Cryptocurrencies, institutions and trust

Prepared for:
Australian Centre for Financial Studies

Authors:
Dr John Vaz
Dr Kym Brown

May 2018
FUNDING AUSTRALIA’S FUTURE

The Australian Centre for Financial Studies (ACFS) instigated the Funding Australia’s Future project in 2012 to understand the changing dynamics of the Australian financial system, and how these will affect future economic growth.

In an economy which has enjoyed 26 years of consecutive economic growth and showed a resilience through the Global Financial Crisis which was the envy of many nations, the financial sector has played an important role. The past decade, however, has been one of significant change. The growth of the superannuation sector, the impact of the GFC, and the subsequent wave of global re-regulation have had a profound effect on patterns of financing, financial sector structure, and attitudes towards financial sector regulation.


This paper is one of four in Stage Four which explore the growth of fintech, its implications on the structure of the financial sector and the value it can produce for the broader Australian community through increased competition in the financial services sector:

- A framework for understanding fintech and its value, David Link (Verrency) and Professor Rodney Maddock (Adjunct, Monash Business School)
- International competition policy and regulation of financial services – Lessons for Australian fintech, Deborah Cope (PIRAC Economics)
- Innovation and fintech policy: Post-Murray developments, Professor Kevin Davis, (ACFS)
- Cryptocurrencies, institutions and trust, Dr John Vaz and Dr Kym Brown (Monash Business School)

All Funding Australia’s Future research papers can be accessed online at https://australiancentre.com.au/projects/faf/
NOTES ON THE AUTHORS

David Link: David Link is Chair of Verrency and an advisor and board member of firms in the global fintech space, David is a retired Managing Director of Accenture, where he held global practice leadership roles in Asia Pacific, Australia, Korea, France, and Benelux, primarily focused on financial services.

Professor Rodney Maddock: Rodney Maddock is a Professor at the Australian Centre for Financial Studies. Prior to this he was a senior executive at the Commonwealth Bank of Australia. He has a distinguished academic record with extensive academic publications and experience working in a number of countries, and his ongoing research is in the areas of Finance and Australian economic development.

Deborah Cope: Deborah Cope is Principal at PIRAC Economics. She has extensive experience in analysing and reforming governments’ economic, social and environmental policies, and has also been involved in developing and implementing competition policy, improving the effectiveness and efficiency of regulation and regulators, and designing and implementing strategies for competitive neutrality between government and private businesses.

Professor Kevin Davis: Kevin Davis is Professor of Finance at the University of Melbourne and Research Director of the Australian Centre for Financial Studies. His primary research interests are financial regulation, financial institutions and markets, financial innovation and corporate finance. He is the Deputy Chair of SIRCA, a member of the Australian Competition Tribunal, and has undertaken an extensive range of consulting assignments for financial institutions, business and government.

Dr John Vaz: John Vaz is a Senior Lecturer at Monash University. Prior to this, John held chief executive and senior management roles from start-ups to large enterprises in the Tech sector across many countries. John has done business and worked in many countries including Australia, SE Asia and the UK. John's research interests follow his PhD in Finance in how the macro-economy impacts financial markets, financial institutions and investor behaviour.

Dr Kym Brown: Kym Brown is a Senior Lecturer in the Department of Banking and Finance at Monash University. She teaches across a number of banking and international finance related subjects. She has research interests in banking, Islamic finance, Chinese banking, ethics in cryptocurrencies and inequality.
CONTENTS

Abstract .............................................................................................................................................. 6

Acknowledgement .............................................................................................................................. 6

1. INTRODUCTION .......................................................................................................................... 7

1.1 What is Trust? ............................................................................................................................... 8

1.2 Trust and Money ........................................................................................................................... 8

2. Fundamental cryptocurrency ingredients .................................................................................... 11

3 The Promises of Cryptocurrencies ............................................................................................... 14

3.1 Security and Protection from Fraud .......................................................................................... 14

3.2 Privacy and Confidentiality ........................................................................................................ 15

3.3 Payment and Settlement Speeds ............................................................................................... 15

3.4 Efficiency and Low Transaction Costs ..................................................................................... 16

3.5 Disintermediation: Eliminate Intermediaries ............................................................................. 18

3.6 Universality of Access: Anyone Can Access ............................................................................. 18

3.7 Borderless and Frictionless ........................................................................................................ 19

3.8 Debasement Protection .............................................................................................................. 20

4. Money, Trust and Institutions .................................................................................................... 20

4.1 The Evolution of Money .............................................................................................................. 20

4.2 Emergence of Digital Currency ................................................................................................. 21

4.3 Trust ........................................................................................................................................... 22

4.4 Semiotics of Cryptocurrencies ................................................................................................. 23

4.5 Institutions and Trust ................................................................................................................. 24
5. Cryptocurrency, institutions and trust .............................................................. 26
5.1 Distributed Ledger Technology as an Alternative to Trust .......................... 26
5.2 Elimination of Intermediaries ....................................................................... 26
5.3 Regulation and Trust ..................................................................................... 27
5.4 Governance and Ethics ................................................................................. 28
5.5 Banking with Cryptocurrency ...................................................................... 29

6. Conclusion ........................................................................................................... 30

REFERENCES ......................................................................................................... 33

APPENDIX ................................................................................................................ 37
ABSTRACT

Specific (non-government issued) cryptocurrencies that are aspired to become widely accepted forms of digital money will need to expand their acceptance beyond the small “tech-eco-systems” into broader acceptance. This can be achieved with a supportive operational environment of trust and confidence. Can the information technology underpinning the design and production of cryptocurrencies, such as blockchain, achieve the necessary trust and confidence without the involvement of financial institutions and government? Participation and rule-setting by financial institutions and governments has historically engendered trust in traditional “fiat money” and bank deposits. We argue that the production of trust for these new forms of money will require the participation of intermediary institutions and much greater regulation, despite being the object of elimination by cryptocurrency creators.

ACKNOWLEDGEMENT

We would sincerely like to acknowledge contributions by Kevin Davis and helpful comments by Christine Brown, John Watson, Jonathan Hatch, Mustafa Yuksel and David Link. Additionally we would like to acknowledge the support and advice from the ACFS Steering Committee on Funding Australia’s Future: Fintech.
1. INTRODUCTION

A vast number of cryptocurrencies and digital tokens representing cryptocurrencies have rapidly emerged following the introduction of Bitcoin in 2009. Coinciding with the financial crisis of 2008, which shook faith in the traditional financial and monetary structures, the emergence and design of these new privately created “currencies” also referred to as tokens reflects both innovations in technology and distrust of financial institutions and government by their creators. Some innovators claim to be motivated by non-profit objectives, but creation and issuance of these “virtual claims” involves seigniorage or issuance profits/revenue, akin to those otherwise accruing to governments and banks charged with the management of national monetary systems.

Nakomoto (2008), the anonymous founder of bitcoin and developer of blockchain technology, argued that a cryptocurrency built on blockchain information technology would eliminate the need for explicit trust provided by financial institutions and government involvement and make those institutions redundant in financial transactions. This paper examines that claim, and thus the potential for privately created cryptocurrencies to assume a role as money. Although cryptocurrencies can take a number of different forms or functionality, particularly when issued as a token¹ which may lead to rights of promised outcomes or investments, our focus is solely on those cryptocurrencies that aim to function as a digital form of currency.²

We first consider what is meant by trust and how it can be engendered within a financial system. Then, we outline the key ingredients in cryptocurrencies to set the basis for identifying possible ways in which trust might be created. This is followed by an outline of the main advantages claimed for cryptocurrencies as alternatives to traditional currencies and money. Then, we briefly examine how trust in traditional money has evolved over time before assessing whether the claimed benefits and characteristics of cryptocurrencies can create sufficient trust to allow for widespread acceptance of them either as a means of exchange or as valuable financial assets.

¹ All tokens are generally not created with the objective of becoming a widely held and exchanged form of money as a competitor (or eventual replacement) for the conventional monetary system.
² Regulators such as ASIC in Australia or the SEC in the United States have expanded regulations over concerns to protect consumers using digital currency exchanges (DCE) using initial coin offerings (ICOs) as capital raising mechanisms which are outside the traditional methods and legal entities. See for example ASIC (2018) or SEC (2018). Investment type schemes using cryptocurrencies may initially in the pre-emptive stage of capital raisings issue an ERC-20 token (based on the Ethereum network), which is then converted to the set-named token once enough capital is raised or a certain date is reached. Some cryptocurrencies operate as part of a platform of services, where the White Paper outlining the expectations and operational aspects suggest the possibility of currency functionality. The definition of a cryptocurrency is used loosely and does not necessarily mean an alternative form of currency.
1.1 What is Trust?

Trust (in an economic setting) can be defined as expectations held by a party engaging in a transaction with a counterparty. Trust by both parties implies an expectation of mutual benefit and facilitates economic exchange. Traditionally trust has been enabled via the prevailing culture and established norms. Trust can be characterised as process-based (reflecting experience), character-based (referential to knowledge regarding the counterparty) or institutionally-based (involving societal structures like intermediaries and regulations) (Zucker, 1986). While the above definition focuses upon engagement in transactions, trust is also relevant for willingness to hold the item received in the transaction for some period of time without fear of its suffering a loss of value.

1.2 Trust and Money

Widespread trust in government issued fiat money and related forms of financial claims providing near perfect substitutes for various features of fiat money, such as bank deposits, have facilitated economic growth and welfare. This has come about through institutional settings involved in sovereign government issuance of national fiat currency and control of bank deposit creation, via the role of central banks and regulation of financial institutions.³

**Fiat Money:** A fiat currency is one that has no intrinsic value but its value is generally established by government authority or regulation that enforces its usage in a particular jurisdiction or domain for exchanges of goods and services as well as financial transactions. Modern fiat currencies are usually manifested as some physical artefact that is stamped or enumerated with the face value usually paper notes or coins. Ownership does not give the holder a claim on any “real” assets backing the currency. There is, in principle, no reason that fiat money could not take the form of a digital claim on an account at the Central Bank – and bank “cash” reserves generally take this form (as well as holding notes and coins for transactions with customers who are unable to obtain such accounts).

The issuer of fiat money benefits from “seigniorage” which is the net gain from the real resources received in exchange for newly issued currency in excess of its low cost of physical production. People accept and hold the currency because others are also willing to do so, enabling its use as a medium of exchange, and unit of account (with prices being quoted in terms of the currency unit). It is also a store of value, unless excessive issuance causes (hyper) inflation and debases its value. The risk that governments will do so (via, for example, budget deficit financing of government

³ There are, of course, groups of scholars who would point to historical eras of “free banking” in which private banks issued bank notes and deposit money, relying on self-regulation to maintain trust and acceptability of those financial claims.
expenditures), to profit from the seigniorage involved, is one factor leading to many cryptocurrency advocates to believe that a privately issued currency with inbuilt limits on its future issuance is desirable. Banks provide deposits which are virtually perfect substitutes for fiat currency, by virtue of exchangeability at a fixed price of unity, and acceptance as a medium of exchange.

These institutional settings have involved governments enforcing fiat currency as legal tender in transactions (including for the payment of tax) and ensuring authenticity (preventing counterfeiting) so that citizens have trust and confidence in the fiat currency. Regulators such as Augustin Carstens from the Bank for International Settlements has stated that “credible money requires institutional backup” (Carstens, 2018).

The physical artefacts (notes and coins) of a fiat currency are useful in face to face transactions, but less convenient for large scale transaction and those where the parties are separated by geography. Banks have provided virtually perfect substitutes for fiat currency in the form of deposits with a value fixed at one-to-one with the fiat currency. Claims on those could be used to achieve an exchange with a third party via the banking system enabling a transfer of value from the deposit account of the payer to a deposit account of the payee at their preferred bank. That could be done using a physical instrument (cheque) or use of electronic transfers to initiate the process. Trust in bank deposits as “money” has been engendered by government regulation of bank activities, and prudential behaviour by bankers’ conscious of their dependence on maintenance of reputation.

A fundamental difference between money in the form of bank deposits and physical fiat currency is that the former is a liability of some entity (the bank) which holds assets to “back” that liability, whereas the latter is issued by a Government or Central Bank and a liability on their part.4

Cryptocurrencies however have no liability as the holder has no claim on an “issuer” of the digital token. “Trust” in a cryptocurrency then becomes a matter of trust in the credibility of the process through which the creation, ownership recording, and exchange arrangements occur, rather than trust in some individual or entity. Thus whether the claimed benefits of cryptocurrencies are widely believed to be real, and ultimately forthcoming, becomes an important component in engendering trust and widespread acceptance.

As well as acceptability in exchange, willingness of individuals to maintain holdings of financial claims in the form of fiat money or bank deposits depends upon trust, in the form of confidence that the purchasing power will be relatively stable and not be eroded over time. Government

---

4 This was changed with the movement from making the US dollar exchangeable for gold in 1971.
self-imposed limits on budget deficit financing and monetary policy controls limiting fiat currency and bank deposit growth relative to real economic growth are fundamental to achieving this trust. Cryptocurrency advocates see the lack of management of deficits funded through monetization that can erode the store of value as a key failure and thus a motivator to eliminate government and bank involvement in managing the money supply.

This “store of value” element of trust also poses a contemporary challenge for widespread eventual acceptance as “money” of cryptocurrencies such as Bitcoin which have experienced marked fluctuations in price (in terms of the fiat currency and hence also in terms of real purchasing power). Whether current perceptions of a cryptocurrency as a speculative asset are compatible with it eventually becoming widely accepted as a form of money with a stable exchange value in terms of real resources is unclear. Although advocates point to the inbuilt limits on growth of the amount on issue as a benefit to achieving price stability, speculative shifts in demand lead to significant price variability even with a stable supply.

If cryptocurrencies are to be widely accepted as money it requires more than just an improvement in the technology enabling performance of the functions of money viz: a medium of exchange, store of value and a unit of account. For cryptocurrencies to be successful as a form of money they need to establish an environment of trust and confidence, which we argue will involve some form of institutions and regulation. Whether a multiple number of cryptocurrencies can become viable competitors with, or replace, fiat money remains to be seen. More generally, what characteristics of a cryptocurrency will engender sufficient trust to lead to it becoming a “financial asset” traded and held by significant portions of the population? Which among the multiple types might succeed and which might fail?

Some commentators have questioned whether a version of Gresham’s Law (“bad money drives out good”) would apply in the case of cryptocurrencies, but it is not clear that this is relevant in its original form. However, if the costs of transacting via a crypto were less than via fiat based methods, it is feasible that even if not held other than momentarily (before exchange into other stores of value) a crypto could become a popular means of exchange even if not a unit of account or store of value. This would require some level of integration with traditional bank payments systems, and consequent interaction with regulators.

Gresham’s Law

This is generally stated in the form “Bad money drives out good”, and was originally developed in the context of metal based currencies where the physical coins had a specified content of gold or
Individuals with knowledge of the actual content could be expected to proffer bad money in a transaction with an unsuspecting counterparty, and hold good money as a store of wealth, principally due to its better commodity value. Widespread use of such practices would lead to unwillingness of counterparties (who eventually discover that they have been “short-changed”) to accept that form of money for transactions, thereby causing it to lose its monetary role as a means of exchange.

2. FUNDAMENTAL CRYPTOCURRENCY INGREDIENTS

Cryptocurrencies are a form of digital coin token that is privately issued and typically marketed as a “currency”. They use sophisticated cryptography to securely manage the creation, transfer and ownership of the cryptocurrency as well as to provide privacy (anonymity) in relation to holdings and uses of that currency by users. Digital wallets, similar to bank accounts with fiat currencies, accessed by public and private keys, are required before you can transact. The practical implementation of cryptocurrencies was only possible due to the availability of powerful cheaper portable computers, the internet and smartphones.

Public keys are the alphanumeric identities which are used to associate each digital token with some anonymous “owner”.

Private keys are the (generally 64 digit) code, known only to the “owner” which is required to be entered by the owner to effect a transfer of ownership to another party. Loss of the private key means loss of digital tokens (such as would occur by burning of bank notes).

Bitcoin was created shortly after a paper published under the nom de plume Satoshi Nakamoto in 2008 at the crux of the financial crisis. Nakamoto claimed that there was a problem with trust-based payment models that relied on financial institutions or other intermediaries. The author proposed an alternative peer-to-peer mechanism for electronic payment transactions but using existing available technology in an innovative way. Nakamoto (2008) proposed an electronic payment system that would use cryptography and complex computer algorithms in a distributed network of computers to operate a distributed ledger in the form of a blockchain eliminating the need for intermediaries. The Bitcoin ecosystem was created in 2009 using this proposal.

The underlying technology, known as blockchain, has experienced very quick adoption amongst segments of the global population and has been followed by many other similar
innovations. The number of cryptocurrencies has rapidly grown since 2013 to over 1,700 as of May 2018. This may partly reflect competition for discovery of the best technology and design in the hope, amongst those distrustful of government, of becoming an alternative to fiat currencies. Advocates also claim that cryptocurrencies eliminate the need for trusted parties or intermediary institutions by enabling peer-to-peer transactions and are therefore better and fairer than fiat currencies. However, it must also be noted that promoters profit from seigniorage from initial holdings acquired in the development process, or value received in an initial coin offering (ICO) without incurring any personal liability, and obtain subsequent capital gains should the cryptocurrency value appreciate.

There are two fundamental features of cryptocurrencies. One is the use of distributed ledger technology (DLT) which is a type of database, which potentially has widespread value in a range of areas independently of its original link to cryptocurrencies. The second is that issuance, ownership recording, and cryptographically securing and processing transactions using a decentralised autonomous organization (DAO) implemented on a distributed ledger often on blockchain(s).⁵

Trust, and thus willingness to use and hold the cryptocurrency, depends on trust in the operational features of the DLT and DAO and consequences for the safety and value of the digital tokens involved. Whether trust can be established which is equivalent to that associated with providers of traditional forms of money (financial institutions such as banks and government) is thus important for widespread acceptance. Looking forward, the potential for Central Banks to introduce Central Bank Digital Currencies (CBDCs) providing an alternative to physical currency and privately issued digital tokens potentially serving as money should also be noted. Although we do not consider CBDCs in detail here, they will hold more trust given their governmental backing which can be considered as an institutional mechanism of trust (Zucker, 1986).⁶

---

**A Decentralized Autonomous Organization (DAO)** refers to the rules used to create and record secure financial transactions on a blockchain. Once the programming software has been developed to allow the creation of digital tokens over time according to particular pre-defined rules, and put into operation, there is (in principle) not further human involvement or control of the process.

---

⁵ Note the DAO in this case refers to the rules to secure the records on the blockchain, not to be confused with investor-directed venture capital firm that was hacked in 2016.

⁶ Central banks are open to implementing a digital cryptocurrency form of money in the future (see for instance Lowe (2018) in regards to Australia).
A **distributed ledger** is based on the concept of maintaining multiple copies of the same records at different physical locations. These records can be sighted by all who maintain them and are verified and updated by consensus.

A **blockchain** is a chain of encrypted and digitally encoded groups of transaction records (blocks) that are validated and updated on a consensus basis by all who participate in the maintenance of the system. Each block is added to the front of the previous block in a time stamped sequence and cryptographically encoded so it is tied to its preceding blocks in a chain forever.

In Bitcoin and similar blockchains, transactions are processed by nodes in the network undertaking and solving complex problems and cryptographic processing (**proof of work or POW**) that take great effort to solve but are easy to verify.\(^7\) This is a deterrent as fraudulent transactions require enormous effort to undertake POW faster than all others, but must also make changes on a majority of computers before the next block is created. The result is that hacking is theoretically more costly than proper participation as a node in the network due to the resources involved and energy costs. Other schemes require participants to make initial investments known as **proof of stake (POS)** in lieu of POW, so a node participant can lose part or all of their stake if unacceptable transactions are processed. Delegated POS based consensus are more efficient in that they consume less power and are faster and are becoming more popular.

Since Bitcoin emerged as the dominant player in the cryptocurrency market, a plethora of alternative cryptocurrencies or ‘altcoins’ have emerged.\(^8\) These have typically also claimed to be motivated to provide similar or greater benefits such as: greater effectiveness through elimination of the intermediaries (smaller size transactions and to transact peer-to-peer); greater efficiency (cost of transactions); social justice (accessibility and availability to individuals); fairness (protection from debasement) and greater privacy and security (pseudonymity due to encryption) (Rosic, 2017).

Most cryptocurrencies utilise some form of distributed ledger implementation, mostly based on blockchain or variations of technology enabling DAOs - for example some use directed acyclic graph technology. All utilise cryptography, a distributed network and various consensus mechanisms parties (which may involve proof of work or proof of stake) to eliminate the need for intermediary trusted. There are many implementations of cryptocurrencies with a variety of features and characteristics, but all follow or build on the distributed ledger concepts

---

\(^7\) The game of Sudoku can be very difficult to solve but can be verified very quickly and easily.

\(^8\) The price of Bitcoin has been volatile. As at the 1\(^{st}\) January 2017 Bitcoin was priced at USD$997.69 per bitcoin but by the 19\(^{th}\) December 2017 it was some USD$18,809.52 and by the 5\(^{th}\) February 2018 it dropped to USD $6,914.26 (www.coindesk.com/price).
established by Bitcoin and its blockchain. Most make similar claims of social benefits from their existence and use relative to traditional currencies.

3 THE PROMISES OF CRYPTOCURRENCIES

3.1 Security and Protection from Fraud

Cryptocurrencies aim to provide security and protection firstly by ensuring that only valid transactions are processed on a consensual basis involving multiple independent parties. Therefore, users can transact with confidence that any transactions allowed onto the distributed ledger can be trusted as involving a receipt of a legitimately owned token from its previous owner. Secondly, transactions once recorded cannot be altered as they will be discovered and stopped therefore managing the double spend problem.

This also means that transactions are irreversible and cannot be corrected or adjusted (or that this could only be done via the creation of a new opposite transaction that both parties are willing to execute). The transactions are cryptographically stored on a distributed ledger in a blockchain or other immutable manner so that they are claimed to be virtually impossible to be hacked (causing either destruction of existing tokens or illegal transfer to third parties). This is because there is no central point of failure or hacking as there are with intermediaries, although this claim is disputed by some newer cryptocurrencies claiming better security as it depends on the implementation. We discuss the security of the blockchain in more detail in the Appendix.

The **Double spend problem** is the possibility that an owner of a token could undertake a transaction to purchase some item involving transfer of the token ownership to the counterparty, and then undertake another transaction with a third party involving transfer of ownership of the same token. If there are lags in the recording of the initial ownership transfer, then a duplicitous individual could engage in a “double spend” of the same token, creating either loss for one of the counterparties when the second transaction was attempted to be registered, or complications for the ledger process. Because the identity of the holder of the token is not known (other than by a public key), obtaining restitutions is highly problematic. Because the token is the liability of no person or entity, there is no issuer against whom recompense could be sought.

To some extent, the double spend problem is similar to the situation where an individual writes multiple cheques on a bank deposit account which has insufficient credit to honour those cheques.
3.2 Privacy and Confidentiality

Digital wallets controlled by private digital keys and public keys (pseudonymous) are argued to be secure and private. Thus, the transactor is anonymous, although a pattern of transactions involving the same public key may generate information enabling the identity of the transactor to be discovered. Others claim to provide total anonymity.\(^9\) Some such as Monero make total anonymity a major selling point offering even higher levels of protection by giving each transaction a unique key rendering them anonymous.\(^{10}\)

This privacy is a benefit for masking activity, but also creates a social problem as it creates an ability to conduct untraceable and anonymous transactions, facilitating fraudulent and illegal behavior. Any losses incurred by users due to improper conduct are also not reversible and therefore consumers, in the absence of financial institutions as intermediaries are unlikely to hold widespread trust. This is exacerbated by the fact that cryptocurrency transactions are not reversible without mutual consent by unidentifiable counterparties.

3.3 Payment and Settlement Speeds

Cryptocurrency advocates argue that it avoids reliance on cumbersome traditional systems that may require multiple layers of intermediation between and within trusted parties (banks). They also claim that parties can transact directly and achieve greater speed in transactions, reducing time from days to seconds depending on cryptocurrency. Nevertheless, throughput capabilities of cryptocurrencies (with certainty of transaction authentication and consensus) vary from seconds to an hour. Payment systems in traditional intermediary systems vary greatly also depending on the types of transfers or payments involved. Credit and debit card electronic payment systems achieve clearing of around 100,000 transfers per second (Visa, 2017), versus days for international bank transfers or paper based cheque transactions.

The effectiveness of cryptocurrencies with respect to throughput of transactions are a major problem in establishing confidence. The principle reason for different (and unproven) transaction throughput is the need to achieve consensus in a distributed ledger, preventing the double spend problem and securing the network from hacking. Schemes for consensus mechanisms such as proof of work (POW) slow the throughput and this is an area that is in a technical race to find the best way of achieving consensus. Blockchain based cryptocurrencies

---

\(^9\) The most well-known cryptocurrency, Bitcoin, whilst enormously popular as a speculative investment also enjoys a reputation as a very private place to transact without the disclosure of identity and ownership but is also opaque to government or regulatory authorities. Bitcoin as do some others have suffered from a poor reputation as a place to launder or hide money from government due to its excellent cryptographic properties that keep transactions anonymous (see for instance Meiklejohn et. al, 2016).

\(^{10}\) https://getmonero.org/
process far less than 100 transactions per second, as at the start of 2018, with the dominant cryptocurrency Bitcoin only able to process around 10 transactions a second. Some altcoins such as IOTA and Ripple claim very high transaction capability but are completely unproven at the scale of existing electronic payments systems, although new implementations such as EOS are emerging rapidly.

Recent moves to improve the transaction completion speeds have seen the introduction of modifications to the network by augmentation, such as “segregated witness” approaches on the bitcoin blockchain to allow faster processing of small transactions. However, this has highlighted a major problem from a governance perspective due to the need to have consensus on any changes to the underlying (open source) software/cryptography. Disagreement about such changes has often resulted in the creation of new cryptocurrencies (for example Bitcoin Cash). However all cryptocurrencies have recognised transaction throughput as a key issue, with IOTA and Ripple claiming to have achieved credit card type volumes. Proposals such as Directed Acyclic Graph (e.g. Tangle (IOTA) and Hashgraph), graphene block-chain and other proposals are all competing to achieve better throughput than even fiat currency based systems.

3.4 Efficiency and Low Transaction Costs

Nakamoto (2008) in founding Bitcoin asserted that:

“The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services.”

Thus, a key benefit advocated is the ability to transact more effectively for smaller transactions benefiting from the elimination of intermediaries and thus reducing transaction costs to a minimum (Richter, Kraus and Bouncken, 2015). The cost of transacting in cryptocurrencies is promoted as very low or near costless (Henderson, 2014), and for the transactor this may appear to be the case since there are no fees levied by third parties or transactions costs (other than being required to have internet access).

This is arguable, since the process of verification of transactions and maintenance and updating of the distributed ledger requires costly activities by participants in the system for which they require rewards. The nature of cryptocurrency design is that those rewards are

11 https://blockchain.info/charts/transactions-per-second?timespan=1year
12 Segregated witness is a proposal to change the blockchain structure so that signature data is handled off the blockchain to free up capacity for more transactions
provided by the creation of new tokens which are awarded to some of those participants according to some rule. Implicitly, the creation of new tokens implies a potential decline in the value of existing tokens, unless demand for them has increased, imposing a cost on existing holders rather than a cost levied on the actual transactors.

Cryptocurrencies claim that because they use the latest technology based on the internet, they are inherently more adaptable, efficient and that transaction costs are very low. Thus they are fairer as they can be used in smaller transactions more effectively. Furthermore, they assert that their costs can scale much more easily due to the nature of technology used compared to existing intermediaries. They claim intermediaries can charge excessively due to their privileged position of dominance and require hierarchical bureaucratic organisational structures and related systems that do not scale well and are slow to respond.

Moreover, one of the major limitations of the cryptocurrency environment is that those facilitating transactions are often incentivized on a transaction or block basis. In the case of Bitcoin a reward is provided per block (of transactions), and a fee offered and set by transactors, so that the highest paying transactions typically get processed first and smaller transactions are in fact delayed. Whilst the schemes vary, many are not clear. The promise of negligible cost of transactions with cryptocurrencies has not been realised yet, particularly in Bitcoin and those using similar blockchain consensus approaches. This also has an effect on those willing to perform transaction processing and therefore doubts on the consistency and reliable availability of transaction processing capacity and throughput.

There are also concerns about their energy usage (depending on mechanism) in processing transactions arising from the replacing intermediaries with DAO distributed ledgers and consensus mechanisms. For example, using analysis from the digiconomist.net\(^\text{13}\), Visa can process over 400,000 transactions for the energy usage for one Bitcoin transaction. This is because with Bitcoin, nodes compete for payment by solving puzzles (POW) during block creation and transaction processing and the process of reaching consensus. This is in addition to the cost of producing and acquiring specialised computer hardware that is needed for the purpose, in a massively duplicated environment that is costly (i.e. the distributed ledger on many computers). Whilst other cryptocurrency models may be better, they all require expensive redundant processing as that is the nature of operating a consensus based distributed ledger as an alternative to intermediation.

\(^\text{13}\) https://digiconomist.net/bitcoin-energy-consumption
The marginal efficiency gains of cryptocurrencies is disputable and the uncertainty and variability in transaction costs do not engender trust and confidence in the process for mainstream usage.

3.5 Disintermediation: Eliminate Intermediaries

Nakamoto (2008) suggested inherent weaknesses in the current system of a trust based model and reliance on intermediation. Bitcoin and its blockchain mechanism claim to address these weaknesses by eliminating the need for financial institutions to function as trusted parties, to enable electronic commerce to succeed and be fairer (Nakamoto, 2008).

The role of intermediary financial institutions as trusted parties to facilitate financial transactions are claimed to be an unnecessary costly construct that can be replaced by technology. Cryptocurrency supporters claim that financial institutions act solely in their own interests and that of their shareholders and do not serve the wider interests of the wider economy (Knight, 2017). In addition financial institutions have unfettered power to transfer wealth from the community at large by charging unreasonable fees for their services and new (non-productive) financial products. Banks in particular, can earn almost free seignorage profits as they have the ability to create money simply by lending more, expanding the money supply and eroding purchasing power and thus the wealth of the general population. Thus financial institutions have unfairly increased their share of the economy through lending, whilst providing less value in facilitating transactions in the economy (Werner, 2014). It is claimed that operation of DAOs using distributed ledger technology such as blockchain makes these institutions redundant and is fairer.

3.6 Universality of Access: Anyone Can Access

Cryptocurrencies are cited by supporters as being more democratic and fair as they enable anyone with a smart phone to transact on a peer-to-peer basis and they also claim the participation in their DAO is equitable with access through open software. They promote the idea that cryptocurrencies such as Bitcoin provide for low cost and almost universal access for all levels of society and therefore are beneficial to developing countries (Dale, 2017). They also claim that they provide for a fairer world and can assist developing nations provide their citizens with access to transact directly on a peer-to-peer basis globally without intermediaries. It has been suggested that cryptocurrency usage on a mobile phone is equivalent to putting a bank account and transaction capabilities in the hands of all (Mougayar, 2015). Some
cryptocurrencies advertise that they empower each holder of the cryptocurrency to be able to act as their own bank.\textsuperscript{14}

Cryptocurrencies require a much more sophisticated setting requiring sound internet infrastructure, and computing resources namely capital. In practice we find that the claims of universality of access is also dependent on lowering transaction costs for smaller transactions. Consequently, developing countries will be disadvantaged in enabling cryptocurrency access to users compared to western countries with well-developed dominant infrastructure and capital. More generally, individuals do not have the computing resources required to become miners, store and update the distributed ledger and can face complications in managing personal key privacy and use. This can limit their access without the aid of “intermediaries”.

### 3.7 Borderless and Frictionless

Almost all cryptocurrencies have been created with the objective of being borderless, which is a basic feature of operating on the internet. Many cryptocurrencies have arisen as a result of entrepreneurs within particular domains targeting a particular transaction density or type of transaction that they wish to facilitate and profit from. Some such as Ripple (XRP) specialise in cross border payments for financial institutions, others such as IOTA are targeted at the internet of things or machine to machine communications globally.

The ability of cryptocurrencies to operate in each country legally will depend on regulation and the ability to convert fiat currencies to and from cryptocurrency. This implies the use of intermediaries. Cryptocurrencies such as XRP (Ripple) have partnered with banks to enable their services in cross border transfers. There have been recent instances of governments intervening to limit the use of cryptocurrencies by their citizens whilst others are investigating controls (Rogoff, 2017). Regulatory certainty is critical to trust and confidence in cryptocurrency usage and many countries are considering their stance. Private and borderless cryptocurrencies are likely to create further global inequality as developing countries do not have resources to equitably participate in these currencies which would also disrupt their economies. Cryptocurrencies also enable currency substitution that impacts the effectiveness of monetary policy controls and reduces the seigniorage governments can use to pay for services and infrastructure.

\textsuperscript{14} https://www.coindesk.com/the-8-steps-to-becoming-a-bitcoin-savvy-bank/
3.8 Debasement Protection

A national money supply is mostly in the form of deposits created from loans written by banks under a fractional reserve banking system. Cryptocurrencies cite bad fiscal management that usually results in excessive taxation and spending requiring expanded money supply or debt that is subsequently monetized.\(^{15}\) They also question government bailouts, such as that after the financial crisis of 2008 using public money, as an example of unfair practices at the expense of citizens. Taking away control of the money supply from government is a key objective of many cryptocurrency advocates so that it is privately controlled, with benefits to the participants and not government or financial institutions.

Cryptocurrency advocates believe that autonomously controlled money supply eliminates the risk of inflation from excessive money creation and is better than a fiat system as it protects the interests of all users. All cryptocurrencies propose strict limits and even absolute caps on the quantity of cryptocurrency that will be created. This is potentially one of the most attractive aspects of cryptocurrencies in that finite supply reduces the risk of falls in its value due to excessive expansion in supply. However, that is also a problem in that speculative investment by those believing that increases in demand will increase the value, can create “bubble” type situations, and potential for price volatility. Were a particular cryptocurrency with autonomously, exogenously, determined supply to become the only form of money, there is a risk of deflation (of real goods prices expressed in that unit of account) unless the money supply is expanded to serve the real economy’s needs.

4. MONEY, TRUST AND INSTITUTIONS

4.1 The Evolution of Money

Money, in whatever form it takes, is the principal way in which societies ascribe and communicate value. For anything or any artefact to be classified as money it must be capable of fulfilling specific functions; namely a medium of exchange, a store of value and a unit of account. These functions however, are a necessary but not a sufficient condition for an artefact to be money. For anything to function as money in an economic sense, it also needs the appropriate social environment of trust. This enables parties to have confidence to exchange safely, efficiently and effectively, and hold the instrument as an asset in the time between transactions (or longer as a store of value) as is currently achieved using fiat currencies such

\(^{15}\) Monetization occurs when the central bank prints money to buy bonds issued by the government treasury.
as the dollar. However, fiat money has taken hundreds of years to develop and has done so in parallel with the generation of trust provided by societal settings notably financial institutions.

Historically, forms of money evolved from traded commodities to more convenient forms such as private banknotes and fiat coin/paper currencies that were mandated as legal tender by sovereign government.\(^\text{16}\) This was further reinforced by formally regulated financial institutions such as banks, who facilitated the use, storage and protection of fiat money held by the populace. Financial institutions also participated, as trusted parties, in the operation of economy wide payment and settlement systems as well as the secure storage of money in the form of deposits. Financial institutions are trusted (either implicitly or due to prudential regulation) to use deposited funds to provide a range of associated lending and investment services, which generate valuable assets backing their deposit liabilities. The success of modern monetary systems is fundamentally due to this evolved framework that engenders trust.

### 4.2 Emergence of Digital Currency

The emergence and widespread adoption of computers into business in the 1960s led to the digitization or electronic storage of records of account. Financial institutions were amongst the first organisations to use computers to conduct business when deposits and transfers at banks were converted from what was originally recorded in paper ledgers.

Digitization of financial records by intermediaries allowed new efficiencies through the conversion of money from a physical form to electronic, but acceptance was only feasible due to the pre-existence of an institutional framework of trust. Furthermore, regulation and certification by government provided trust and confidence that electronic records were safe and the exact equivalent of fiat money. The entrusted financial institutions would be able to convert this digital currency record into cash or bank notes and vice versa to allow physical exchanges of currency as well as electronic transfer of digital currency. In the event of loss or destruction of a physical record of money or transactions between individuals or entities it was not lost. The financial institutions could certify or guarantee ownership of money or existence of a transaction providing confidence and certainty of completion of transactions done on computers. This provided further trust and confidence to conduct transactions in the fiat system electronically. Toward the late 1990s increased computer technology,

\(^\text{16}\) In August 1971 US president Nixon announced a change to a key component of the Bretton Woods system of international financial exchange in that the US Dollar would no longer backed by gold and made it a fiat currency. Since this time most countries have adopted a fiat currency system.
telecommunications networks and the internet has enabled even more ways to conduct electronic transactions.

New internet retailers such as Amazon, Alibaba and eBay as well internet presences of existing retailers have resulted in the emergence of new digital payment intermediaries and methods such as Paypal, Apple Pay and Samsung Pay. Financial institutions have also enabled contactless payment systems, such as Visa payWave© or NFC payments\footnote{Near Field Communications (NFC) use secured communication devices mounted on cards or devices to securely transact without the need to present cards or authenticate and identify individuals as this is guaranteed by the financial intermediary.} using card or smart phones, and these payment methods are widely trusted and accepted. This capability has resulted in a reduced proportion of physical cash transactions. Facilitating this has been the role of trusted parties, ostensibly financial institutions who would be able to remedy disputed transactions on behalf of their clients.\footnote{We will see later that this important capability capability is not available on cryptocurrencies due to the nature of their design to achieve secure peer-to-peer transactions.}

\section*{4.3 Trust}

Trust is fundamental to achieve efficient mechanisms in market exchanges or transactions (Zucker, 1986). Trust is not a measurable commodity but an intangible condition that creates confidence to encourage exchanges. Zucker describes three modes of trust production: process trust (tied to past experience or expectations), characteristic trust (tied to or arising from a person, group, ethnicity or family) and institutional based (tied to formal societal structures).

Money mediates exchange in that parties only need to understand the value of the exchange in terms of the artefact being used as money and thus minimises search costs necessary in a barter exchange. However, it is critical that parties to transactions are able to have mutual expectations of a safe environment for the exchange without economic loss, as this generates trust. Consequently, that trust provides the confidence to transact but it also implies the ability to manage the risk associated with dealing with a potentially unknown counterparty. During periods of change and transformation there are disruptions to trust (Zucker, 1986). We are at that point, with the advent of the new technologies and cryptocurrencies that are based on them, where institutions that can support the production of trust are not in place.

There is also the fact that cryptocurrencies involve (anonymous) usage across countries and it is to be expected that there also exists cultural heterogeneity among users. Therefore, there is a need to create an environment of trust normally enabled by regulated institutions and government, particularly when dealing cross border with unidentified parties. When a contract...
is undertaken, there is an expectation of reciprocity that the counterparties can expect of each other, but it can also be reasonably expected that counterparties will act in their own self-interest.

4.4 Semiotics of Cryptocurrencies

The rapid growth in the number of cryptocurrencies (and market prices expressed in terms of traditional money) has attracted much attention in the press, but it has been difficult for the public to understand how they function as money. Growth has been driven by speculation and, among some participants, perception of cryptocurrencies becoming an alternative and viable form of money in the future. For cryptocurrencies, many doubts exist as to whether they can be trusted as they exist only as digital records on unknown computers managed by unknown parties and are hard for the general public to understand.

A significant part of the public awareness of cryptocurrencies apart from their growth in reported value is also due to their marketing and branding. Cryptocurrencies are presented with imagery as so to appear as equivalent (electronic versions) of traditional forms of fiat currency issued by governments or central banks. Branding as a form of marketing is an important element in the development of trust and confidence in that the customer (or holder of the cryptocurrency) may believe that the firm (the DAO operating the token coin) will act in their best interests (Chaudhuri and Holbrook, 2001).

Evidence of branding by cryptocurrencies to emulate fiat currencies is very common. When the media reports on Bitcoin or where advertisements are presented, the cryptocurrency is often depicted as an image of a gold coin stamped with the letter ‘B’ with two vertical lines through it, like traditional currencies written in short form (e.g. $, ¥, £, €). Other cryptocurrencies similarly have a line through the letter (mimicking fiat currency) used to market their brand (e.g. Monero, Litecoin, Dash). Other marketed images used may represent something that depicts the network effect of the blockchain (which is the main security feature and a buzz word) or something that carries that symbolism of security.
Blockchain is a buzz word and some companies have used this word in their titles or have adopted the word to gain stronger branding and raise capital. Some companies such as Kodak, benefited by an immediate increase in its share price when it announced they would use blockchain technology and produce a cryptocurrency termed Kodakcoin. This behaviour has parallels to the dot.com boom where companies that changed their name to internet related dot.com names reaped on average a 74% abnormal stock return around the announcement date (Cooper, Dimitrov and Rau, 2001). Nevertheless, cryptocurrencies such as Bitcoin are not trusted anywhere to the same extent as fiat and are often viewed as scams not withstanding recent fraud events involving large losses to hackers.

### 4.5 Institutions and Trust

Banking is an institutional arrangement with intermediary mechanisms, which can be characterised as providing trust when there is evidence of an active market (Zucker, 1986). Cryptocurrencies without intermediaries have very limited ways of building trust, and only on process-based trust, which can only depend on prior experience with the process. Characteristic based trust is not achievable with cryptocurrencies due to the inability to identify counterparties depending on the nature of the trade to be conducted. Therefore, there is a need to build trust in such a way so as to socially legitimize it, so that a particular cryptocurrency can be traded and used to a greater extent, particularly when a key feature is that parties can be effectively be anonymous.

The need for trusted intermediaries arose not just for transacting purposes but also to assist in protection or storage and transport of wealth, physically and in time as investment. Financial intermediaries have met the need to reduce risk in undertaking transactions between two

---

19 The Long Island Tea Company changed its name to Long Block Chain and then tried to raise capital it needed (Morris, 2018).
parties who may not trust each other and may also not be known to each other. Depositors had a degree of confidence that bank notes and deposits would be honoured and this trust in such institutional arrangements evolved into early banks. This was possible due to process trust acquired by community experience (reputation) and institutional trust established norms (later regulations) from dealings with intermediaries. Characteristic trust was also achieved as banks were a group given special status and legitimacy by government.

From the foregoing, it can be seen that one of the major modes of trust production in our society has been ‘institutional trust’ built on formalised institutions and regulations that provide for trust both between firms and across economic sectors (Zucker, 1986). Trust is imperative for transactions to occur as counterparties need to be able to transact in their own self-interest with a degree of expectation of counterparties. Institutional trust can assist in making the parties to a transaction confident that their interests are protected (Zucker, 1986). Many institutions taken for granted in the U.S. began back in the period 1840 to 1920 when institutions were built to provide trust with formal hierarchies and regulations (Zucker, 1986). The impetus for change was uncertainty and a loss of trust. This was due to internal migration of people across the U.S. and the influx of immigrants from Europe (many without English skills) which meant that cultural norms and expectations in regard to transacting were different between counterparties. Thus, an alignment in the expectations of exchange in transactions was difficult, leading to a loss of trust. Disruption of trust may also occur where there is a wide geographic distance between the counterparties involved. Historically trust must be built in periods of uncertainty with the development of institutions and regulations, this parallels the uncertainty with the current environment of cryptocurrencies being proposed as a form of money.

Institutional trust enables parties not known to each other to transact with confidence confident that each party is likely to fulfil their obligations in an exchange because the institution involved will assist in ensuring that the transaction can be concluded out securely and safely. The current environment of financial intermediaries has been critical to the attainment of a trusted environment for transacting yet cryptocurrencies advocates argue that these institutions are not needed. They assert that technical measures used by blockchains and other distributed ledger technology can eliminate the need for trust parties as intermediaries. Cryptocurrency proponents propose the elimination of intermediaries and yet they will need to co-exist in a hybrid environment with both fiat currencies and cryptocurrencies. To transact in this environment will require intermediaries as is already evident with the creation of cryptocurrency exchanges.
5. CRYPTOCURRENCY, INSTITUTIONS AND TRUST

The originators of cryptocurrencies are typically IT entrepreneurs intent on making profits in their industry (e.g. online gaming) by addressing transacting needs in a particular domain (or area of use). They often proffer ambitious claims about the ability of a cryptocurrency without a full understanding of the wider needs (beyond a particular domain) and the social environment necessary for cryptocurrencies to be trusted to operate as money. This section describes and assesses the important attributes of trust and confidence that are critical to the successful adoption of cryptocurrencies as money.

5.1 Distributed Ledger Technology as an Alternative to Trust

Supporters of cryptocurrencies argue that blockchain design can give people a sense of security and protection from hacking so that trust is implicitly provided. This ignores the importance of establishing a trusted social environment in the first place. There can be little process trust (without experience) and there is no characteristic and institutional trust to provide confidence to transact. The many incidences of fraud due to ICOs and stolen token coins in this largely unregulated market is problematic to generation of widespread trust in any cryptocurrency due to spillover effects.

We question whether technological innovations and the inherent complexity can engender at least an equivalent environment of institutional trust as per Zucker (1986). The equivalent of institutional trust in a fiat currency world is well established but it took several centuries. In that vein if central banks introduce their own digital the trust issue may be addressed in a large part as governments and financial institutions can build on their existing status as a functioning trusted institution by most consumers as they have done for fiat (Bech and Garratt, 2017).

5.2 Elimination of Intermediaries

In a hybrid fiat-cryptocurrency environment there is a need for intermediaries to enable conversion from fiat currencies to cryptocurrencies. In addition “intermediaries” have already emerged as essentially providers of cryptocurrency “deposits” which facilitate the involvement of individuals in use and storage of cryptocurrencies. Several cryptocurrency exchanges have been established, crypto-banks in some cases, that provide for services such as recovery of a wallet if keys are lost, similar to account and safe keeping services of established financial institutions. These institutions are also evolving to lend cryptocurrency, giving them a currently unregulated intermediary role.
There have been several major fraud events that have resulted in over a billion dollars of accrued losses in cryptocurrencies e.g. Coincheck in Japan (Hagiwara and Nakamura, 2018) and in some cases the exchanges reimbursed their customers (Harding, 2018). Failures of such entities reduce trust in the underlying cryptocurrencies and indicate the need for regulation to protect against fraud and intermediary failure. Newly proposed cryptocurrency platforms such as EOS claim to address this shortfall in intermediary functions by allowing for them in a DAO construct using software.

Advocates for cryptocurrency, usually information technology aficionados, would argue most fraud occurred at exchanges and not the distributed ledger. They also suggest that individuals do not need intermediaries and should manage the digital wallets themselves. This seemingly ignores the fact that individuals may get hacked far more easily and be subject to scams than professional organisations with access to their digital wallets being lost forever (Sedgwick, 2018). Paradoxically, it is often suggested that people use cold wallets (disconnected from the internet) or printed copies of wallet codes to protect from loss on the internet and store them in a safe place, such as with a trusted intermediary providing safety-deposit box or other facilities.

Financial innovation means that new intermediaries are emerging and working with other intermediaries such as cryptocurrency exchanges and mainstream banks to provide fiat and cryptocurrency loans including margin lending for shorting purposes, sharing the profits based on cryptocurrency deposits. These intermediaries including cryptocurrency exchanges, are likely to earn revenue from providing value added services to users such as account management, fraud prevention and wallet/account recovery. The existence of financial intermediaries albeit in a different form will be intrinsic to the attainment of trust under cryptocurrencies.

5.3 Regulation and Trust

Institutional trust is supported by formalising expected norms through regulation. Cryptocurrencies create a potential environment for fraudulent activity (Lam and Jensen, 2017) to occur undetected (Levine, 2018) and without channels for recourse due to lack of regulation of institutions involved. Cryptocurrencies have facilitated money laundering including the ability to undertake and mask questionable transactions on the dark web and to facilitate tax avoidance (Bloomberg, 2017).

This regulatory challenge is amplified with the rapid growth in capital raisings using ICOs, many of which appear to be scams (Zetzsche et al., 2018). Initial Coin Offerings (ICOs) are
the cryptocurrency market equivalent of initial public offerings (IPO) in the stock market but differ vastly in terms of regulation and in associated obligations of the issuers. IPOs in contrast to ICOs have onerous conditions regarding representations and disclosures as regulators go to great lengths to ensure the market is informationally efficient to engender fairness, trust and confidence. Licenced financial institutions facilitate IPOs as trusted parties as they provide confidence to investors to place capital.

Cryptocurrency exchanges apparently provide similar services to existing financial intermediaries in the fiat world but operate without any regulatory oversight and can easily mask their activities creating great opportunity for exploitation of private information and fraud (Bercetche, 2017). The foregoing raises many questions about the fairness and ethics of cryptocurrency markets and lack of regulation that is likened to the Wild West. Worse, it allows cryptocurrencies to disrupt established well-regulated financial institutions and markets who are at a disadvantage in attracting capital and trading in those markets.

5.4 Governance and Ethics

The community and sovereign governments aim to foster ethical behaviour and standards of fairness and recognition of property rights through trusted institutions such as the courts and enforcement of regulations. It is apparent that most cryptocurrencies have governance issues that bring into doubt their claims of fairness, efficiency, and effectiveness and in some cases involve questionable ethics. They vary in the effectiveness of decision making with respect to managing functionality in distributed ledger implementations, incentives for processing transactions and for the management of the supply of the tokens involved.

Governance issues often occur due to the difficulty in reaching consensus about how to manage software to make essential improvements or to fix bugs and problems. For example, there have been several instances where the inability to achieve consensus on how improve the transaction effectiveness of Bitcoin and Ethereum that has resulted in hard forks.

A hard fork is a juncture when operators/miners of a blockchain cannot agree on changing functionality of blockchain software which results in two versions of blockchain from that point on, a new and the original.

In some cases this has arisen due to conflicting interests such as large miners (who may also be cryptocurrency exchanges) acting collectively trying to extract more fees versus other DAO parties who want to adhere to core principles and focus on long term viability. New currencies
being created alongside the existing currency potentially introduces problems with integrity with respect to double spend and can undermine trust.

Some cryptocurrencies operators are being investigated for their alleged suspect claims by government authorities, and some organisations and individuals have been convicted of money laundering\(^\text{20}\). Furthermore, there are major concerns about conflicts of interest due to ownership and control of cryptocurrency exchanges (Leising, 2018).

Tether, link the value of this cryptocurrency to the U.S. dollar to provide confidence in that currency and stability\(^\text{21}\) in the price. However, it is apparent that the currency may not actually backed by reserves of adequate US dollars (or US dollar denominated assets), unlike requirements for banks. Trust in the distributed ledger process relies on the existence of a diversity of node operators or miners in the DAO. However, there is evidence of some node operators acquiring significant numbers of processing nodes due to large computing capacity and thus voting power over making of changes to underlying software.

These issues in the governance of the cryptocurrency is in large part due to the lack of developed institutional trust which is supported by regulations or professional standards. Some cryptocurrencies are controlled in less than democratic ways which gives rise to the issue of whether they are run for the benefit of those in control or for the benefit of the users. In some cases they are private individuals or corporations that have retained or reserved significant quantities of currency supply without transparency and commitments on possible changes to the release of that supply. Resulting seignorage gains at the expense of purchasers of the currency renders criticisms of bank profit making made by advocates of cryptocurrency moot.

### 5.5 Banking with Cryptocurrency

Banks facilitate payments, store and enable deferring use of wealth, and channel financial resources obtained from deposits to those needing debt capital. Trust and development of specialist skills enables those roles. Cryptocurrencies can, arguably, provide the first two of these functions, but are limited in ability to facilitate the last one of provision of loan finance. Individuals can enter contracts with counterparties to transfer tokens to them now in exchange of a promise for a subsequent retransfer of a larger value. However, such peer-to-peer transactions would not involve making use of specialised third-party (intermediary) credit

---


\(^{21}\) Tether is believed to also be controlled to a significant degree by Bitfinex a major exchange for Bitcoin and Tether and other cryptocurrencies (Leising, 2017).
assessment knowledge. Moreover, knowledge of the identity of the counterparty would appear to enable association of the public key (and electronic wallet) associated with that individual, and thus removal of the claimed benefit of anonymity from use of cryptocurrency.

Various forms of peer-to-peer lending platforms can alternatively provide, via rating of potential borrowers, the credit assessment skills for potential lenders of tokens and maintain anonymity of each counterparty from the other. However, the ultimate reliance upon knowing the identity of the borrower to assess likelihood and ultimate collection of repayment by the platform operator still prevents completely anonymous transactions.

It thus would appear that a process of credit creation using cryptocurrency as money is inconsistent with the claim of complete anonymity of transactions – at least where those transactions involve credit. More generally, the functioning of the economic system depends on adequate provision of credit. The private and restricted money supply regime implied by cryptocurrencies would impede the credit creation process and implementation of monetary policy. While the “money supply” might be autonomously generated, and possibly consistent with price stability, the supply of credit required for investment and consumption deferral needs is problematic. This creates a major hurdle.

6. CONCLUSION

This paper set out to investigate the premise that to succeed as money cryptocurrencies need to go beyond having improved technical capabilities of money, they also need to create an environment of trust and confidence. Historically the joint evolution of institutions and money has provided this framework of trust.

Cryptocurrencies are unlikely to achieve their promised capabilities unless they address the need to establish a trusted environment to operate. If they are governed better though, they may be able to achieve limited process-based trust due to experience (Zucker, 1986), but this will be limited by word of mouth, due to the opaque characteristics of cryptocurrency transactions. At this stage, they are unable to provide any characteristic based trust and they resist regulation or referential government or institutional group oversight to provide this, preferring anonymity.

The absence of regulation means that there is no institutional framework of expected norms that can lend certification to cryptocurrencies as a trusted form of money. Furthermore, they have not demonstrated that they can operate without the need for some form of intermediation to mitigate the risks to the users of the currency particularly given that they would, at least for
some time, operate in a hybrid fiat and cryptocurrency environment. Lack of regulation limiting fraud and exploitation of informational inefficiencies will further limit the trust and confidence in participation in the market.

There is currently a problem with the imbalance of regulation between cryptocurrency DAOs and related exchanges and established financial institutions such as banks. Cryptocurrencies have a cost advantage due to a lack of regulation and could potentially cause significant disruptions to the business models of established regulated financial institutions.

Perhaps more problematic than the emergence of competing forms of money to bank deposits is the lack of regulation of the ICO market and exploitation of investors. The existence of fraud in the ICO market as well as the many failed ICOs (and unfulfilled “promises”), detracts from any form of trust production. At a macro level, whether substantial subscriptions to ICOs affect overall economic growth depends on whether these activities involve productive real investment, or involve primarily a transfer of wealth from investors to promoters. Growth of cryptocurrencies has also involved significant wealth transfers. We suggest that cryptocurrencies are a new form of financialization with no productive value to the economy over existing money systems.

Cryptocurrencies have not demonstrated efficiency gains in the narrow focus of the transaction payment domains that they have targeted (although they are relatively immature and will improve throughput rates). However, there is no certainty of completion of small transactions at an efficient cost – limiting a more general role as money. In addition the lack of reversibility of transactions poses risks to individuals, which are less problematic in transactions via existing intermediaries.

Transaction processing incentives, necessary to induce participation in the verification process, are complex and confusing. Intermediaries/exchanges have emerged to facilitate transaction cost mechanisms, particularly for smaller transactors, but governance arrangements, with opportunities for conflicts of interest between operators, exchanges and users also need to be resolved.

Cryptocurrencies as currently proposed, namely as private money, are under increasing scrutiny from governments. As well as concerns about money laundering, tax avoidance, fraud, etc., there is also the potential that wider acceptance could lead to national currency substitution involving borderless cryptocurrencies and implications for monetary and financial control. It is unlikely that they will be allowed to operate without regulation or governments’ action to restrict their usage to lower level payments systems for smaller “ecosystems” of
participants, undermining trust in them as fully functioning money. More likely governments will investigate or implement their own cryptocurrencies to prevent disruption to sovereign money and the ability to manage the wider economy. Cryptocurrencies fail to meet the promise of fair and equal access due to the need for access to technology and computing resources.
REFERENCES


APPENDIX

In the case of a blockchain such as Bitcoin, when a new transaction is input to the network it is placed in a pool before it is subsequently drawn by nodes and accumulated with other transactions in a block\(^{22}\). POW is then undertaken (mining) prior to a consensus process of approving the addition of the block. A hash\(^{23}\) code for the new block is generated from the transaction data and hash value of the previous block and is published as a candidate for verification and consensus in the blockchain. The new block is only added as a candidate if POW is satisfied and\(^{24}\) that the block is valid and then accepted by the majority of the nodes by appending the candidate block onto the blockchain. The block that is connected to the longest list of previous valid blocks will be adopted by nodes in the blockchain that block becomes the next consensus block.

Once added to the blockchain each block is cryptographically linked by current hash to the prior hash code to its preceding block and so on, in a chain that grows in length over time. In Figure 1, Block N is encoded so its hash code exactly represents the transaction data in Block N and the hash for block N-1, Block N-1 is encoded so its hash represents the transaction data in Block N-1 and the hash for Block N-2 and so on. If fraud is attempted by altering the content or data of a past transaction, a different hash-code will be produced for all subsequent blocks to what is recorded by all nodes. If the code changes, it will then be rejected as it will not match what is recorded on the nodes of the network. Money cannot be spent or used unless it existed in the blockchain through a previously approved transaction, and once spent cannot be used again. Transactions on the blockchain cannot be deleted or reversed.

\(^{22}\) Cryptocurrencies vary in the way they group transactions as some do not use blockchain.

\(^{23}\) A hash is a unique cryptographically generated code that is calculated on a set of data.

\(^{24}\) Consensus in a bitcoin is where the first valid block that is created in time is eligible for addition to the blockchain provided it is the associated with the longest number of consensus validated preceding blocks (which can differ until consensus is achieved) and is adopted by the majority of nodes. There are other methods employed by cryptocurrencies for achieving consensus that do not involve POW or blockchain.
**Figure 1: Security Features of the Blockchain**

*Altered blockchain will have a mismatched hash and will be rejected.*

Figure 1 illustrates a valid blockchain on the left and an invalid blockchain on the right hand side (RHS). Assuming two new candidate blocks are proposed simultaneously block n (good) and block n’ (bad) and on the right but the second block (n'-1) on the RHS chain is also a fraud. Remembering that the hash is an encoded representation of the data so if data changes the hash changes. Each block’s hash is generated using the data that comprises the transactions contained in the current block as well as the previous block hash and is time stamped so they can be time sequenced on the chain. Then block n-1 hash is based on data for block n-1 which includes the hash for n-2 and so on and a chain is formed linked by block hashes.

The first block presented to the nodes operating the blockchain would be a candidate for a new block. A bad candidate block has a mismatched prior block (n'-1) hash and would be rejected. Note that the hash for block n and n’ would be different anyway if different transactions are inserted in each block so a choice is made on the basis of consensus for the first block and if valid then the second block is examined and so on until the longest chain is fund (usually within 6 blocks). However, if the majority of computers had already accepted good block it will be added to all nodes operating on the blockchain or they risk having an invalid
chain needing reprocessing as any new blocks would be added to block n not n'. The invalid chain would only be accepted if majority of computers participating at the time were dishonest and choose the RHS block in the first instance and then they would look at the second block and reject it. The only way for the RHS to be accepted is if the majority were hacked and prior records were changed or they were collaborating against the good computers. If it is also possible to control 34% of the bad computers and block 33% of honest computers using a Distributed Denial of Service attack or to isolate and deactivate those computers then it is possible to hack the system. This is known as the Byzantium tolerance problem.