the supply of 'coins' ([Johnson and Pomorski, 2014](#)). Positive growth rates are achieved in the Peercoin and Blackcoin frameworks by minting more coins proportional to all the account balances.

The quantity theory of money suggests that the stock of money ( $M$ ) multiplied by its 'velocity' ( $V$ ) equals transactions ( $T$ ) multiplied by the price level ( $P$ ):  $MV = PT$ . As with many other crypto-currencies, Bitcoin and Litecoin have operational constraints that limit the number of transactions that can be processed in a given period of time. The block size for Bitcoin is constrained to be a maximum of 1 million bytes, and blocks usually contain somewhere between

---

<sup>14</sup>Each bitcoin is divisible into small units called satoshis: one hundred million satoshis equals one bitcoin, just as one hundred cents equals one dollar. Alternatively, a bitcoin is sometimes divided into one million bits.

a couple of hundred and a couple of thousand transactions.<sup>15</sup> The programming protocols also limit how fast a block can be processed. Bitcoin and Litecoin thus constrain both money supply and velocity.

Superficially, it would seem that crypto-currencies with a fixed  $M$  and fixed  $V$  should be deflationary, so that changes in price level offset changes in the volume of transactions  $T$ ; the latter is expected to grow through time in tandem with the economy. In the quantity theory of money the price level adjusts to equilibrate the supply of money with the demand for money for transactions purposes. This equilibration process presumes that each sub-unit of currency – cents when thinking about dollars – has the same velocity as the major units. One cent in a dollar, say, has the same velocity as the dollar itself. If velocity is one transaction per second, then the quantity theory for physical money assumes that 100 cents could be used to implement 100 1-cent transactions per second. However, the transaction velocity constraints for Bitcoin imply that (approximately) 2000 bitcoin transactions could be validated per ten minute period or 2000 satoshi transactions. Dividing up an electronic currency unit into sub-units does not increase the number of achievable transactions. Consequently, it does not seem that changes in the price level can equilibrate a demand for real transactions with the supply of a given crypto-currency. It seems more likely that equilibration between the demand and supply of electronic transaction media will be achieved by producing additional crypto-currency variants.

## 2.4 The mechanics of Bitcoin and the blockchain

In the rest of this sub-section we describe the validation process of Bitcoin, the original crypto-currency. While the details for other crypto-currencies may differ, many of the key elements are similar. For a more in-depth treatment of the technical details of Bitcoin transaction see [Narayanan \*et al.\* \(2016, chs. 1-3\)](#) and [Antonopoulos \(2015, chs. 5-7\)](#). [Vigna and Casey \(2015\)](#) provide a more informal exposition.

In order to transact using Bitcoin, a user usually possesses a ‘wallet’. A wallet typically contains:

- ‘Addresses’

<sup>15</sup>See <https://blockchain.info/charts> (downloaded 16 June 2017) for the average number of transactions per block.

- Private cryptographic keys
- Public cryptographic keys, and
- A sequence of past transactions, which is akin to an account balance.

An address is similar to an identifier for a bank account. It should be noted that there is no physical 'address' within the hardware of some computer that 'stores' crypto-currency coins. Instead, the address is best thought of as specifying an identifier in the duplicate ledgers that record all transactions, similar to an account number in a commercial bank's ledger. In practice, an individual may have multiple addresses, and indeed could use each address for only a single onward transaction. We will come back to this issue in a moment.

Each address is uniquely associated with a pair of private and public keys. In fact, an address is essentially short-hand for its corresponding public key.<sup>16</sup> These keys are simply strings of letters and numbers used to protect messages cryptographically. The account address is public and the contents of an address can in some sense be viewed by everyone, but only the private key can be used to 'unlock' the address to undertake a transaction. Furthermore, although different address balances are public information, it is not possible, or at least not easy, to connect addresses to specific individuals, unless they themselves disclose ownership.

A wallet is typically software on an electronic device – such as an app on a smartphone – that helps a person to manage their public and private keys, their addresses, and their balances. Some wallets are 'full nodes' that contain the entire history of transactions. These nodes can use computing power to validate transactions, adding them to the ledgers, while others are 'lightweight' clients that only focus on the addresses and past transactions relevant for a given person or business. In some ways, digital wallets are akin to EFTPOS<sup>17</sup> cards that enable one to access a bank account balance, with the EFTPOS card's security pin serving the same role as the private cryptographic key, preventing illegitimate access to an account.

Here we provide a brief description of a generic transaction using Bitcoin.<sup>18</sup> If person A wants to send crypto-currency to café B, then person A sends a message to the network of 'miners' who

<sup>16</sup>The account address is a transformed, shorter function of the public key. Some of the transformations are to make numbers distinguishable (avoiding lowercase L, uppercase i, capital 'oh' and zero), while others are to provide an internal cross-check on the number (like a 'checksum' for a file), to ensure that the address is valid.

<sup>17</sup>Electronic Fund Transfers at Point of Sale.

<sup>18</sup>See [Antonopoulos \(2015\)](#) and [Narayanan et al. \(2016\)](#) for more details.

---

undertake the financial book-keeping. This message contains a Bitcoin address for Café B and the amount to be transferred. Person A secures the contents of the message cryptographically by digitally signing it using their private key, so that the miners know that the transaction is correctly authorized. These cryptographic details are discussed in greater depth shortly.

Transactions are characterised as a combination of 'inputs' and 'outputs'. The inputs can be thought of as the 'from' details of the transaction, while the outputs are the balancing details of the 'to' payment. To transact, person A transfers bitcoins from previous transactions on to person B. If the transaction with B is large then A may need to transfer bitcoins from multiple previous inflows (multiple 'inputs' may be required). Conversely, if the transaction is small then a single previous inflow may suffice. Since previous transactions may not be exactly the same size as the current transaction, person A will need to redirect the excess amount, the 'change', back to an address that she or he controls. The output of the transaction 'encumbers' the bitcoins used in the transaction with Café B's public key: B's *private* key needs to be used to 'spend' those coins in their next future transaction. The miners authenticate A's message containing the transaction details – verifying its accuracy – using A's public key, the signature and the message. Person A does not – and should not – reveal the private key that proves he or she is the owner of the address that is being debited.

If café B is selling a sandwich, they need to provide their address and the amount to A. Café B can convey that information by producing a QR (quick response) code with the requisite information or by using a phone's NFC (near field communication) capability. A QR code is typically a black-and-white square image, akin to a barcode, that can encapsulate information. See figure 1 for an example. Buyer A can use a camera on a smart phone to decode the QR code to provide the transaction details directly to the wallet, making it easier to implement the transaction, eliminating the need to write out long addresses and other transaction details by hand. To illustrate why addresses are more convenient than public keys and to show why QR-codes or NFC capabilities are desirable, we replicate the genesis address from the first bitcoin transaction and report Satoshi Nakamoto's PGP (pretty good privacy) public key in figure 2. Satoshi used the latter key to digitally sign emails sent to the original Bitcoin developers, making those messages tamper-proof.

Potential transactions are first stored in the Mempool (the Memory-Pool) when they are sent to

Figure 1: Example QR-code



Figure 2: Genesis address and Satoshi Nakamoto's public PGP key

```

Address:
1A1zP1eP5QGeFi2DMPTfTL5SLmv7DivfNa
Source: http://www.theopenledger.com/9-most-famous-bitcoin-
addresses/

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.7 (MingW32)

mQGiBEkJ+qcRBADKDtZlYDRtP1Q7/ShuzBJzUh9hoVvowogf2W07U6G9BqKW24r
pi0UymErjMfFvNtozNk+33cd/sq3gi0501ImZzg2rbF4ne5t3ip1XnNuzNn+j+6
VxxA16GPhBRprvng8r9GYALLUpo9Xk17KE429YKfGvvtTPtEGUlp01EwCg7FmW
dBbRp4mn5GfXQNT1hZp9WgkD/3p20cB5m4enzfYlOHXmRfJKBMFO2ZDnsY1GqEhV
/LjkhCusTp2qz4thLycYOFKGMAddpVnMsE/TYZLgpsxjrJsrEPNSdoXk3lGfStow
mXjTfr9xN0rB20Qk0Z001mip0Wmgse4PmIu02X240apWtyhdHsX3oBLcwDdke8aE
gAh8A/sHlK7fL1B18rFzx6hb+2y1lD/fazMBVZUe0r2uo7ldqEz5+GeEiBFignd5
HHhqjJw8rUJkfeZBoTKYlDKo7XDrTRxfyzNuZZPxBLTj+keY8WgYhQ5MwsSC2MX7
FZHaJddYa0pzUmFZmQh0ydu1VUQnLkzRSunsjG0nmxiWBZwb6bQjU2F0b3NoaSB0
YwthbW90byA8c2F0b3NoaW5AZ214LmNvbT6lYAQTEQIAIAUCSQn6pwIbAwYLCGgH
AwIEFQIIAwQWAgMBAh4BAheAAoJEBjAnoZeyUihXGMAnjiWJ0fvmSgSM3o6Tu3q
RME9GN7QAKCGrFw9SUD0e9/YDcqhX1aPMrYue7kCDQRJCFqnEA9A90TCjLa6Sj7t
dZcQxNurSDSCSB+yznIGzFGXXpJk7GgKx3H9Z14E6zJTQGL2GAV4k1kSfNtvs
SGJQCnebuZVwtqy1vXRNVPFQFvLVVo2jJCBHWjb03fmXmavIUtRChoc8xgVJMQ
LrwwS943GgsqSbdokZwdTfnEq+UaGo+QfV6NpT3Y1OCXUiNBITZ0JcJdJHD7BO
XRqomX2wSguv+btYdhQGGQiaEx73XMftXNCxbOpqwsODQns7xTc12ENru9BNIQME
I7L9FYBQUiKhm1k6RrBy1as8XE1S2jEos7GAmLfF1wShFUX+NF1VOPdbN3ZdFoWq
sUjKk+QbrwADBQgA9DiD4+uuRhwk2B1TmtrXnwhcdkE7ZbLHjxBfCsLPAZiPh8c
ICfV3S418i4H1Ycz2ItcnC8KAPoS6mipyS28AU1B7zJYP0DBnE7aPSPzHJfudMK
MqiCH1jVrE23xsKTC0sIhhSKcr2G+6ARoG51wuoqJqEyDrb1VQFPvXBNPHSTqu
05PoLQc7PKG5SyQuZgEALekIt12SL2yBRRG01VJLnvZ6eaovkA1gsbGdlie0r0
UwWuJCwzZuBDrumYAfyQBvYfXZun3Zm84rW7Jclp18mXITwGCVHg/P5n7QMbfZQ
A25ymkuj636Nqh+c4zRnSINfyrDcID7AcqEb6ThJBBgRAgAJBQJJCfqnAhsMAoJ
EBjAnoZeyUihPrCAniVW15M44RuGctJe+IMNX4eVkc08AJ9v7cXsp5uDDQn08q3R
8RHwN4Gk8w==
=3Fte
-----END PGP PUBLIC KEY BLOCK-----
Source: https://bitcointalk.org/Satoshi_Nakamoto.asc

```

the peer-to-peer network of nodes. At this point they have not been verified and incorporated into the blockchain ledger. As illustrated in figure 3 the network of nodes is connected to each other in a random, non-hierarchical manner, and so transaction messages may take time to disseminate across the entire network. Because of the vagaries of the network one cannot guarantee that all Nodes (Miners) will have access to the same Mempool of forthcoming, desired transactions. Consequently, the transactions are *not* processed on a first-in-first-out basis. Indeed, different nodes may have received messages in a different order.

Adding blocks to the ledger is performed by the 'miners' associated with the different nodes. The term 'accountant' is a more appropriate label than miner, since the important responsibility of the miners is to *validate* transactions and maintain the integrity of the duplicate ledgers that record transactions. The miners are rewarded with crypto-currency for this validation service as part of the programmed protocols underpinning the currency. Satoshi Nakamoto 'mined' the first block in January 2009 and received 50 bitcoins as a reward. Satoshi later sent coins to Hal Finney, an early developer. Other transactions followed and more users became involved in the mining (validation) process creating the supply of bitcoins.

---

The blockchain has the details of all the transactions that a particular account holder has previously undertaken, both additions and subtractions to their implicit account balance ([Extance, 2015](#)). By going through the history of transactions, miners verify whether person A and other transactors have enough coins to undertake their transactions. This validation prevents double spending: a transactor cannot use the same inputs in two different transactions. In traditional e-payment systems, financial intermediaries such as banks keep track of ledgers and prevent such double-spending. Although seemingly complicated, validating transactions, ensuring that account balances are non-negative, is relatively simple from a computational perspective.

In figure 3 the network of miners is an undirected graph, and the blue arrows represent the flow of information about the  $A \rightarrow B$  transaction through the network. In this figure we assume that Node/Miner 1 is the first to solve the computational problem that provides them with the right to augment the blockchain with an additional block. We talk more about this computation problem below. The new extended blockchain propagates back through the network, depicted with the dotted red arrows. We are assuming that Café B learns that the blockchain has been updated from Node/Miner 4 – signalling that payment has been made for the cup of coffee. Each Node has access to a full rendition of the blockchain up to time  $t$ , subject to the vagaries of network communication, and has its own version of the Mempool, which we have not depicted in the figure.

A transaction between person A and café B will be visible to the network nearly immediately, but it will only be confirmed once it is collated into a ‘block’ of transactions that is incorporated into the distributed ledger. The miner who successfully adds the block to the blockchain has their own balance in the ledger increased with an accounting fee – this is the point at which new ‘bitcoins’ come into existence and the aggregate bitcoin balance is increased. Implicitly, the miner adds the fee transaction to the block. Note that the newly ‘minted’ bitcoins do not have distinct serial numbers associated with them, as paper notes do. Instead, bitcoins are associated with a given history of transactions over time. In principle, two or more bitcoins could be used for the same transactions, and thus end up with the same transaction history. The minting analogy is a little unfortunate because it is suggestive of a physical existence for bitcoins, which is not the case in practice. The exact number of miners participating in the competition to validate and authenticate blocks is difficult to ascertain. One estimate from late 2016 suggested that there

were as many as 100,000 miners.<sup>19</sup> Miners are free to join or leave the network, responding to the relative costs and rewards associated with validating transactions.

The right to augment the chain proceeds roughly in the following manner. Miners protect the integrity of the ledger(s) by hashing blocks of transaction data. First, to protect the integrity of the message/transaction, miners reduce the message into an encrypted 'hash' – a 64 character representation of the message using (hexadecimal) digits 0-9 and letters a-f. As an example, the SHA-256 hash for "The quick brown fox jumped over the lazy dog." (with quotes) is:

```
309eaf49c77e61a70a20b848a494ce13235d13e7297a2033ca18ee3a59b48fd1
```

while the hash for the same sentence without quotation marks is:<sup>20</sup>

```
68b1282b91de2c054c36629cb8dd447f12f096d3e3c587978dc2248444633483
```

Even tiny changes in the underlying message lead to substantial changes in the hash used to represent it. The hash from the first transaction in the block is combined with the next subsequent transaction and the first hash plus second messages are then hashed together in turn. This process is conducted a number of times, forming a 'block' of transaction data that is due to be added to the blockchain. Even extremely long 'messages' can be compressed into a hash with a similar number of characters. For example, the hash for an earlier version of this entire paper was:

```
62acfa1247b7e23d35f6f0a3eb7d683f685b75ac1eea7ae56cd21ec2db128079
```

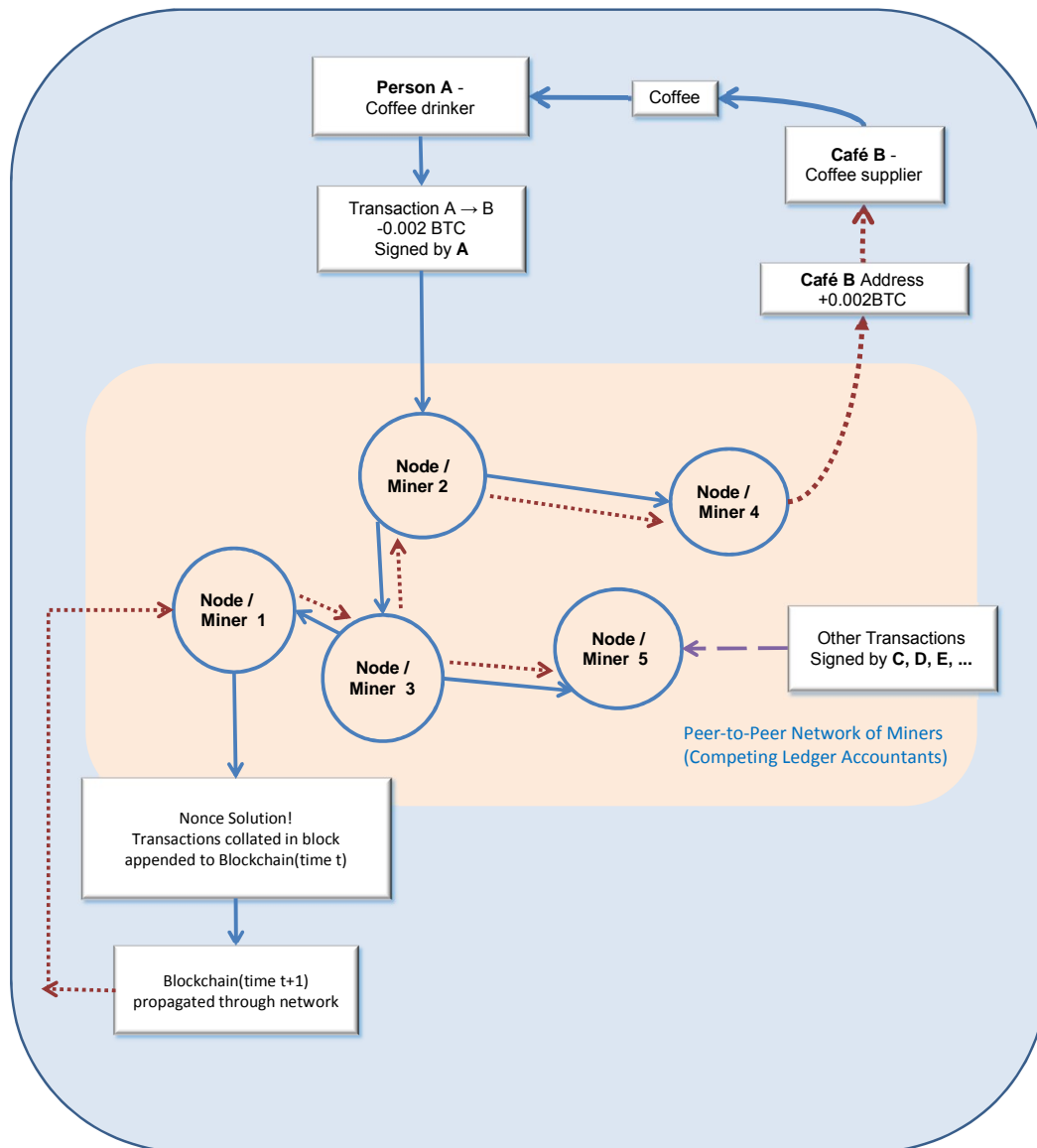
Hashing is a one-way function. It is not practically possible to reverse the process, to map from the hash back to the original message. However, if one has a message and its hash (with no counterfeiting concerns for the latter), it is easy to recompute the hash of the message to ensure that the message replicates the hash, verifying the integrity of the message. Hashes are not necessarily unique. Two different blocks of text could in principle result in the same hash – known as a 'collision' – but such instances are extremely uncommon. [Narayanan et al. \(2016, ch. 1\)](#) discusses 'collision resistance', the likelihood of being able to find an alternate message with the same hash. Practical experience with commonly-used hash functions suggests that it would take a very long time to identify collisions, though there is no definitive proof of collision resistance. It

<sup>19</sup><http://organofcorti.blogspot.co.nz/>, downloaded 14 June 2017.

<sup>20</sup>See for example <https://quickhash.com/> to generate these hashes.



Figure 3: Stylized Bitcoin transaction



is even more unlikely that a counterfeit transaction message suitable for Bitcoin, complete with a counterfeit address controlled by a specific individual, would have the same hash as an original, non-counterfeit transaction.

The miners search for a 'block hash' to capture the information in the block that links together with the hash of the previous block in the chain ([Extance, 2015](#)). The blockchain hashes are thus recursively connected to each other.<sup>21</sup> If an individual tried to subvert the ledger by revising a transaction message, say to institute a double-spend, it would contaminate that transaction message's hash, the hash of the entire block containing the transaction message, and then the hashes used to link all subsequent blocks together.

The block hash is required by the protocols of the blockchain to have a certain number of zeroes at the beginning of the hash. The only way to generate an acceptable hash is to add a 'nonce' – a made-up segment of text – to the block of messages. The miners search across different nonces to find a hash with the required number of zeroes. A suitable nonce is difficult to find, but once found it is easy to verify that the nonce, in conjunction with the hash of the preceding block and the transaction messages embodied in the block, results in an acceptable hash with the desired number of zeroes. The nonce is referred to as a 'proof of work'.

The time delay introduced by this nonce-search prevents an 'attacker' from falsely amending the history of the ledger and then recomputing all the recursive hashes; to be successful an attacker would need to be able to find hashes faster than all honest nodes combined ([Nakamoto, 2008](#)). Importantly, the search for the nonce randomizes the miner who gets to update the chain, which prevents a single miner from monopolising control over the ledger. Having found the nonce, the miner can augment the blockchain, claiming their reward. Transactors may also reward miners with an additional transaction fee to encourage them to process the transaction. Since the search for the correct solution is something of a lottery, some miners form syndicates to diversify the risk and reward associated with the search for solutions.

With Bitcoin protocols, the difficulty of finding an acceptable nonce is adjusted by changing the number of required zeroes, offsetting changes in the number of miners and changes in computing power. On average it takes ten minutes for each new block to be added to the ledger ([Narayanan](#)

---

<sup>21</sup>These intertwined sequences of hashes are akin to a 'Merkle tree'. See [Narayanan et al. \(2016\)](#) for a more explicit characterisation of the differences.

---

*et al.*, 2016). The delay that results from the proof of work also provides a window of time for an elongated chain to propagate across the network, and reduces the likelihood that different nodes will have different ledgers. Some alternative crypto-currency algorithms generate blocks more quickly. For example, Litecoin, which is based on Bitcoin, adds blocks every two and a half minutes (Adamsson and Tahir, 2015). Miners now use fast, specially-designed computers to evaluate candidate nonces by brute computational force. This computational process literally takes time and energy. Under this scheme, miners incur costs associated with the investment in computing power and electricity to solve the hash problem, to add the new block.

The new block is verified by other miners and the new elongated chain is accepted if the transactions are all valid. Although the longest blockchain becomes the distributed ledger of record, which is then adopted by all computer nodes, distinct blocks will occasionally be added (near) simultaneously creating a 'fork' – two competing chains. One of these chains will ultimately be discarded, eg if another block is successfully added to the second chain it will become clear that the second blockchain is longer. Consequently, the block on the first shorter chain will become 'orphaned'. The transactions in the orphaned block will need to be incorporated into the longer chain that has ultimately become the ledger of record, delaying the validation of these orphaned transactions.

For Bitcoin, the reward for finding a suitable nonce (and adding the block to the blockchain) was initially 50 bitcoins, but the reward is automatically decreasing in size as the total supply of coins increases. Given the diminishing reward structure, the transactions fees that transactors offer for authentication will eventually become important to ensure that miners continue to perform authentication services. Even with the current validation rewards, considerable backlogs of transactions requiring validation have occasionally built up – over a 150,000 transactions in at least one instance. In such cases, the supply of transactions is simply exceeding the validation capacity of the network, and there is little that even the miners can do to rectify this imbalance, as devoting more computational resources leaves the average processing time unchanged.

The reward system keeps multiple parties involved in the validation and ledger (blockchain) process, ensuring that it remains decentralized. While a strength in diffusing influence over the system, this system also introduces computational costs and expense. In principle, a single, trusted authority maintaining the ledger would reduce the duplication of effort required to update records.

However, decentralisation reduces the risk that the central ledger fails, either for technical reasons or because of malfeasance.

In this section we have devoted considerable effort to explain proof of work schemes to maintain the integrity of Bitcoin ledgers. Other crypto-currencies, such as Peercoin and Nextcoin, use alternative validation schemes, such as 'proof-of-stake'. In Peercoin's schema, the probability of updating the chain depends on the 'age' of coins that are staked.<sup>22</sup> The 'stake' is sent to one's self in a transaction, which re-sets the age of the coins to zero. Other variants of proof-of-stake are used by other crypto-currencies. Again, the intention is to ensure that no single entity has a monopoly on updating the ledger, protecting the integrity of the ledger at a lower cost than the proof-of-work protocol. For further discussion, see [Narayanan \*et al.\* \(2016, sn. 8.5\)](#).

### 3. What purpose do crypto-currencies serve?

#### 3.1 Crypto-currency and the basic functions of money

In this section we compare the properties of crypto-currencies to the basic functions of money.<sup>23</sup> Money is traditionally associated with three main purposes: it is a generally accepted form of payment (a medium of exchange); it is a unit of account that can be used to compare prices of different goods; and it acts as a store of value ([Lipsey, 1963](#); [Burda and Wyplosz, 1993](#); [Bank of Canada, 2014a](#)).<sup>24</sup> How do crypto-currencies stack up in these terms?

Despite growing popularity, crypto-currencies are far from being a generally accepted form of payment. Once again, we focus on Bitcoin, as the most popular crypto-currency. [Weber \(2016\)](#) reports that 106,000 businesses accepted bitcoins as payment. While this seems like a non-trivial number of retailers, the scale of Bitcoin is still very small relative to traditional payments systems. In 2010 there were approximately 27.9 million small businesses in the United States alone.<sup>25</sup> [Szczepánski \(2014\)](#) compares the Bitcoin market to Visa and Mastercard in 2014 and notes that

<sup>22</sup>'Age' is the length of time one has owned coins.

<sup>23</sup>See also [Yermack \(2013\)](#).

<sup>24</sup>Other useful characteristics for money include divisibility, portability, indestructability, and 'cognizability', amongst others; see [Jevons \(1896, ch. 5\)](#).

<sup>25</sup>[https://www.sba.gov/sites/default/files/FAQ\\_Sept\\_2012.pdf](https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf).

Bitcoin undertook less than USD100 million worth of transactions per day, which is 1 percent or less of the (daily) USD16.5 billion and USD9.8 billion of transactions that were mediated by Visa and MasterCard respectively.

Next we compare Bitcoin to transactions mediated by New Zealand's financial system. We first provide a sense of scale and context for the New Zealand economy: New Zealand's population is less than 5 million people, roughly the size of Louisiana, and its per capita income in 2016 was roughly USD39,500, a little less than that of the state of Mississippi or the United Kingdom.<sup>26</sup> New Zealand's financial system is dominated by four large commercial banks. The number of 'unbanked' individuals in New Zealand is comparatively low: 99.4 percent of adults 15 years old and above have accounts in formal financial institutions.<sup>27</sup> Debit and credit cards are used extensively to conduct transactions in New Zealand, typically at EFTPOS terminals at local retailers.

Between May 2016 and April 2017 approximately NZD80.6 billion of electronic transactions were processed by New Zealand financial institutions, which corresponds to about NZD221 million per day in roughly 4.4 million transactions.<sup>28</sup> To process 4.4 million transactions, Bitcoin would need to process  $4,400,000 \div (24 \times 6) \approx 30,555$  transactions per ten minute period, roughly *twelve* times the number of transactions that Bitcoin can currently handle. Unless the underlying software protocols are amended, Bitcoin could not cope with the volume of transactions undertaken in New Zealand, let alone the world. These scalability issues are particularly acute since part of the appeal of crypto-currencies is that they could facilitate transactions in multiple jurisdictions. The ECB (2015) provides a comparison to a much larger economic region, noting that there were 274 million electronic retail transactions per day in the European Union. In contrast, even with recent data from 1 January – 12 October 2017, Bitcoin was facilitating around 270 thousand transactions in the world as a whole – though exactly how many of these were retail transactions for goods and services is unclear.<sup>29</sup>

Scalability issues are already a problem, with an increased number of transactions ending up in the queue awaiting confirmation – the 'mempool'. See figure 4. Furthermore, Bitcoin seems to have reached its maximum processing capacity, given the one million byte constraint on block-size.

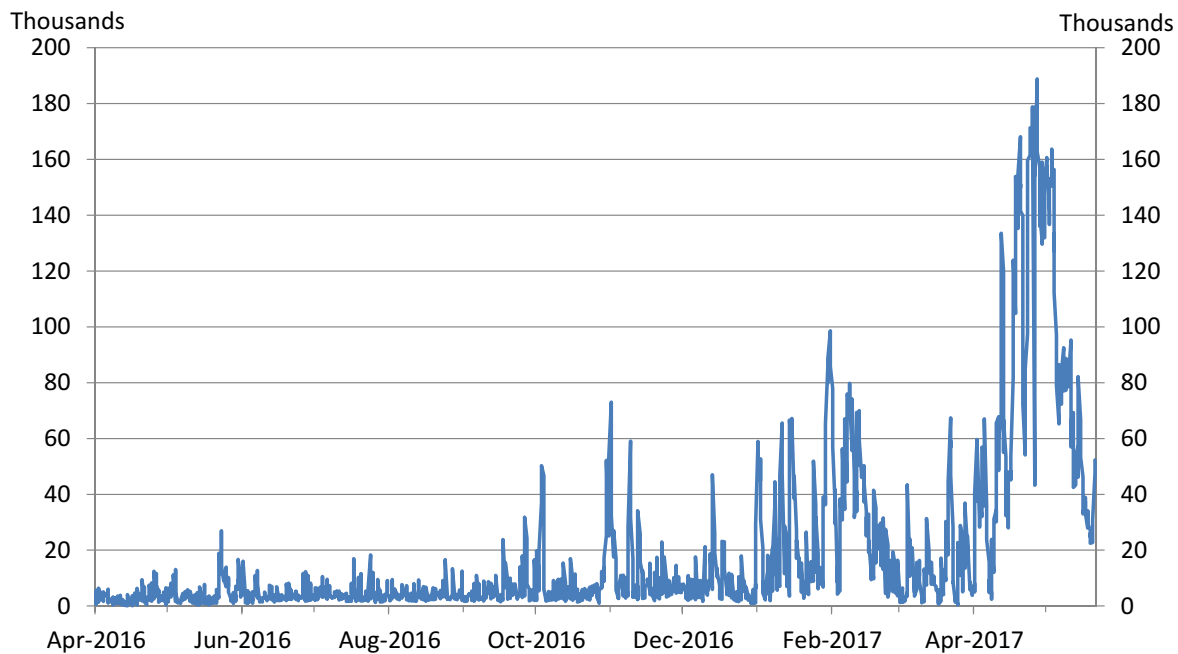
<sup>26</sup><https://data.worldbank.org/indicator/NY.GDP.PCAP.CD>.

<sup>27</sup>[http://siteresources.worldbank.org/EXTGLOBALFINREPORT/Resources/8816096-1361888425203/9062080-1364927957721/GFDR-2014\\_Complete\\_Report.pdf](http://siteresources.worldbank.org/EXTGLOBALFINREPORT/Resources/8816096-1361888425203/9062080-1364927957721/GFDR-2014_Complete_Report.pdf).

<sup>28</sup>Electronic Card Transactions: April 2017. Statistics New Zealand.

<sup>29</sup><https://blockchain.info/> accessed 15 October 2017.

Figure 4: Unconfirmed transactions in the mempool

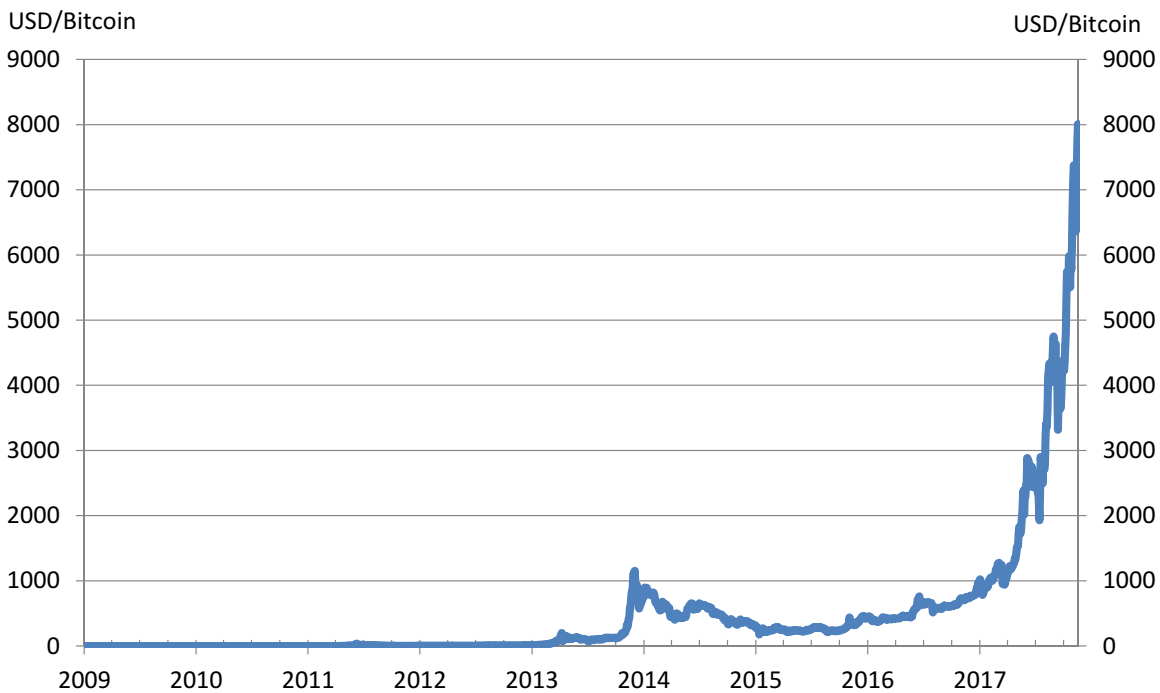


Gavin Andresen has suggested that the average transaction size is about 250 bytes,<sup>30</sup> implying that roughly 4000 transactions can be squeezed into a block. Given that each block takes ten minutes to process on average, Bitcoin can process a maximum of  $4000 \times 6 \times 24 = 576,000$  transactions per 24 hour period. In practice, the largest number of Bitcoin transactions processed in a single day, on 23 May 2017, was 367,000. And May 3, 2017 had the highest daily average number of Bitcoin transactions/block, 2236, well short of the hypothetical maximum.

Crypto-currencies have been a highly volatile store of value, which is most apparent in the extremely high volatility exhibited by Bitcoin relative to traditional fiat currencies. *Böhme et al. (2015)* suggest that the Bitcoin market is relatively shallow and that people attempting to trade large volumes relatively quickly may affect the Bitcoin exchange rate. *Yermack (2013)* notes that the law of one price does not seem to work very effectively for Bitcoin, with different exchanges transacting at materially different USD/BTC exchange rates. *Böhme et al.* argue that Bitcoin's exchange rate volatility is of concern to users who are transacting in Bitcoin as well those who are

<sup>30</sup><https://bitcointalk.org/index.php?topic=813324.0>, accessed 12 October 2017.

Figure 5: Price of Bitcoin (USD)



Source: Blockchain.info

using Bitcoin as a store of value. Using monthly data, we find that the standard deviation of the month-on-month percentage point changes in Bitcoin/USD is 73.1 percent, while the equivalent for the NZD/USD exchange rate is 3.6 percent.<sup>31</sup> While there have been a few large (positive) outliers, most percentage point changes have been between -40 and +89 percent for Bitcoin, cf. -9.7 and +6.6 percentage points for the USD/NZD exchange rate. [Yermack \(2013\)](#) notes that this volatility is large even relative to risky equities. The volatility of the Bitcoin exchange rate against the US dollar is particularly problematic if users' assets are denominated in Bitcoin and liabilities are denominated in US dollars. If, for example, Bitcoin users have liabilities such as taxes denominated in USD then volatility in the Bitcoin-USD exchange rate creates volatility in their tax liabilities and hence their net worth. [Yermack \(2013\)](#) discusses Bitcoin as an additional asset class, largely discounting its value as a risk management tool.

Volatility in the value of Bitcoin is also a negative feature for real transactions. In principle, any

<sup>31</sup>We use data from August 2010 - May 2017 for these calculations. We compute the standard deviation of  $100 \times (BTC_t/BTC_{t-1} - 1)$ , where  $BTC_t$  is USD/bitcoin at time  $t$ , and compare to the USD/NZD equivalent.

---

good or service could be used as a unit of account – a common standard for comparing the prices of different goods and services. We could figure out how many hamburgers it takes to obtain a taxi ride home. Or how many kilogrammes of carrots it would take to purchase an iPhone. In practice, it is helpful to economise on the number of prices one remembers by using a single common numeraire to evaluate transactions. A good numeraire will exhibit stable purchasing power with respect to some average of goods and services, though individual prices may fluctuate. Prices in a given numeraire should not fluctuate because of issues specific to the numeraire. For example, carrots would not be a good numeraire if carrot blight suddenly affected the availability of carrots. Suppose we took a Red taxi yesterday and a Blue taxi today, both paid in kilogrammes of carrots. Ideally, these two prices will be informative when choosing which company to use in future. But if the Blue taxi price in carrots today is high simply because of carrot blight then the allocative signal provided by these two prices is distorted.

In practice, merchants that accept bitcoins usually price their goods in fiat currency units, such as US dollars, and accept the equivalent number of bitcoins based on the exchange rate at the time of the transaction ([Johnson and Pomorski, 2014](#)). Most merchants convert their bitcoin holdings into US dollars straight away, using a Bitcoin currency exchange such as Coinbase ([Davidson, 2015](#)). Bitcoin thus does not really serve as a unit of account. [Cheah and Fry \(2015, p. 33\)](#) argue that Bitcoin's volatility undermines its use as a unit of account.

The New Monetarist literature described by [Williamson and Wright \(2010\)](#) and [Williamson and Wright \(2011\)](#) emphasizes the simultaneous existence of money and credit markets and the need to be specific about the frictions that motivate these payment mechanisms. One imperfection emphasized by [Kocherlakota \(1998, 2000, 2002\)](#) is the existence of imperfect 'memory' in relation to past transactions. Digital currencies replace physical currencies by providing memory via the ledger of transactions. [Hendrickson et al. \(2016\)](#) make use of the search and matching framework commonly used in the New Monetarist literature, and develop a model that simultaneously contains government legal tender and Bitcoin. They then investigate the conditions under which a government could deter the use of Bitcoin. They find that Bitcoin usage may still occur in equilibrium even if the government refuses to transact in it, provided that some transactors are sufficiently committed to its use.



## 3.2 Motivations for using crypto-currencies

Given that there are alternative methods of payment, why are crypto-currencies being developed and adopted? The original paper that spawned interest in crypto-currencies, [Nakamoto \(2008\)](#), aimed to develop a method of exchange that did not require trust in third party financial intermediaries. The 'genesis block' first verified by Satoshi Nakamoto referenced a 3 January 2009 *Times* headline 'Chancellor on brink of second bailout for banks'. It is apparent that the crypto-currency movement was in part motivated by the global financial crisis and a lack of trust in traditional financial intermediaries and the regulatory authorities responsible for ensuring financial stability.<sup>32</sup> Nevertheless, as fiduciary currencies, trust is *essential* for the continued acceptability of crypto-currencies. Crypto-currency users must trust the computer programmers who have taken up the design mantle for crypto-currencies, users must trust the miners responsible for validating transactions, and indeed transactors need to trust that others will continue to value and accept crypto-currency units.

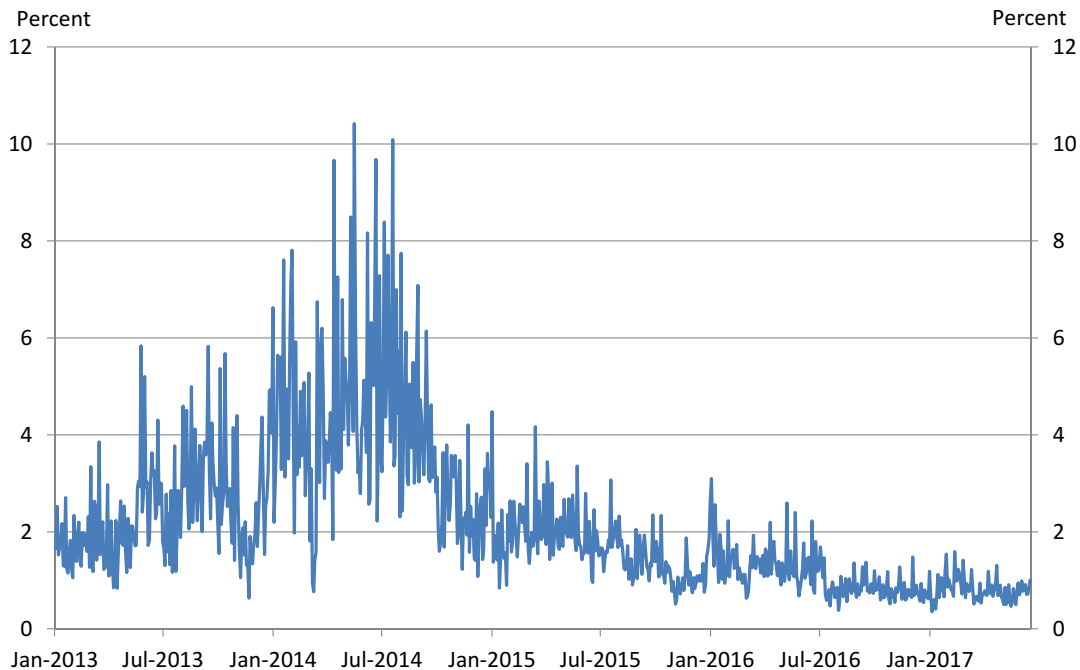
Although crypto-currencies arguably fail to satisfy the basic functions of money, their increased popularity is also motivated by genuine economic considerations, including lower transaction costs, 'pseudonymous' payments, transaction irreversibility, and the potential to attract a new customer base. We discuss these reasons in turn.

The [BIS \(2015\)](#) identifies transaction costs as an important demand side factor motivating the use of crypto-currencies. Transaction costs are very important to small businesses. For example, high credit card fees (2.5 - 4.5 percent of the value of goods and services being exchanged) mean that 55 percent of American small businesses do not accept credit cards ([Kloc, 2014](#)).

Reduced transactions costs may be a particularly important advantage in relation to international transactions. The ubiquitous nature of the internet means that crypto-currencies are relatively unconstrained by geography as physical transportation costs and physical security concerns are negligible for digital currencies. Some early analysis by [Goldman Sachs \(2014\)](#) noted that transaction costs for international remittances were around 1 percent using Bitcoin, relative to 8-9 percent for traditional remitters, implying scope for a significant reduction in costs. More recent

<sup>32</sup> [Antonopoulos \(2016\)](#) provides a polemical view of financial and regulatory surveillance. [Ali et al. \(2015\)](#) discuss these libertarian motivations further.

Figure 6: Transactions costs (percent of transaction value)



Source: <https://blockchain.info/charts/cost-per-transaction-percent>

2016-2017 data suggests that Bitcoin transactions fees range from 0.35 to 3.1 percent of the value of transactions, with a median/mean transaction cost around 0.9-1.0 percent.<sup>33</sup> See figure 6.

Aside from economic considerations, many users of crypto-currencies are drawn to them because they are thought to be anonymous – or at least more anonymous than electronic transactions facilitated by regulated banks, which are required to adhere to ‘know your customer’ protocols. Anonymity is of obvious value to individuals undertaking illegal transactions, such as those associated with trade in illegal drugs. Of course, as [Szczepáński \(2014\)](#) and others point out, decentralised ledger systems are not totally anonymous. Although users are not explicitly identified, distributed ledgers typically have a public record of every transaction undertaken ([ECB, 2012](#)). If investigators can link a transactor to an address, then they can ascertain all their previ-

<sup>33</sup>See <https://blockchain.info/charts/cost-per-transaction-percent>.

ous transactions via the public information on the blockchain (Marian, 2015). Such analysis does become more difficult if individuals cycle through multiple addresses, but various other techniques can be used to undermine the anonymity of the system, such as tracking the IP (Internet Protocol) addresses of account holders, and data mining of the blockchain to try to identify transactors. Narayanan *et al.* (2016, sn. 6.2) discusses mechanisms to deanonymize Bitcoin. Conversely, a number of crypto-currencies, such as Zerocoin and Zerocash for example, have been developed to try to achieve total anonymity. Böhme *et al.* (2015) and Narayanan *et al.* (2016, sn. 6.3) provide details of 'mixing' mechanisms used to achieve anonymity.

Irreversibility is another motive for using crypto-currencies, one that received considerable emphasis in Nakamoto (2008). There are currently no mechanisms to reverse transactions in the crypto-currency domain. This is an advantage for merchants: in current payment systems involving credit cards, merchants are susceptible to fraud and may have transactions reversed after customers have received goods/services (BIS, 2015). Yet irreversibility may be a deterrent for customers, because they rely on merchants to provide redress if a good or service is faulty. Of course, legal systems and the ongoing value of merchant reputations may help to provide redress, provided transactions are documented, eg with receipts.

Merchants may also adopt crypto-currencies to attract new customers. Early adopters of technology may be more inclined to use services of companies that offer crypto-currencies as a payment method simply because they like being involved with new technologies (BIS, 2015). Consistent with this thesis, technology and telecommunication firms have been among the early adopters of crypto-currencies. In New Zealand, for example, internet and telecommunications companies such as Slingshot and 2talk have established mechanisms to accept bitcoins. A number of international companies that accept crypto-currencies for some goods or services are listed below, many of which have strong links with the technology industry.<sup>34</sup>

<sup>34</sup>See also <https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/>. Note that some firms only accept crypto-currencies for some of their goods or services.

- 
- Amazon
  - WordPress.com
  - Bloomberg
  - Dell
  - Microsoft
  - Virgin Galactic
  - Expedia.com
  - PayPal

### 3.3 What are crypto-currencies really used for?

Crypto-currencies are regularly associated with four types of transactions or motivations: speculation; illegal transactions; gambling; and cross-border transactions such as remittances. [Glaser et al. \(2014\)](#) examine whether users' interest in digital currencies stems from their utility as transaction media or because of their appeal as an asset class and conclude that it is the latter aspect for most holders.<sup>35</sup> Fred Ehrsam, a co-founder of Coinbase, one of the leading digital wallet providers, estimated that 80-95 percent of transactions in 2013 and 2014 using Coinbase were related to speculation (see [Goldman Sachs 2014](#)).

Regulatory frameworks can be slow to adjust to emerging technologies. As a result, criminals have an incentive to take advantage of new transaction media. Money laundering is a common financial crime in the crypto-currency domain due to pseudonymity and a lack of regulation ([ECB 2012](#), [European Banking Authority](#), [Federal Bureau of Investigation 2012](#)). Ponzi schemes are also a threat in the virtual currency domain, and have garnered the attention of the United States Securities and Exchange Commission ([SEC, 2013](#)).

[Trautman \(2014\)](#) discusses the regulation of crypto-currencies and provides details on many of the highest profile criminal cases up until 2014. To cite just a few, the Liberty Reserve case involved money laundering; the Western Express International case involved money laundering and servicing criminal transactions in Eastern Europe; and the e-Gold case involved money laundering and unlicensed money transfers ([Trautman, 2014](#); [Levin et al., 2014](#)). [Böhme et al. \(2015\)](#) and [Ali et al. \(2015\)](#) discuss the online Silk Road market place, which facilitated transactions in drugs and firearms and other illegal activities until it was shut down by the Federal Bureau of Investigation

---

<sup>35</sup>Empirically [Cheah and Fry \(2015\)](#) find that the Bitcoin exchange rate has a “substantial speculative bubble component” and suggest that “the ‘fundamental value of Bitcoin is zero.’”

in 2011. Silk Road used bitcoins to settle transactions and had an estimated revenue of USD1.2 billion annually (Ali *et al.*, 2015). Crypto-currency transactions made it possible for sellers on the Silk Road market place to remain pseudonymous because there was no centralised authority connecting addresses to individuals, though these safeguards did not prevent Silk Road's founder, Ross Ulbricht, from being identified and sentenced to life in prison.

The pseudo-anonymity of crypto-currency has also increased the rewards associated with Ransomware attacks, by providing a vehicle for ransom payment. Even law enforcement departments have fallen victim to such attacks (Ali *et al.*, 2015, p. 287). In May 2017 a Ransomware attack was implemented by the 'WannaCry worm', which required payments implemented via Bitcoin. Hundreds of thousands of computers were affected.

Online gambling has been another prominent source of transactions for crypto-currencies. In a fascinating study using cluster analysis, Meiklejohn *et al.* (2016) undertook transactions with entities known to accept bitcoins and then used the resultant addresses to classify transactions on the Bitcoin blockchain. They found that around 64 percent of Bitcoin accounts have never been used and 60 percent of transaction activity occurs through gambling sites. Narayanan *et al.* (2016, ch. 6) discussed this analysis further in the context of anonymity.

Besides Bitcoin, there are other crypto-currencies that have more specialised purposes. Ripple for example, uses a distributed ledger to make cross-border bank-to-bank transactions easier. Ripple is a payment solution that allows users to exchange local currency for a crypto-currency that can be exchanged for a foreign currency. Ripple is thus competing with SWIFT<sup>36</sup> and SEPA,<sup>37</sup> to connect diverse financial markets. See ECB (2015) for more information.

Other applications have also been proposed for distributed ledgers. Koepl and Kronick (2017), for example, suggest that blockchains could be applied to corporate governance to facilitate shareholder voting or to provide timely updates on firm accounts. Distributed ledgers are being developed to assure the provenance of diamonds, to reduce fraud and prevent blood diamonds from entering the market, and have also been proposed as mechanisms to reduce the costs of settlement, custody and registration of financial securities (UK Government Office for Science). Land registries, such as Sweden's Lantmäteriet, are also trialling blockchain ledgers to keep track

<sup>36</sup>Society for Worldwide Interbank Financial Telecommunication.

<sup>37</sup>Single Euro Payment Area.

of land transfers. [Tasca \(2015\)](#) discusses a number of specific projects aimed at asset registry applications. Open access ledgers are a useful mechanism in these applications because they disseminate ownership information to a wide population of potential transactors.

## 4. Implications for all and sundry

Since transacting is at the centre of economic activity, crypto-currencies have implications for consumers, firms and banks. Crypto-currencies also raise legislative design issues regarding the treatment of crypto-currency transactions/contracts, law enforcement issues, taxation issues, and concerns for monetary authorities and financial regulators. In the remainder of this article we discuss the implications that crypto-currencies have for consumers, the financial system, and monetary and regulatory authorities, and make a few comments on taxation. Since this domain is very broad, our discussion is necessarily at a very high level.

### 4.1 Implications for consumers

We noted earlier that there are a number of genuine reasons why consumers may wish to use crypto-currencies to implement transactions. In this section we highlight some of the risks that consumers face using crypto-currencies.

It is well-understood that the integrity of the blockchain rests heavily on the miners. One concern is that a majority of the miners could collude to control the future evolution of the blockchain, in what is known as a '51 percent attack'. It is suggested that the miners in control of the blockchain could reverse transactions during the attack (enabling double-spending of balances), potentially prevent some people from transacting, and could monopolise the creation of new coins.<sup>38</sup> The sequence of hashes connecting blocks in the blockchain would make it difficult to tamper with the history of transactions embedded in the chain, but the other aforementioned actions might still degrade trust in the currency as a medium of exchange, with the potential to undermine its acceptability.

<sup>38</sup><https://learnblockchain.com/cryptocurrency/51-attack>.

---

[Böhme et al. \(2015\)](#) observe that Bitcoin miners are incentivised to maintain the integrity of the crypto-currency because they are rewarded in the same currency. However, [Eyal and Sirer \(2014\)](#) argue that colluding miners could attack the currency to obtain a disproportionate revenue share by selectively revealing the blocks that they have discovered, intentionally forking the blockchain. When the colluding group gains a large enough share of computing power, other miners are incentivised to join the colluding group resulting in the collapse of decentralised blockchain validation.

The security of cryptographic systems also relies on algorithms being more complex than current state-of-the-art computers are capable of solving. If quantum computers were developed with much faster speeds and capabilities then cryptographic techniques would need to be amended to compensate. Technological developments could have a material impact on the security of crypto-currency systems, and the safety of address balances.

Even if the protocols and cryptography used to implement crypto-currencies are secure, consumers may be vulnerable to errors and exploitation in a number of ways. First, if a transactor unintentionally discloses their private key then the balances associated with their addresses could be depleted of value by unauthorised transactions. Second, if the private key is lost then the balance associated with an address would become permanently inaccessible. Yet another risk is that a transactor could erroneously send crypto-currency balances to an incorrect or non-existent address. As there is no central authority, there is no mechanism to reverse unintended transactions. If there is a non-zero probability of sending transactions to uncontrolled or defunct accounts then the aggregate supply of bitcoins could eventually begin a slow dance towards zero. Third, crypto-currency exchanges and even the providers of digital wallets might be susceptible to fraud. [Ali et al. \(2015\)](#) cite research by Dell indicating that 146 strains of malware have been discovered that are designed to steal bitcoins from individuals' computers, by stealing private keys from digital wallets or switching addresses to deliver funds erroneously; half of these malware strands avoided detection from antivirus software.

[Yermack \(2013\)](#) notes that there is no deposit insurance for crypto-currency balances, in contrast to the schemes that exist for bank deposits in most countries (New Zealand being a rather unique exception.) However, the absence of deposit insurance may not be a material issue since crypto-currencies are not a liability of a financial institution, and cannot be extinguished by the failure

of a financial intermediary. That said, mechanical failures or theft as described above could still result in crypto-currency balances disappearing.

A final, deeper concern for consumers is the governance of the currency. Crypto-currency source codes are often contained in Git repositories, which implicitly provides a small number of developers with the ability to amend the source code, subject to an uncertain peer review process. Exactly who has influence over such processes, and the checks and balances on their behaviour, is quite unclear. In contrast, the governance of central banks is typically made explicit in legislation. With respect to Bitcoin, at least one prominent developer, Mike Hearn, has suggested that Bitcoin has failed because of its inability to reach agreement about how to resolve scalability issues (which has caused wildly volatile fees and large transaction backlogs), as well as other governance issues.<sup>39</sup> While users of Bitcoin ‘vote with their feet’ – by using the currency or not – the role of developers is a source of uncertainty for the durability and longevity of the source code, a point also made by [Velde \(2013\)](#): “the governance of the bitcoin code and network is opaque and vulnerable”. Interestingly, a new variant of Bitcoin was introduced in August 2017 to try to resolve the scalability issues discussed in section 3.1. This new Bitcoin variant, termed ‘Bitcoin cash’, changed rules around block size but adopted the Bitcoin ledger at the change-over date, enabling users to spend their traditional bitcoin balances. This fork in the Bitcoin protocol has not gained universal acceptance and most users continue to use the old protocol, ‘Bitcoin’. As at 30 September 2017, ‘Bitcoin cash’ had the fourth highest market capitalisation among crypto-currencies, after Bitcoin, Ethereum, and Ripple.

## 4.2 Implications for financial institutions

[Freixas and Rochet \(1997\)](#) argue that banks provide four main services: i) banks offer access to a payment system; ii) they transform assets (eg maturity); iii) they manage risk; and iv) they process information and monitor borrowers.

Crypto-currencies are focused on the payment system function of banks, enabling peer-to-peer exchanges between counter-parties that may not have enduring transactional relationships. The

<sup>39</sup>See <https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7> and <https://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html>, downloaded 2 August 2017.



---

introduction of crypto-currencies clearly increases competitive pressure on financial institutions providing payment services. However, distributed ledgers clearly involve a duplication of effort that is more costly than maintaining a single ledger. Furthermore, maintaining the entire history of transactions instead of simply current balances increases storage requirements of distributed ledger systems based on transactions.<sup>40</sup> It is not clear that crypto-currencies' alleged cost advantage (see the earlier discussion on transactions costs) is in fact large enough to out-compete traditional financial institutions.

The provision of credit involves ongoing relationships between creditor and borrower. Credit relationships are closely related to banking functions ii), iii) and iv). Credit relationships are largely incompatible with anonymity, since the capacity of Borrower B to repay a loan – and hence Lender W's willingness to lend – depends on expectations of B's future income. As a simple example of functions iii) and iv), Lender W might like to diversify exposure across borrowers  $B_1, \dots, B_n$ , which increases the analytical burden on W of assessing and monitoring potential counter-parties. Financial institutions can do the same monitoring for many individuals, economising on this analytical cost.

The blockchain's underlying premise of pseudo-anonymity is essentially incompatible with borrowing transactions, as it would invite both adverse selection and moral hazard problems. Adverse selection might arise if good quality borrowers are discouraged from borrowing because high interest rates are required to compensate for risky borrowers, further worsening the average riskiness of borrowers. Moral hazard problems might arise because truly anonymous borrowers would have an incentive to default on their loans; ex ante promises to repay debts would not be credible ex post.

Most crypto-currency frameworks are not currently well-designed to handle credit. Crypto-currencies like Bitcoin are designed so that transactions can only be verified and completed if the sender has enough crypto-currency to make the purchase – account balances must be non-negative. Efforts are being made to mend these characteristics, to make it possible to decentralise credit. Platforms such as Ethereum, and an add-on to Bitcoin called Counterparty, have been developed to implement 'smart contracts'.<sup>41</sup> Smart contracts use computer protocols to ensure

---

<sup>40</sup>There are, however, mechanisms to try to 'prune' transaction content from ledgers when that content is no longer needed.

<sup>41</sup>Ripple introduces the concept of IOUs, whereby a person or company grants credit limits for known counter-parties.

that certain features of a contract are executed automatically. For example, Lender W could send 400 coins to Borrower B in exchange for receiving 10 bitcoins from B every month for the next four years. However, enforcement of such a contract is still complicated. For example, it is not clear what mechanisms would be put into play if borrower B exhausted their balance of coins before meeting their obligations under the smart contract.<sup>42</sup> Ethereum envisages using arbitrators or courts to resolve such disputes, which again relies on transactors being identifiable.<sup>43</sup> He *et al.* (2016, box 3) raise additional concerns with smart contracts, including concerns about the legal status of such contracts, consumer protection issues, and concerns that smart contracts, like automated high-frequency trading, might adversely affect asset pricing, with possible implications for financial stability.

The original crypto-currency, Bitcoin, faces competitive pressures on all sides. As discussed in section 3, the open source nature of Bitcoin has made it comparatively easy to create new variant crypto-currencies. Although Bitcoin has network effects that work in its favour as the first crypto-currency, emerging crypto-currencies may offer more efficient or cheaper transaction services, potentially eroding the value of bitcoins. Blockchain technology also has applications in the closed financial networks that are predominantly used to facilitate transactions. Traditional intermediaries such as banks are evolving their business practices to respond to the competitive pressures of crypto-currencies. As an example, the 'R3' consortium of large financial institutions began to develop 'Corda' in September 2015, a platform to facilitate interbank transactions using distributed ledger technology. See [www.corda.net](http://www.corda.net) and Brown *et al.* (2016).<sup>44</sup>

Central banks are also investigating these technologies. In collaboration with private financial institutions, both the Bank of Canada and the Monetary Authority of Singapore are exploring options to use distributed ledger technology to facilitate wholesale transfers.<sup>45</sup> Interestingly, the Bank of Canada has recently concluded that distributed ledger technology is unlikely to yield positive net benefits relative to the centralised system currently employed for wholesale

<sup>42</sup>The International Chamber of Commerce provides contract terms and conditions to try to facilitate the resolution of contracts agreed electronically, which could perhaps be used for smart contracts. See <http://www.iccwbo.org/products-and-services/trade-facilitation/tools-for-e-business/>.

<sup>43</sup><http://legal-tech-blog.de/smart-contracts-ethereum-future-of-contracting>.

<sup>44</sup>In 2016 and 2017 a number of large financial institutions left the R3 consortium to pursue their own distributed ledger initiatives. <http://www.reuters.com/article/us-jpmorgan-r3/jpmorgan-chase-co-leaves-blockchain-consortium-r3-idUSKBN17T2T4>. Downloaded 5 September 2017.

<sup>45</sup>For Canada see <http://www.bankofcanada.ca/research/digital-currencies-and-fintech/fintech-experiments-and-projects/> and for Singapore see <http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox.aspx>.

payments, and suggested that the complexity of decentralized systems could increase operational risks (Chapman *et al.*, 2017). Other central banks are investigating digital currencies to replace cash. In 2015 Ecuador introduced a 'Sistema de Dinero Electrónico', a digital currency system implemented via mobile phones, ostensibly in an effort to reduce the costs of using physical US dollars (the US dollar has been used as legal tender in Ecuador since 2000).<sup>46</sup> A year later, in November 2016, the People's Bank of China quietly opened a 'Digital Currency Research Institute'.<sup>47</sup>

### 4.3 Monetary policy, financial stability, and regulation

In the near term, the development of crypto-currencies should not materially impact central banks' ability to implement monetary policy in their own fiat currencies. Contracts in most economies are predominantly denominated in fiat currency units and as the residual suppliers of local currency central banks can affect their own local interest rates, influencing private agents' liquidity, short-term debt obligations, and incentives to substitute intertemporally. However, central banks will not necessarily be able to influence the interest rates charged in the 'foreign' crypto-currency.

If crypto-currencies become more popular as a payment mechanism, central banks' influence on economic activity might be diminished, adversely impacting macro stabilisation. The Reserve Bank of Australia (2014), in its submission to an Australian Senate inquiry into digital currencies, made essentially the same observation, noting that wide-scale adoption of digital currencies could hinder the Reserve Bank of Australia's ability to deliver low and stable inflation because crypto-currency schemes usually have a predetermined supply path that cannot be altered to match the business cycle. These longer-run concerns about the growth of crypto-currencies and analytical issues about the relationship between measures of crypto-currency and activity are also discussed by the ECB (2012).

Crypto-currencies pose a challenge for all regulators, because the decentralised ledger system means there is no central authority to regulate. In response to this difficulty, the Financial Action

<sup>46</sup>See Wang (2016) and <https://www.cnn.com/2015/02/06/ecuador-becomes-the-first-country-to-roll-out-its-own-digital-durrency.html> (downloaded 2 August 2017). White (2014) suggests that the introduction of the digital currency may be an effort to 'de-dollarize' the Ecuadorean economy.

<sup>47</sup><https://www.yicai.com/news/people%E2%80%99s-bank-china-opens-digital-currency-research-institute>.<sup>48</sup> (downloaded 2 August 2017).

---

Task Force, initiated by the G-7 countries in 1989 to combat money laundering and the financing of terrorism, has called for the regulation of the exchanges that act as the gatekeepers or interfaces between crypto- and fiat currencies (He *et al.*, 2016). The US Treasury's Financial Crimes Enforcement Network also regulates certain crypto-currency service providers as money transmitters (Marian, 2015). Of course, transactors might still be able to find bilateral counter-parties that enable them to transfer in and out of crypto-currencies, and regulation of the exchanges would not necessarily prevent such transactions. Marian (2015) suggests that the regulatory net could be extended by co-opting legitimate merchants into implementing a sales tax on all crypto-currency transactions, with rebates to be provided to purchasers if they forego anonymity. The aim of this sales tax is to penalize crypto-currency holders that have obtained balances illegally.

One of the largest Bitcoin exchanges, Mt Gox, was hacked in 2014 and had bitcoin balances stolen, reducing trust in the currency and causing the failure of the exchange (Ali *et al.*, 2015). After the Mt Gox debacle, Jiro Aichi, the Japanese minister of finance at the time, made a case for international laws governing crypto-currencies (Knight, 2014). The problem is a familiar one from financial regulation: globally inconsistent laws could result in regulatory arbitrage, favouring some jurisdictions at the expense of others, distorting economic outcomes by prompting exchanges to domicile in low-regulation countries.

Countries currently take different approaches to taxing and regulating crypto-currencies. The Inland Revenue Service in the United States treats crypto-currencies like property for tax purposes. Wages paid in virtual currency and contracts settled in virtual currencies are both subject to taxation. Gains and losses from the sale of virtual currencies could also be taxed depending on whether it is a capital asset or not (Levin *et al.*, 2014). The Australian Tax Office treats crypto-currencies as an asset for capital gains tax purposes and does not regard crypto-currencies as a currency.<sup>49</sup> Rather, transactions implemented using crypto-currencies are seen as barter arrangements subject to the Australian goods and services tax, and wages paid in bitcoins could be subject to fringe benefit taxes. The European Union Court of Justice has declared that the exchange of fiat currency for 'bitcoin virtual currency' is exempt from value added tax (Court of Justice, 2015), essentially treating Bitcoin as another currency. The Inland Revenue Department in New Zealand apparently treats crypto-currencies like another foreign currency for tax purposes

<sup>49</sup>See <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/>, downloaded 2 August 2017.

(Vaughan, 2014), but details on the New Zealand tax treatment are reasonably scant.<sup>50</sup>

Central banks and other regulatory authorities appear to be relatively sanguine that cryptocurrencies do not pose an immediate threat to financial systems, in part because mainstream financial systems continue to predominate. See for example Reserve Bank of Australia (2014), Ali *et al.* (2014), and Federal Advisory Committee (2014). The European Central Bank's position is similar to that of other central banks (ECB, 2015). The use of virtual currencies remains limited and the European Central Bank (ECB) sees no immediate threat to the operation of payment systems, monetary policy, price stability and financial stability. The ECB acknowledges that virtual currencies have potential advantages over traditional payment systems especially for cross-border transactions. The ECB's current strategy to deal with 'virtual' currencies is to continue to monitor developments and amend the regulatory and supervisory framework in future, as needed. In most jurisdictions, anti-money laundering (AML), taxation, and terrorism issues are of more immediate concern than payment system, monetary policy or financial stability aspects of crypto-currencies (representatively, see Federal Advisory Committee 2014).

The Reserve Bank of New Zealand's regulatory focus is on systemically important banks, non-bank deposit-takers, insurers, and systemically important financial infrastructure.<sup>51</sup> The overall intent of the Reserve Bank's regulatory framework is to promote a sound and efficient financial system for New Zealand. The Reserve Bank does not regulate all non-bank schemes that provide for the storage and transfer of value. For example, the Snapper cards mentioned earlier fall outside the Reserve Bank's regulatory net, since they are small in value and the balances are thought of as a form of pre-payment rather than as deposits per se. Like Snapper, crypto-currency schemes are neither systemically important nor materially important for financial efficiency and therefore have not yet been brought into the Reserve Bank's regulatory ambit.

The Reserve Bank of New Zealand retains a monopoly on issuing NZD notes and coins that are legal tender in New Zealand.<sup>52</sup> The impact of currency substitutes has become an important issue for the Reserve Bank of New Zealand, as it develops its strategic plans for future currency

<sup>50</sup>See <http://www.ey.com/nz/en/services/tax/ey-tax-watch-edition-6-2014-crypto-currencies-a-growing-market> and <https://www2.deloitte.com/nz/en/pages/forensic-focus/articles/bitcoin-101-back-to-basics.html>, downloaded 3 August 2017.

<sup>51</sup>More details on the Reserve Bank's regulatory responsibilities can be found here: <http://www.rbnz.govt.nz/regulation-and-supervision>.

<sup>52</sup>Section 25 of the Reserve Bank Act of New Zealand, 1989: "The [Reserve] Bank shall have the sole right to issue bank notes and coins in New Zealand."

---

issuance. Work is currently under-way to assess the future demand for New Zealand fiat currency and to consider whether it would be feasible for the Reserve Bank to replace the physical currency that currently circulates with a digital alternative. Over time, analysis associated with this project will filter through into the public domain.

## 5. Conclusion

In this article we discussed crypto-currencies and described a prototypical example of how transactions are facilitated using Bitcoin, the first decentralised crypto-currency. Crypto-currencies offer some distinct features, such as quicker cross-border transactions, possibly lower transaction fees, pseudo-anonymity, and transaction irreversibility. These features help to explain the growing demand for crypto-currencies, even though they fail to satisfy many of the basic functions of money. Most crypto-currency accounts lie dormant and many of the active accounts are used only for online gambling or speculative purposes. Perceptions of anonymity have also created a demand for such currencies to facilitate illegal transactions, but the anonymity embodied in crypto-currencies has been over-stated. There have been a significant number of crypto-currency prosecutions in relation to money laundering and other crimes, illustrating that there is no guarantee of anonymity.

While crypto-currencies are growing in popularity, they currently facilitate a very small proportion of transactions. Because crypto-currencies intermediate such a small proportion of transactions, central banks do not presently view crypto-currencies as a material threat. Since crypto-currencies are not well-adapted to the provision of borrowing and lending, we also foresee an enduring role for traditional financial intermediaries.

Crypto-currencies and blockchain technology could well become an important part of global payment systems, but wide-scale adoption will depend on competition from alternative transaction technologies, and on regulation to provide users with security. Crypto-currencies will also need to address technical, scalability issues if they wish to intermediate the volume of transactions undertaken globally.

We conclude that all crypto-currencies are experimental in nature and users face material risks by transacting with them or by holding significant crypto-currency balances. Individual crypto-

currencies may be more Betamax than VHS, and more MySpace than Facebook. Even if some of the constructs are enduring, such as distributed ledgers and the use of cryptography, specific crypto-currencies may be supplanted by competing transaction technologies. We close with a Latin expression much-beloved by contract lawyers and economists alike – *caveat emptor* – buyer beware.

## References

- Adamsson, S and M Tahir (2015), *From one to many – The impact of individual's beliefs in the development of cryptocurrency*, Master's Programme in Technical Project- and Business Management, Halmstad University.
- Ali, R, J Barrdear, R Clews, and J Southgate (2014), "The economics of digital currencies," *Bank of England Quarterly Bulletin*, 54(3), 276–286, URL <https://ideas.repec.org/a/boe/qbullt/0148.html>.
- Ali, S T, D Clarke, and P McCorry (2015), "Bitcoin: Perils of an unregulated global P2P currency," in *Revised Selected Papers of the 23rd International Workshop on Security Protocols XXIII*, vol. 9379, 283–293, New York: Springer-Verlag, URL [http://dx.doi.org/10.1007/978-3-319-26096-9\\_29](http://dx.doi.org/10.1007/978-3-319-26096-9_29).
- Antonopoulos, A M (2015), *Mastering Bitcoin: Unlocking Digital Cryptocurrency*, Sebastopol, Ca: O'Reilly Media.
- Antonopoulos, A M (2016), *The Internet of Money*, Merkle Bloom LLC.
- Bank of Canada (2014a), "Decentralized e-money (Bitcoin)," *Backgrounders*, Bank of Canada, URL <http://www.bankofcanada.ca/wp-content/uploads/2014/04/Decentralize-E-Money.pdf>.
- Bank of Canada (2014b), "E-money," *Backgrounders*, Bank of Canada, URL <http://www.bankofcanada.ca/wp-content/uploads/2014/04/E-Money-Backgrounder.pdf>.
- BIS (2015), "Digital currencies," *Mimeo*, Bank for International Settlements, committee on Payments and Market Infrastructures, URL [www.bis.org/cpmi/publ/d137.pdf](http://www.bis.org/cpmi/publ/d137.pdf).

---

Böhme, R, N Christin, B Edelman, and T Moore (2015), “Bitcoin: Economics, technology, and governance,” *Journal of Economic Perspectives*, 29(2), 213–238.

Brown, R G, J Carlyle, I Grigg, and M Hearn (2016), “Corda: An introduction,” URL [https://docs.corda.net/\\_static/corda-introductory-whitepaper.pdf](https://docs.corda.net/_static/corda-introductory-whitepaper.pdf).

Burda, M and C Wyplosz (1993), *Macroeconomics: A European Text*, Oxford: Oxford University Press.

Chapman, J, R Garratt, S Hendry, A McCormack, and W McMahon (2017), “Project Jasper: Are distributed wholesale payment systems feasible yet?” in *Financial System Review*, 59–69, Bank of Canada.

Cheah, E-T and J Fry (2015), “Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin,” *Economics Letters*, 130, 32–36.

Court of Justice (2015), “The exchange of traditional currencies for units of the ‘bitcoin’ virtual currency is exempt from VAT,” *Press Release 125/15*, Court of Justice of the European Union, judgment in case C-264/14 Skatteverket v David Hedqvist, URL <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf>.

Davidson, J (2015), “No, big companies aren’t really accepting Bitcoin,” *Time Magazine*, 10 January 2015, URL <http://time.com/money/3658361/dell-microsoft-expedia-bitcoin/>.

ECB (2012), “Virtual currencies,” *Mimeo*, European Central Bank, URL <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>.

ECB (2015), “Virtual currencies – A further analysis,” *Mimeo*, European Central Bank, URL <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>.

European Banking Authority (2013), “Warning to consumers on virtual currencies,” *Mimeo EBA/WRG/2013/01*, European Banking Authority, 12 December 2013.

Extance, A (2015), “Bitcoin and beyond,” *Nature*, 526(7571), 21–3.

Eyal, I and E G Sirer (2014), “Majority is not enough: Bitcoin mining is vulnerable,” in *Financial Cryptography and Data Security*, eds. N Christin and R Safavi-Naini, vol. 8437, Berlin: Springer.



---

Federal Advisory Committee (2014), *Record of meeting*, Board of Governors, Friday, 9 May 2014, URL <https://www.federalreserve.gov/aboutthefed/fac-20140513.pdf>.

Federal Bureau of Investigation (2012), "(u) Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity," *Intelligence assessment*, Federal Bureau of Investigation.

Freixas, X and J-C Rochet (1997), *Microeconomics of Banking*, Cambridge, Mass.: The MIT Press.

Fung, B, M Molico, and G Stuber (2014), "Electronic money and payments: Recent developments and issues," *Discussion Paper 2014-2*, Bank of Canada, URL <http://www.bankofcanada.ca/wp-content/uploads/2014/04/dp2014-2.pdf>.

Glaser, F, K Zimmermann, M Haferkorn, M C Weber, and M Siering (2014), "Bitcoin – asset or currency? Revealing users' hidden intentions," in *Proceedings of the European Conference on Information Systems (ECIS)*, Tel Aviv Israel: Association for Information Systems, URL <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1131&context=ecis2014>.

Goldman Sachs (2014), "All about Bitcoin," *Global Macro Research Top of Mind 21*, Goldman Sachs, 11 March.

He, D, K F Habermeier, R B Leckow, V Haksar, Y Almeida, M Kashima, N Kyriakos-Saad, H Oura, T S Sedik, N Stetsenko, and C V Yepes (2016), "Virtual currencies and beyond: Initial considerations," *IMF Staff Discussion Notes 16/3*, International Monetary Fund, URL <https://ideas.repec.org/p/imf/imfsdn/16-3.html>.

Hendrickson, J R, T L Hogan, and W J Luther (2016), "The political economy of Bitcoin," *Economic Inquiry*, 54(2), 925–939.

Jevons, W S (1896), *Money and the Mechanism of Exchange*, New York: D. Appleton and Company.

Johnson, G and L Pomorski (2014), "Briefing on digital currencies," *Briefing to the Senate of Canada*, Bank of Canada, URL [http://www.bankofcanada.ca/wp-content/uploads/2014/04/Senate\\_statement.pdf](http://www.bankofcanada.ca/wp-content/uploads/2014/04/Senate_statement.pdf).

- 
- Kloc, J (2014), "Bitcoin makes the jump to brick-and-mortar in Cleveland," *Newsweek*, 162(22), 6 June 2014.
- Knight, S (2014), "Japan says any Bitcoin regulation should be international," *Reuters*, 27 February 2014, URL <http://www.reuters.com/article/us-bitcoin-mtgox-japan-idUSBREA1Q0I520140227>.
- Kocherlakota, N R (1998), "Money is memory," *Journal of Economic Theory*, 81(2), 232–251.
- Kocherlakota, N R (2000), "Creating business cycles through credit constraints," *Federal Reserve Bank of Minneapolis Quarterly Review*, 24(3), 2–10.
- Kocherlakota, N R (2002), "Money: What's the question and why should we care about the answer," *American Economic Review: Papers and Proceedings*, 92(2), 58–61.
- Koepl, T and J Kronick (2017), "Blockchain technology – what's in store for Canada's economy and financial markets," *Commentary 468*, C.D. Howe Institute.
- Levin, R B, A A O'Brien, and S A Osterman (2014), "Dread pirate Roberts, Byzantine generals, and federal regulation of Bitcoin," *Journal of Taxation & Regulation of Financial Institutions*, 27(4), 5–19.
- Lipsey, R G (1963), *An Introduction to Positive Economics*, London: Weidenfeld and Nicolson, fourth impression June 1965.
- Marian, O Y (2015), "A conceptual framework for the regulation of cryptocurrencies," *The University of Chicago Law Review*, 82(1), 53–68.
- McBride, N (2015), "Payments and the concept of legal tender," *Reserve Bank of New Zealand Bulletin*, 78(6), 3–7, URL <http://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Bulletins/2015/2015sep78-6.pdf>.
- Meiklejohn, S, M Pomarole, G Jordan, K Levchenko, D McCoy, G Voelker, and S Savage (2016), "A fistful of bitcoins: Characterizing payments among men with no names," *Communications of the ACM*, 59(4), 86–93.
- Nakamoto, S (2008), "Bitcoin: A peer-to-peer electronic cash system," *Mimeo*, Bitcoin.org, URL <https://bitcoin.org/bitcoin.pdf>.

- 
- Narayanan, A, J Bonneau, E Felten, A Miller, and S Goldfeder (2016), *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton, NJ: Princeton University Press.
- Peters, G W, A Chapelle, and E Panayi (2015), "Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: An operational risk perspective," *Journal of Banking Regulation*, 17(4), 239–272.
- Reserve Bank of Australia (2014), "Submission to the inquiry into digital currency: Senate Economics References Committee," November 2014, URL [http://www.aph.gov.au/Parliamentary\\_Business/Committees/Senate/Economics/Digital\\_currency/Submissions](http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Digital_currency/Submissions).
- SEC (2013), "Ponzi schemes using virtual currencies," *Investor Alert 153 (7/13)*, United States Securities and Exchange Commission.
- Szczepáński, M (2014), "Bitcoin: Market, economics and regulation," *Tech. Rep. 11/04/2014*, European Parliamentary Research Service.
- Tasca, P (2015), "Digital currencies: Principles, trends, opportunities, and risks," *Research working paper*, Ecurex, URL <http://ssrn.com/abstract=2657598>.
- Trautman, L (2014), "Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?" *Richmond Journal of Law & Technology*, 20(4), 1–109, URL <http://jolt.richmond.edu/v20i4/article13.pdf>.
- UK Government Office for Science (2016), "Distributed ledger technology: Beyond block chain," URL [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/492972/gs-16-1-distributed-ledger-technology.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf).
- Vaughan, G (2014), "IRD says bitcoin should be treated in the same manner as foreign currencies for tax purposes," Accessed 17 May 2017, URL <http://www.interest.co.nz/personal-finance/71048/ird-says-bitcoin-should-be-treated-same-manner-foreign-currencies-tax>.
- Velde, F R (2013), "Bitcoin: A primer," *Chicago Fed Letter 317*, Federal Reserve Bank of Chicago.
- Vigna, P and M J Casey (2015), *The Age of Cryptocurrency*, NY: St. Martin's Press.

- Wang, S (2016), "Examining the effects of dollarization on Ecuador," *Mimeo*, Council on Hemispheric Affairs, URL [http://www.coha.org/wp-content/uploads/2016/07/Sam-Wang-Ecuador-Dollar\\_Final.pdf](http://www.coha.org/wp-content/uploads/2016/07/Sam-Wang-Ecuador-Dollar_Final.pdf).
- Weber, W E (2016), "A Bitcoin standard: Lessons from the gold standard," *Staff Working Paper 2016-14*, Bank of Canada.
- White, L (2014), "Defending dollarization in Ecuador," *Mimeo*, Alt-M.org, 4 December 2014, URL <https://www.alt-m.org/2014/12/04/defending-dollarization-in-ecuador/>.
- White, L H (2015), "The market for cryptocurrencies," *Cato Journal*, 35(2), 383–402.
- Williamson, S and R Wright (2010), "New monetarist economics: Methods," *Federal Reserve Bank of St Louis Review*, 92(4), 265–302.
- Williamson, S and R Wright (2011), "New monetarist economics: Models," in *Handbook of Monetary Economics 3A*, eds. B M Friedman and M Woodford, 25–96, San Diego, CA: Elsevier.
- Yermack, D (2013), "Is Bitcoin a real currency? An economic appraisal," *Working Paper 19747*, National Bureau of Economic Research.