Cryptocurrencies: The New Common Good or a ‘Pig in Lipstick’?

Abstract: The governance of the fiat money system via democratically elected government and financial institutions aims to ensure that all can transact fairly and safely with confidence in the stability and viability of that system for the common benefit of all. But the global crisis of 2008 brought into question the fairness of capitalism utilising fiat money. Cryptocurrencies have been proposed by some as an alternative form of money justified on the basis of giving users more sovereignty and greater fairness and justice implying a greater common good than existing fiat money. This paper considers these claims with an analysis that demonstrates that in practice cryptocurrencies are more susceptible to the ‘tragedy of the commons’ due to governance problems and contradictions of claimed benefits. We use some examples such as the allocation of resources and incidence of ‘forking’ as a result of failures in governance structures as parties vie for a greater share of the ‘lake’ at the expense of the commons. We apply the theoretic framework of Elinor Ostrom (2005) and suggest ways to improve governance to ensure that common good objectives including ethics and sustainability are achieved.

Keywords: commons in finance; cryptocurrencies; money; ethics of money

JEL: E42, E40, B53
Cryptocurrencies: The New Common Good or a ‘Pig in Lipstick’?

1 Introduction

The attainment of a fair system of managing the use of public or shared resources has been the subject of much analysis in social sciences and management literature (e.g. Evans, 1991; Sison, Hartman and Fontrodona, 2012). Resources that are owned by the public and available for use by the public but, without appropriate governance can result in suboptimal outcomes, as each party acting in their own interest deplete or spoil the resource for all removing its availability in the future (Ostrom, 2012). In a well ordered society where citizens can live with a sense of fairness and equivalence, it is imperative that major political and social institutions can effectively work together for the greater good with an overwhelming sense of justice where utility of the average person is maximised (Rawls, 2001).\(^1\) However, fairness for the common good may be seen as a form of constraint on profit seeking (Kahneman, Knetsch and Thaler, 1986) for what Meyer and Hudon (2018) term the ‘commercial commons’ or market economy. The effects from the global crisis of 2008, highlights a perceived lack of justice for the public in the name of capitalism as a result of unfair practices of banks and governments based on fiat forms of money which motivated the creation of cryptocurrencies (Nakamoto, 2008). The term the ‘tragedy of the commons’ was first used by Lloyd (1833) and later developed into a wider context by Hardin (1968) to describe such situations but initially in the natural rather than economic world.

\(^1\) Rawls (2001) contrasts this alternative to a form of society as one where the main aim is to maximise the output of goods and services and where equality or fairness may not exist.
Fiat money\(^2\) can be considered a common good that is used to function as a medium of exchange, store of value and a unit of account, to ensure a well-functioning economy for all participants. It is governed by a formal structure of government and authorised financial institutions, who are elected through democratic processes, for the benefit of all users. The governance of the fiat money system aims to ensure that all who choose can transact fairly and safely with confidence in the stability and viability of that system for common benefit.

Increasing feelings of inequity of fiat monetary systems in particular geographic or social domains have motivated alternative monetary systems or complimentary Currencies (Lietaer, 2001).

Other alternatives to improve fiat money as commons, utilising Central Bank Digital Currencies,\(^3\) are also being examined as ways of reducing inequity (Andolfatto, 2018). In this paper we examine cryptocurrencies that are being proposed as alternative forms of private money for the common benefit. Cryptocurrencies take a number of different forms and can offer different functionality, particularly when issued as a token\(^4\) 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 money.\(^5\)

---

\(^2\) 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 but can also be represented electronically with the backing of financial institutions such as banks.

\(^3\) Allow ordinary business and people to use the central bank to hold accounts that can transact digitally and settle directly without going through banks as these accounts have equivalent access to banks.

\(^4\) 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.

\(^5\) Regulators such as the SEC in the United States have expanded regulations over concerns to protect consumers using digital currency exchanges (DCE) using initial coin offerings (ICO)s as capital raising mechanisms (see 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
1.1 Financialization and the Global Financial Crisis

During the 1980s through to 2000s there has been tremendous growth in the financial sector as a proportion of GDP in a phenomenon that is described as financialization (Krippner, 2005). Financial institutions were heavily vested in looking at ways to create new financial products and sources of revenue (with considerable risk) and in the process drove a boom in credit and a significant expansion of the money supply exploiting the fiat money system. Financialization is criticized as it has used the fiat money system and diverted resources from the real economy to benefit banks. This was as a result of financial institutions creating new products (larger nets if we use a lake with a finite supply of fish as a commons analogy) and non-industrial (financial) activities of non-financial firms capturing an increasing share of the economic value for no real output or real benefit to the economy. Collins (2015) reported that the finance industry was responsible for 20% of GDP in the United States doubling its size since 1970 whilst manufacturing fell from 30% to 10% in the same time.

The global financial crisis (GFC) of 2008 triggered by the creation of bad securities was seen as a failure of financial institutions and government to administer the fiat monetary system on behalf of all at the expense of the many. The government significantly expanded the supply of

token once enough capital is raised or a certain date is reached. Some cryptocurrencies operate as part of a platform of services, and White Papers outlining expectations and operational aspects. The definition of a cryptocurrency is used loosely and does not necessarily mean an alternative form of currency.

6 Financialization according to Krippner (2005) refers to the accumulation of profits through financial activities rather than trade or commodity production.

7 It is a popular misconception that all money is created by government. Banks create the majority of all money through the provision of credit in a fractional reserve banking system.
money to acquire the bad securities at the heart of the GFC to bail out the very banks that had created those securities (such as mortgage backed bonds) trying to earn excess profits through financialization. The money created represents an indirect tax on the wealth and standard of living of the public as it results in eventual debasement of the value of money in the fiat system.

Traditional forms of institutions failed the general taxpayer because of financialization – banks captured more of the financial system that do not give any real return other than to the financial sector. Governments let people down against the common good because they should act for the commons, but appeared to act on behalf of special interest groups. For instance, banks which were considered Too-Big-To-Fail (TBTF) by politicians were bailed out by governments.\(^8\) This was done by creating or printing more money or borrowing more leading to further debts, specifically to support the parties abusing the system i.e. banks and governments. Therefore the bailout of banks represented crony capitalism that saw a privatization of profits and socialization of losses, which led to activist groups such as the Occupy Wall Street movement and motivated alternatives.

1.2 The emergence of cryptocurrency as an alternative common good

In the shadow of the financial crisis of 2008 and excessive financialization profits, Nakomoto (2008) in the belief of a need for a fairer monetary system, proposed the Bitcoin cryptocurrency. Built on a public open blockchain using publicly available software the Bitcoin

\(^8\) Politicians are concerned about maintaining the viability of banks. People who rely on banks with their wealth for instance with money in bank accounts are likely to protest against the government if the bank fails and their funds are seemingly jeopardised. The failure of a TBTF bank would also have even more dire consequences including loss of trust in the financial system of a country.
whitepaper suggested the private currency would be fairer and eliminate the need for financial institutions and government in financial transactions along with lower costs. Based on the principle of finite private money (which excludes government) but open and borderless for public use, that allows settlement on a peer-to-peer basis. The idea is to build and operate a shared currency system that is a common good, namely a shared public resource that benefits all users fairly and makes the governance of money by government and financial institutions redundant.

Money, whether it be in a physical or digital form, is something that most people rely on universally as a means to transact. We argue that money is for the common good of the people in society and it is important that it operates efficiently, effectively and fairly regardless of which alternative is used. One reason for this is that if people do not trust money they will use alternative forms.

Related ‘commons’ research has considered the ability of the cryptocurrency miners or those who transact blocks of transactions, to drive the reward price given to miners for successfully transacting blocks down, to the detriment of the commons (Bentov, Lee, Mizrahi and Rosenfeld, 2014). But we expand this consideration beyond the mere information technology structures to consider the overall governance and ethical claims of cryptographic money and the financial architecture it operates within, in the context of the common good. Literature considering the economic consequences of cryptocurrencies as a form of money have tended to focus on the functions of money often highlighting the volatility of price not being conducive to a store of value and in particular using the example of Bitcoin (e.g. Yermack, 2015). An exception considering cryptocurrencies as a commons include Meyer and Hudon (2018) where they highlight that cryptocurrencies are a man-made commons where the governance needs to
be set up rather than driven by nature. They consider the users of cryptocurrencies could be considered as a group which could classify them as a ‘social commons’ with holistic ambitions for the good of society, while others may not operate in that manner and be a ‘commercial commons’ instead. We propose that cryptocurrencies that try to operate as a form of money for the common good are in fact at this stage ‘commercial commons’ despite their ‘social commons’ claims.

Cryptocurrency proponents cite that their system is better as it takes away control of the money supply from government and financial institutions to one that it is decentralised, public and controlled privately so that there are common benefits to all participants who operate the currency (Nakamoto, 2008). Cryptocurrencies arose because of government largess i.e. printing money for government purposes or spending too much money on defence or concessions in order to improve their chances of being re-elected - or printing too much money to bail out banks. In addition, the banks lent out too much money under the fractional reserve system and even though the fractional reserve system was created for the common good. If the banks behave properly then the money could be circulated fairly. But the financial sector of many western economies has become very large, called financialization, which has reduced resource availability to the real sector (Stockhammer, 2004). Recall in countries that have suffered from extreme inflation such as Argentina, Venezuela or Zimbabwe governments have printed money and exacerbated the situation (Lin and Chu, 2013). Inflation is like a tax on everyone and therefore plunders the common good. This background is useful because it is what motivated a new proposal for a cryptocurrency as a common good type system for one that can replace conventional fiat money with cryptocurrencies So our paper uses the commons research area to critically evaluate the claims that cryptographic money can be considered as a
fairer and more just form of money compared to traditional fiat money, very similar to Rawls (2001) notion of a society built on justice for all.

We take an analytic view of cryptocurrencies—that have the ambition of being an alternative form of money to traditional fiat systems—and undertake an in-depth analysis of their promises and governance mechanisms to expose the ‘tragedy of the commons’. Cryptocurrencies have unique governance propositions that eliminate the traditional institutional governance employed for fiat money. There is a need to use various decision rules to update incentives, allow information to be shared, to oversee the use of the common good and engender compliance. We then use the theoretical framework of Ostrom (2005) to explore the ways in which the governance can be addressed to prevent the failure to achieve the common good.

The remainder of this paper is organised as follows: first we discuss the theory and concept of the commons and its application to money and cryptocurrency. Secondly we describe and present the salient aspects of cryptocurrencies in terms of their promises, features and the governance arrangements. Thirdly we critically evaluate the failures of cryptocurrency with respect to their promises and the failure of governance and incentive issues that result in a tragedy of the commons. Finally we discuss the problems with governance and ethical issues and propose processes to rectify or minimise the potential for failure of the commons by exploring the Ostrom (2005) principles and end by outlining our conclusions.

9 Dietz, Ostrom and Stern (2003) suggest that governance should be determined at various levels e.g. hierarchies, community self-governance and markets.
2 Theory of the commons applied to money and cryptocurrency

2.1 Theory of the commons

The commons can be defined as a resource owned by all that should be passed on from one generation to the next (Bollier, 2002). Examples of the commons often relate to the delicate balance in the natural world to maintain the system. Lloyd (1833) for example considered population levels that could be adequately maintained without leading to poverty and repression. Hardin (1968) suggested that the finite ability of the natural world to support life was limited because each living organism requires resources which are limited. Hardin (1968) also created the term ‘tragedy of the commons’ using an example of a shared pasture or common land. Herdsman will tend to take their own self-interest first and try to maximise their short term returns with the number of cattle they can graze on the shared pasture. But the problem is then that if too much grazing occurs the land will degrade and the grass will not grow and then everyone in the commons will suffer (Hardin, 1968).

In an effort to manage the commons more effectively Hardin suggested either government regulation or exclusive private ownership where the latter option is considered more likely that the owner of the land will have it in their best interests to maintain the land. Ostrom et al. (1999) also suggested that institutions can be built to prevent the commons from being misappropriated rather than having to necessarily privatise common goods or services. The same sort of commons analogy can apply to a lake with a finite supply of fish. You may have fisherman who would like to fish, but the number of fish that is taken must be sustainable to ensure future viability of the lake.
2.2  *Money as commons*

Fergusson (2008) reports that Friedrich Engels and Karl Marx considered money as an instrument of capitalist exploitation. He also suggested that European Communists even to the 1970s considered using some form of utopian state with no money but this has not been achieved. Money has numerous benefits including being able to store value for future use and removes the double coincident of wants as with barter transactions. Dodd (2015) posits that where money is actively created by its users then it could be considered a form of commons as it is ‘a social agreement amongst users’. Future money could become more pluralistic if money is treated as a form of commons but concerns remain over ownership and governance of money. Payment systems are increasingly privately run and that profit is sought in their transactions in a form of profiteering. The ‘new seignorage’ Dodd (2015) contents has the ability to be ‘equally corrosive’. Using an example to contrast the wider ability of Bitcoin to be spent in many countries but with less acceptance, Dodd contrasts it to London’s Brixton Pound which can only be spent locally supporting the community where there is wider acceptance. Although Dodd (2015) suggests that alternative money is not mainstream at this stage we could argue if the governance issues can be addressed perhaps it can become a ‘social commons’.

2.3  *Cryptocurrency as commons*

Cryptocurrencies are yet another form of money that is privately controlled using complex computer programs to produce a digital form of money that is transacted with a digital wallet perhaps on a smart phone. In a number of ethical areas cryptocurrencies and their blockchain technology can impact society. According to Perrilleux and Nyessens (2017) the world is currently facing three major crises: the effects of the aftermath of the global crisis, overuse of natural resources and an increase in inequality and related social impacts. Cryptocurrencies claim to directly address two of these areas as it began initially with Bitcoin following the
global crisis of 2008 to address inequality issues related to money.\textsuperscript{10}

The technology around the new private currency was seen as a way to give power back to the individual. In other words, cryptocurrencies are seen as a way to return the common good of money back to the people by by-passing the traditional institutional structure supporting the financial system. Cryptocurrencies are therefore motivated with a social justice theme given a seeming failure by the institutions and governments that were meant to be acting in the common good. It could be argued as per Rawls’ (2001) assessment of justice as fairness, that cryptocurrencies were promoted as a form of political liberalism articulating moral values. According to Rawls (2001) justice is applicable in a democratic society where people are free and treated equal and the institutions support that notion. Cryptocurrencies can be considered by libretarians to support justice given they are promoted on anti-government, anti-capitalist or anti-institutionalist ideals following the anti-capitalist sentiment from the global crisis (e.g. Nakamoto, 2008). They are proffered as a better form of money in providing for the common good.\textsuperscript{11}

The traditional financial structure using fiat money led to enormous moral hazard issues because the banks could operate and take excessive risk by lending more, knowing governments would bail them out. So, the banks could operate unethically aided by government to the detriment of the financial and monetary system and the all users who rely on it. A small

\textsuperscript{10} Adams, Kewell and Barry (2018) also outline how the blockchain technology can better record transactions related to the natural world to better manage these resources. So in effect the cryptocurrency and blockchain technology are related to all three crisis areas.

number of banks deemed with a too-big-to-fail status received subsidies funded by excessive money creation at the expense all users bearing the costs of devaluation. Thus the failure of governance in operation of fiat money allowed a minority group namely banks, to extract rents and other surpluses through seigniorage.\textsuperscript{12} This can be considered as a tragedy of the commons because fiat money does not operate fairly and sustainably, and thus becoming the key motivator of proponents of cryptocurrencies.

While the benefits of private money have been considered (e.g. Williamson, 1999), this has been within the framework of the traditional financial architecture including banks who fulfil the important role of trusted intermediaries in financial transactions. Cryptocurrencies operate in a decentralized manner independent of banks and governments and with a new form of governance, raising questions about the need for the traditional financial architecture. Dierksmeier and Seele (2018) were concerned from an ethical standpoint that cryptocurrencies can support illegal activity and money laundering. They suggested that further work was required in the area to clarify apparent moral ambiguities and to find ways to improve the ability of cryptocurrencies to support the betterment of society.

The ethical use of alternative forms of currency systems including cryptocurrency as a shared resource, are analysed as a new commons under the common good framework as developed by Meyer and Hudon (2018). They classified cryptocurrencies as a common good delineating their theoretical framework of commons into ‘social commons’ versus ‘commercial commons’ with

\textsuperscript{12} Seignorage is the net gain from the resources received in exchange for newly issued currency in excess of its cost of production
a market interest. A social commons should promote social cohesion and sustainability with a community of users, whereas a commercial commons has a profit or market interest. We would argue that although cryptocurrencies have been promoted on the basis of a ‘social commons’ they are in fact run as a ‘commercial commons’ under that framework.

Importantly, Meyer and Hudon (2018) considered the distinction between the terms ‘commons’ and ‘common good’. The term ‘commons’ can be considered as the governance mechanisms of a shared resource on how people can behave (Hess and Ostrom, 2011), whereas ‘common goods’ can be considered as the ethical perspective of a process and how it impacts an individual and shared community. The people who operate or manage the computers that process the transactions for cryptocurrencies like Bitcoin are called miners. Incentive schemes determine how miners or operators are rewarded for operating within the systems framework of the cryptocurrency. Incentives for miners can vary from a cryptocurrency payment or perhaps free processing of the miner’s own transactions. Governance systems are typically on a consensus basis by all miners and or users, therefore they are more difficult to change as people will have set their behaviour given by the rules of what is allowed. Cryptocurrencies typically announce their governance structure in their White Paper which can be found on their related website. The governance rules may be altered by a number of means but often with divergent views with hard forks\textsuperscript{13} which we will discuss later.

\textsuperscript{13} A hard fork arises when there is a proposition to change the system of governance which is embedded into the software and two or more versions of the software are adopted in effect creating additional versions of cryptocurrencies, akin to dividing the lake into two smaller lakes of a fishing common.
Our suggestions on how to update cryptocurrencies to make them a viable social commons are guided by Ostrom’s (2005) principles for designing a robust social-ecological systems for self-governance. Elinor Ostrom won the Nobel Prize in economics in 2009 for her body of work on how best to govern the commons. She was an avid supporter of the commons systems after basing her research on observing communal systems in many countries and various settings, operating free from government regulation. She warns that application of the guidelines be adjusted to the particular scenario of commons. Ostrom (2005) suggests that smaller sized groups are easier to manage, while Hardin (1968) suggested that the number of variables to consider increases with size. Ostrom (2005) points to a common understanding, a low discount rate, and an ability to determine the rules, and importantly trust as being a required features of the common group for success.

3 What are Cryptocurrencies

3.1 Overview of cryptocurrency

Bitcoin began in 2009 after a person or persons under the pseudo name Satoshi Nakamoto put forward a new form of electronic payment system using Bitcoin as the alternate form of money (Nakamoto, 2009). The Bitcoin system uses 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. Therefore, cryptocurrencies are claimed

---

14 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 of the majority of ledgers.

15 A blockchain is a set of linked, 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
to be superior as they allow a number of efficiency gains and more effective transactions, and additional functional benefits and lower costs.

Cryptocurrencies such as Bitcoin are created and maintained in open software, that is identical and which is used to create, transact and record financial transactions and also have the ability to implement and settle smart contracts\textsuperscript{16}. So far cryptocurrencies have been privately run so that they do not have the involvement of government or regulators and nor are they enforceable legal tender able to assert property rights. Money takes the form of cryptographically secured digital tokens which are placed in encoded digital containers known as wallets that are accessed by digital keys (the wallet account identifier) and private keys (the lock signature held by the owner). This is similar to a bank account that only accepts transfer instructions by a registered signatory. The distributed ledger is a database is a blockchain that is replicated on many computers with the efforts and resources of multiple operators, all of whom must run the same software. This is so as to have the same record of transactions they collect and process (usually into blocks) accepted by the majority of users. Any operator using different software runs the risk of being excluded from the consensus distributed ledger system and will not receive any reward as they will be deemed to have ‘hard forked’ from the main database. To record transactions, they use sophisticated cryptography (and Merkle trees to securely link and collect transactions into sets or blocks that are then appended into block chains after solving cryptographic puzzles (to find a special number known as a nonce). The practical

---

\textsuperscript{16} First proposed by Szabo (1994) a smart contract is one that has its terms and conditions encoded as an algorithm for execution in software.
implementation of cryptocurrencies at the scale of adoption necessary for mass usage in the general population only became possible in early to mid-2000s with the ubiquity of smartphones and powerful cheaper portable computers as well as mobile internet.

In contrast to fiat money systems government earns seigniorage profits when they print more money after allowing for production costs but also put in place an enormous infrastructure of regulators, intermediaries, legal protection and enforcement. In the case of cryptocurrency this profit can be made by the operators and the platform developers’ benefit with seignorage by holding coins acquired in the processing process or received in an initial coin offering (ICO). But this is without incurring any personal liability for failure or to provide any support to users beyond transacting. Thus because of easy creation of cryptocurrency in software, without the need to provide any institutional or legal infrastructure and support service to users apart from operating the computers, they earn enormous seigniorage profits.

There are four major characteristics of cryptocurrencies: firstly they all use distributed ledger technology (DLT) a type of database that is updated by various consensus mechanisms (which may involve proof of work, POW, or proof of stake, POS) to eliminate the need for trusted intermediaries. The second is that coin issuance is private and controlled by software embedded rules (but can be changed by consensus). Third, they are cryptographically secured as are processing and recording of transactions. Fourth they mostly use some form of decentralised autonomous organization (DAO\textsuperscript{17}) to govern their ecosystems.

\textsuperscript{17} 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.
Trust is critical if there is an expectation that users will be confident of using the cryptocurrency and this depends on the effectiveness and features of the governance of the ecosystem in ensuring safety in usage and securing the value of the digital tokens. Aglietta and Orlén (1998) described three aspects for the attainment of confidence in money: methodical, ethical and hierarchical. Methodical confidence refers to the confidence that come from regular and routine use, learning and knowing that it will be successful. Ethical confidence is related to the policies and values that govern the system whereas hierarchical confidence relates to the competent institutions given the responsibility for issuing and managing the money. Alternative forms of money to fiat need to have more than embedded trust but some form of exogenous reinforcement. Central banks may introduce central bank digital currencies in the future (CBDCs) (BIS, 2018) providing an alternative to physical.

Since Bitcoin there have been many implementations of cryptocurrencies with a variety of features and characteristics, but all follow or build on the distributed ledger concepts established by Bitcoin and its blockchain (Rosic, 2017). Most make similar claims of social benefits from their existence and use relative to traditional currencies.

3.2 Promises of cryptocurrencies

Table 1 sets out claims by cryptocurrency proponents or on the relevant cryptocurrency websites, that are aiming to be an alternative form of money, such as Bitcoin, Ethereum, Bitcoin Cash, EOS and Monero to name a few.
Table 1: Promises of Cryptocurrency

<table>
<thead>
<tr>
<th>Promise</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| Trust without intermediaries (Knight, 2017)  | • Software carries out settlement using “atomic” (simultaneous) swaps  
• Transactions can be completed as settlement is assured on all sides  
• Only valid wallets (accounts) can transact and double spend is impossible  
• All transactions and existence of funds are verified by consensus  
• All records are verified by consensus majority  
• Transact directly on peer to peer basis without intermediary friction/costs |
| Privacy and confidentiality (Rosic, 2017)    | • Secure cryptographic wallets cannot be hacked or accessed without keys  
• Transactions are not identifiable to individuals  
• Wallets are not identifiable to individuals  
• External parties cannot exert control on system but can view blockchain |
| Greater security and immutability (McCallum et. al, 2017) | • Transactions once written are immutable forever  
• Transactions secured by cryptography and once executed are irreversible  
• Digitally unique cryptocurrency cannot be forged or counterfeited  
• Blockchain ensures historical sequence and content of all transactions |
| Faster more effective transactions (Schwartz et. al, 2014) | • Transactions are done instantly but subject to consensus, faster than banks  
• Smart contract capability when transacting eliminates counterparty risk  
• Does not need many layers of trusted parties and bureaucracy to complete  
• Validation of transactions provides greater certainty of completion  
• More effective cross border transactions due to simplification of hierarchy |
| Efficient and lower transaction costs (Richter et. al, 2015) (Bouncken, 2015) (Henderson, 2014) | • More efficient new technology so more rapid settlement across borders  
• Open source software means anyone can operate and compete for service  
• Infrastructure simpler, more scalable than traditional financial institutions  
• Elimination of intermediary banks lowers costs and prevents high charges  
• All transactions sizes are equivalent in effort due to scalability |
| Greater fairness and protection from debasement (Frisby, 2015) | • The money supply is finite and is governed by operators and users  
• Government debt cannot be monetized.\textsuperscript{18} under private cryptocurrency  
• Only money that exists can be transacted so no fractional reserve banking  
• Protected from government fiscal policy and inflationary policies |
| Borderless and frictionless (Rogoff, 2017) | • Transactions occur seamlessly across borders and can ignore regulations  
• Access is available through any internet connected smart device  
• Transactions can be executed independent of regulator or government  
• Regulators and government are unable implement controls or constrain us  
• Only requires party to transactions and consensus of operators to complete |
| Universality of access (Dale, 2017) | • Operators can participate from any connected point on the globe  
• Users have open access anywhere anyhow with a wallet and digital key  
• Financial & payment services once available on ecosystem available to all  
• Distributed ledger totally transparent verifiable data by authorised parties |
| Public benefit | • Governance is under a DAO arrangement so that it benefits all users  
• Cannot be dominated based on size of user or wealth of user  
• Equality in use as all users have equal access with digital wallets/keys  
• System is governed for the benefit of all users and not intermediaries  
• Resources are maintained on a shared basis for all users |

*Double spend is a potential issue with digital forms of money as money should only be capable of being spent once.

\textsuperscript{18} Monetization occurs when the central bank expands the money supply to buy bonds issued by the government treasury.
The Benefits are not common across all cryptocurrencies, but the majority of the benefits are claimed by all; in some cases there are additional features and benefits.

3.3 Governance features of cryptocurrency
The governance of cryptocurrencies can be compared to the idea of a social contract first proposed by Jean-Jacques Rousseau (1773) which seeks to protect certain rights and to moderate power. Cryptocurrencies are a shared public or community resource using with many separate operators (nodes), utilising distributed ledger technology of some description, usually a blockchain. The updating of transactions and records follows some form of consensus mechanism for updating\textsuperscript{19} across the nodes and for most cryptocurrencies in accordance with an implied social contract. Node operators facilitate the recording of transactions and contribute to create and maintain the blockchain with the incentive of earning cryptocurrency\textsuperscript{20} on behalf of all users of the system according to processing rules embedded in the same version of software. This software, which also ensures the blockchain is tamperproof, determines the circumstances for creating new currency as well as treatment and processing transactions onto the blockchain managed by consensus.\textsuperscript{21} Incentives for node operators are also based on rules embedded in software. The ability of node operators to process transactions is dependent on their ability to numerically solve cryptographic problems that take enormous processing capacity, which means that it is tied to money for processing resources.

\textsuperscript{19} These operators in the case of Bitcoin and Ethereum use a proof of work (POW) consensus system are known as miners while other cryptocurrencies such as EOS and XRP use different schemes such as proof of stake (POS).
\textsuperscript{20} There are some variations in terms of the degree of decentralisation and indeed the consensus mechanism used.
\textsuperscript{21} Consensus in this case means that block and longest chain of valid blocks that is adopted by the most operators (on the same software).
Depending on the governance arrangements of the cryptocurrency, there are some aspects of the processing rules that also rely on the operators’ choice. For example, which transactions are processed can be selected by the operator from a pool, allowing prioritization of user transactions to be determined by the operator. Changes to software (and the embedded rules) can only be made by consensus or in some less decentralised schemes by voting based on stake or value of cryptocurrency held. For most cryptocurrencies, this means the majority adoption by operators of their chosen version of software determines the rules implemented (and may not be a consensus of all users). In the event that more than one version is adopted this creates what is known as a hard fork, enabling two or more versions of the cryptocurrency to emerge after the change so that operators and users must choose which version of cryptocurrency to use or operate, potentially reducing the benefits of the cryptocurrency to the user public.

4 Cryptocurrency – A pig in lipstick?

4.1 The failure of cryptocurrency as commons
Cryptocurrencies were proposed as an alternative and a fairer form of money for all users on the basis of their greater social benefits; often using a halo effect of social justice contrasted to the excesses of government and financial institutional governance under a fiat monetary system. This is achieved by taking take away the ability of banks to charge (excessive) fees as compulsory trusted intermediators who have failed to govern fiat money for the common good. Many entrepreneurs in the cryptocurrency arena added to the halo effect by being anointed as gurus reinforcing their halo via social media including Vitalik Buterin (Ethereum), Dan Larimer (BitShares, Steemit, EOS) and Chris Larsen (Ripple) and Roger Ver, Jimmy Song and Andreas Antonopoulos (Bitcoin) to name a few. The association of well-known technologists to new ventures, along with the price increase particularly of Bitcoin seems to have driven
interest in cryptocurrencies. But it is not always evident that the users have a full understanding of the underlying governance structures.

Some have labelled cryptocurrency proponents as ultimate libertarians characterised by the term ‘anarcho capitalism’ (e.g. Flood and Rob, 2017). The promotion of cryptocurrencies as a means to voice anger, in this case as against the behaviour of banks and governments, is a practice that Hayek (2001) suggested could bring people together against the so called “better off”. In this case we could interpret the ‘better off’ as perhaps bankers and the politicians that bailed out the failing banks with bad financialization practices where both parties had built up excessive money created at the expense of taxpayers and users of fiat currency during and leading up to the financial crisis of 2008.

Cryptocurrencies are based on the idea they are more democratic and peer-to-peer oriented so that no party dominates (Nakamoto, 2008), and a more just alternative that operate for the benefit of all, where anyone can access and use the system. Furthermore there is an implied social contract based on rules or statement of intent that is typically enunciated in a White Paper22 issued by most cryptocurrency proposers but mostly embedded in software that governs the operation and use of the system. The rules in the traditional monetary system are derived by legislation from governments and executed by banks. But in the cryptocurrency world a DAO system (Decentralised Autonomous Organisation system) theoretically all who participate have the ability to influence the way it operates (voting by processing power or...

22 The White Paper is generally available on the website of the cryptocurrency, with the aim to explain how the DAO or rules of the program will operate.
coins held effects the governance). Therefore the expected rules for operating the system for
the common good are a social contract of a fairer system together with the promise of low cost
transactions as well as fair and equal access. In practice this has not been the case and we
provide examples of failure to achieve the promises of cryptocurrency giving rise to ethical
concerns and the major problems with their governance that are a tragedy of the commons.

Has the emergence of cryptocurrency, enabled the operators or founding members to profit
from seigniorage, or value received in an initial coin offering (ICO) without any personal
liability to ensure they meet their social contract of providing a fair public system. There are
many examples of crypto-millionaires extracting significant private capital gains when the
cryptocurrency value appreciated due to the public buying cryptocurrency on an expectation
of the operation of social common. Contrast this with a similar analogy to fiat money where
the government and financial institutions profit from seigniorage with the intent of benefit of
all, albeit it fails in a crisis from time to time. Under the traditional fiat system, there is a process
for rectification of failures through democratic election of government by users; the same does
not hold for cryptocurrency node operators who are anonymous.

An example of exploratory research in regards to the commons and cryptocurrency can relate
to transaction costs. Bentov et al. (2014) suggested that cryptocurrency miners, or users and /
or computers that are used to process transactions in a blockchain, can compete with each other
to drive down the price to attract more transactions. This may lead to a detriment of the
commons in that the price may reduce so low that it becomes difficult to cover the actual costs
of mining. This then provides no incentive for miners to process transaction and makes the
overall system unreliable, inefficient and uncertain with respect to transaction completion.
4.2 Failed promises of cryptocurrencies
We summarise some of the failures in the promises of cryptocurrency in Table 2 as a commons and match this for each of the claims summarised in Table 1. While it is recognised that some of the cryptocurrencies are relatively new and therefore are in the process of getting established, the dominant cryptocurrency, Bitcoin, has been in operation for 10 years.
Table 2: Failed Promises of Cryptocurrencies under Commons

<table>
<thead>
<tr>
<th>Claimed Benefit</th>
<th>Operational Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust without intermediaries</td>
<td>• Ability to enforce contract execution with unknown third parties&lt;br&gt;• Significant other services necessary for transacting are absent&lt;br&gt;• Disabled or handicapped persons are disadvantaged&lt;br&gt;• Inability to gain assistance with recovery from losses&lt;br&gt;• Seigniorage captured impacts if using institutions at cost to all</td>
</tr>
<tr>
<td>Privacy and confidentiality</td>
<td>• Ability to conduct financial crimes undetected&lt;br&gt;• Multiple identities are possible so unable to trust counterparty&lt;br&gt;• Ability to identify and trade is reduced&lt;br&gt;• Reduces property rights enforcement&lt;br&gt;• Reduces accountability for ill gains or liability for damage to others</td>
</tr>
<tr>
<td>Greater security and immutability</td>
<td>• Dependent on technology, not secure to new quantum technology&lt;br&gt;• Inequitable and depends on control of processing power&lt;br&gt;• Significant losses can occur due to hacking of exchanges&lt;br&gt;• Inability to correct fraudulent transactions&lt;br&gt;• Diminished ability to rectify economic damage</td>
</tr>
<tr>
<td>Faster more effective transactions</td>
<td>• Existing systems are much faster by several orders of magnitude&lt;br&gt;• Lost or stolen wallets cannot be recovered&lt;br&gt;• Uncertainty of viability of processing pool of available operators&lt;br&gt;• Transactions (small) not treated equitably in POW scenarios&lt;br&gt;• Consensus process to eliminate intermediaries slow transactions</td>
</tr>
<tr>
<td>Efficient and lower transaction costs</td>
<td>• Cost of cryptocurrency is volatile and less efficient to transact&lt;br&gt;• Volatility of cryptocurrency creates uncertainty on cost&lt;br&gt;• Enormous externalities of energy cost to operate relative to fiat&lt;br&gt;• Externality: Environmental damage due to excessive energy usage&lt;br&gt;• Rectification of failures falls outside of cryptocurrency ecosystem</td>
</tr>
<tr>
<td>Greater fairness and protection from debasement</td>
<td>• Impact on fiat money supply by elimination of fractional reserve&lt;br&gt;• Deflationary due to decoupling of money supply to real economy&lt;br&gt;• Decoupling of monetary policy to domestic economy</td>
</tr>
<tr>
<td>Borderless and frictionless</td>
<td>• Transacting in/with illegal funds/criminals poses legal risk on user&lt;br&gt;• Dilutes legal authority and ability to manage criminal/illicit activity&lt;br&gt;• Facilitates tax avoidance across borders&lt;br&gt;• Enhances opportunity for cyber-crime and scams undetected</td>
</tr>
<tr>
<td>Universality of access</td>
<td>• Small transactions are not treated fairly&lt;br&gt;• Requires significant resources/capital to participate as operators&lt;br&gt;• Inequality: smart phones unaffordable in developing world&lt;br&gt;• Inequality: Clustered processing power by capital or energy cost&lt;br&gt;• Reduces the ability to provide credit under fractional reserve</td>
</tr>
<tr>
<td>Public benefit</td>
<td>• Seigniorage is private reducing funding for same benefits to public&lt;br&gt;• Does not provide any institutional benefit for confidence&lt;br&gt;• Mining pools who have large voting blocks resist change&lt;br&gt;• Diminishes government ability to manage monetary &amp; fiscal policy&lt;br&gt;• Easier currency substitution can create greater volatility in fiat&lt;br&gt;• Bias of gains to dominant holders at the expense of the majority</td>
</tr>
</tbody>
</table>
4.3 Governance failures

The idea of cryptocurrencies which are decentralised and governed as what is known as a DAO, is that everyone who uses the system benefits equitably and its’ structure is run with this intent. Adapting the initial example of a tragedy of commons example of a herd and over grazing due to self-interest by Hardin (1968), a similar fishing analogy is equally famous. All have an equal chance of capturing fish if we maintain the lake and stock of fish sustainably for everyone’s benefit. That is fisherman all catch a fair share determined on rules of long-term viability of the fish population determined by the ecosystem; and consumers of fish (users) pay the fisherman a fair price so that they are viable. The metaphor of fishing is apt here if you look at the case of cryptocurrencies and software. In the case of cryptocurrencies, the ecosystem is a system of shared resources (fish and a lake) in the form of digital money (fish) in software operated on a distributed ledger (the lake) by many operators (fisherman). While the software and distributed ledger is maintained by operators, it is also up to users to agree as on how the cryptocurrency is maintained and used. In other words, how the ‘fish in the pond or lake’ should be shared and cultivated for the benefit of all. Ostrom (2012) reminds us that fisheries are generally self-regulated rather than having a guard watching over the fishermen.

We have seen numerous examples in cryptocurrencies in a relatively short time where due to failure in governance that the promises under which they were proposed will be compromised at best or not practical due to their chosen rules. For example disputes over versions of software with different rules means there have been several hard forks of cryptocurrencies where they could not agree. In addition node operators have been able to use their processing power to
achieve a 51% share\(^\text{23}\) (majority so they can change the rules) to influence the rules in software so as to benefit the “fishermen” without regard to the viability of the “lake” and the availability of the fish or the frequency and cost at which the fish (or money) are available to “consumers”.

In an attempt by collaborative enterprises nested within the commons (mining pools\(^\text{24}\)) or economic joint ventures to capture more of the benefits through voting control; operators try to use a bigger or better ‘net’ in the ‘lake’. Evidence of this activity is that the major public cryptocurrencies such as Bitcoin and Ethereum and others have had hard forks. The operators behind this split believe they have a better long term system (motivated by getting power over the governance) and the ability to attract a greater reward by choosing a particular version of cryptocurrency software. An example of this is with a split of Bitcoin with the new version to the split into two cryptocurrency chains being Bitcoin and Bitcoin Cash in August 2017. Further examples are the later split of Bitcoin Cash into Bitcoin Cash and Bitcoin SV in November 2018. The most popular cryptocurrencies, Bitcoin and Ethereum\(^\text{25}\), are having difficulty in agreeing on improved forms of software and the rules needed to the extent there have been significant controversies in governance and delays. This is also true of new cryptocurrencies such as EOS which was created on the basis of a better system, albeit with more corporate controls, as it is already facing challenges investigating changing its operating model.

\[^{23}\text{Remembering that in practice, as long as a majority (51\%) of operators choose to adopt a particular version of software, used for adding transactions to the blockchain then that becomes the version of the rules.}\]

\[^{24}\text{Mining pools are coordinated activities of node operators in a commercial or collaborative arrangement to provide negotiating or consensus power to groups of operators. Interestingly some of the “halo” individuals are being relied in almost a tribal manner influencing some of these pools or the operation of the platform operators.}\]

\[^{25}\text{Ethereum is the most successful cryptocurrency in regards to helping others get into the market using smart contracts, has also had a hard fork and still struggles to gain consensus on implementing new features or rules.}\]
So where have they failed? The hard forks are evidence of failure of governance. Some cryptocurrency models such as Ripple and EOS, award enormous amounts of the cryptocurrency that are created and held in reserve for the people who operate the platform i.e. not for the common good but for developers that earn enormous seigniorage for the people who run the platform. They argue that it is essential to incentivise them to develop and maintain it and could be seen as analogous to financial institutions who earn profits and operate on behalf of everyone else. There have also been numerous ICOs that have been issued to start cryptocurrency to encourage money to be invested in order to make speculative profit on the basis of providing a better system of money only to find that they do not provide any benefit or value to the larger community of the commons, although promised (Bercetche, 2017; Zetzsche et al, 2018). A key issue with cryptocurrencies is that there are a lot of operators in this area who have made lots of seigniorage profits by investing in early who need to have more people come and, like a Ponzi scheme, bring new money in so they can maintain the illusion of available profits. In many instances the only way that cryptocurrency operators can make money is by attracting new transactions and this has eroded the confidence and trust essential to operating as social commons.

Others have tried more innovative approaches to address the problems of consensus governance in cryptocurrency, we take other examples with EOS for example, it uses delegated proof of stake (POS) meaning you must have, to be a potential operator of a node, a certain amount of cryptocurrency at stake, meaning it can be lost if you are malfeasant. Operators are nominated as candidates for processing transactions and receiving rewards by holders of the coins and are then randomly chosen to be in a processing pool of operators. This is much more efficient but has governance complexity. EOS uses a voting system called a referendum to
update the rules in software. So after a vote and the majority decides then software will change and it is binding on everyone. Bitcoin, uses a completely open decentralised model where everyone gets to vote. Others use even more centralised governance structures which is not much different to banks. For example, Ripple or XRP uses a very much a federated but centralised model to decide on how the governance operates and how the system updates.

Modern democratic society evolved with a system of taxes for protection of property rights, national boundaries, and system of law. Cryptocurrency advocates rationalise by claiming more equitable governance, avoiding taxes but benefit from operating in a greater society extracting resources but not contributing to maintaining that system. In other words casting a net in a bigger lake that they do not maintain. We now summarise some of these issues of governance\textsuperscript{26} and use the theoretical framework for good governance of a commons following the seminal work of Ostrom (Ostrom, 1990, 2005) in Table 3.

\textsuperscript{26} Cryptocurrencies all differ on their governance all based on the claim that they are decentralised but some are more centralised than others Bitcoin (open) vs Ripple (Permissioned) EOS uses a different scheme to Bitcoin i.e. a delegated Proof of Stake (POS) system based on voting power of coin holders. They all rely on some form of governance and consensus is how the actual system is updated.
Table 3: Cryptocurrency Governance Failures Under Commons

<table>
<thead>
<tr>
<th>Governance Principle*</th>
<th>Issue</th>
</tr>
</thead>
</table>
| **Clearly defined boundaries** | • Open systems allow anyone to participate and define the extent  
• Operators can cast as many “nets” resources as they like in the lake  
• Boundaries are defined by resources and requires only money  
• Rights limited to software which can only be changed by consensus  
• No usage boundaries exist as users are anonymous  
• Possible to extract rents and externalise costs to others via pooling  
• Commons benefits can be reassigned by few with economic capital |
| **Proportional cost benefit equivalence** | • Users unable to affect changes in the rules employed by operators  
• This is subject to consensus of holders of coins or processing power  
• Long term viability hindered by disputes on cost-benefit changes  
• Block size arguments to alter costs and benefits have failed |
| **Collective-choice arrangements** | • Concentrated majority, e.g. 5 groups majority power in Bitcoin  
• Operators are acting in groups to implement rules for their group  
• DAO difficult to enact changes to maintain systems or tailor rules  
• No exogenous or regulatory oversight and no recourse  
• Only monitoring and control is endogenous (software in use) |
| **Monitoring** | • Not possible to know who is accountable and identity is divisible  
• Possible to pseudonymously detect groups but not tied to individual  
• Monitoring is at a user level with power imbalance with operators  
• Relies on endogenous detection and enforcement  
• Most breaches achieved by non-compliance outside of software  
• Anonymity and cross border nature reduces accountability  
• Some use economic (mining) power to vary rules |
| **Graduate sanctions** | • Requires consensus for implementation of sanctions  
• Sanctions are not graduated but binary generally  
• Likely to be directed at usurping groups who can veto  
• Current resolution is forking that harms users and imposes changes  
• Who to sanction in pools? |
| **Conflict resolution** | • Forking is the current undesirable resolution process  
• Mining attacks or other cyber-attacks are used in conflict  
• Rule change done by operators as cartel like actions (ignores users)  
• Resolution of conflict is based on computing or economic power |
| **Recognition of rights to organise** | • Unlimited rights to organise and given rise to pools and forks  
• No ability to resolve disputes  
• Mining attacks by Bitcoin forks evidence of ‘might is right’ approach  
• No limitation on methods of “fishing” other than software |
| **Nested enterprises** | • Governance is not implemented in layers (operators vs users)  
• Polycentric systems not recognised in governance  
• No protection from cartel behaviour with externalities  
• Cartel like dominance over value detrimental to goals/viability  
• Polycentric (pools) discourage participation of operators |

*The governance principles are based on Ostrom’s (2012) framework of how best to manage a shared social commons.
4.4 Discussion

We briefly make some suggestions that may go some way to addressing the issues and failures for cryptocurrencies as a commons but not it is not in the scope of this paper to provide remedies for all cryptocurrencies due to the number and the idiosyncrasies involved. To be considered properly they would warrant investigation on a case by case basis for each issue raised and others excluded for brevity.

The need to address the failures in cryptocurrency may be to a large extent addressed by governance but are also related to but not exclusively tied to the settings or design of cryptocurrencies.

Addressing Failures of the Promises of Cryptocurrencies under the Commons

This sections relates to Table 2, but suggests ways to address the failures under the commons. At the heart of governance failures are the incentive schemes of cryptocurrency (by design or by governance outcomes) that can be unethical at worst and at best naïve but most likely are misleading. This is because they utilise the principal of the common good to benefit the holders of capital or processing power in that system and thus are driven by single motive of profit like any other capitalistic system. Thus benefits accrue to those who can optimise the opportunities and dominate the gains.

Trust without intermediaries, with privacy and confidentiality and greater security issues are difficult to resolve without some form of institutional involvement convincing users in a system of rules that is embedded in software that is anonymously maintained and provided. This could be in the form of monitoring or regulation of the operations regarding the benefits promised to users as well as providing some support. Perhaps by considering the establishment of
alternative institutional and support structures to alleviate wrong doing and create greater confidence. This can also be achieved by technology but supported by some intuitional aspect to give confidence to users that their rights are protected or wrongdoing rectified by whatever process is proposed.

Following Aglietta and Orléan (1998) methodological confidence in cryptocurrency will increase with greater use. It will require a less complex usage environment with supportive services to rectify problems or services to protect users from loss should there be failures e.g. what to do when a digital wallet is lost. This does not necessarily mean the banks of old but reliable institutions. This will allow users to be more willing to adopt cryptocurrency and increase its usage, provided other factors are addressed.

Faster more effective transactions as well as efficient and lower transaction costs will require changes to the systems design and operation to be augmented by governance. The technology used is a function of the governance chosen for operating and securing the distributed ledger. There are many alternatives being proposed that claim superiority with security such as Hashgraph, Iota and others but are unproven. The existing POW systems have not been successful due to externalities and misuse, possibly arising from governance.

Greater fairness and protection from debasement give rise to questions in relation to the benefits of public versus private money, a discussion that is beyond our scope. Regardless of this there needs to be a clear position by regulators on their attitude to cryptocurrency. Furthermore systems can be changed by operators to increase the money supply so that debasement protection may not exist despite promises if it is profitable to expand the money supply, without recourse to regulation under current structures.
There is little that can be done by regulators in a system that is designed to evade control of borders and shields the identification of its users other than trying to shut it down, at risk to its users. This can be addressed by governance choices made by cryptocurrencies by the implementation of a limited access regime to regulators for the purposes of crime management, but here in lies the dilemma. The basic ethos for the system is to reduce borders and frictions of government. Cryptocurrency operators need to consider changing their design to allow engagement by authorities trying to implement sovereignty of law. In a similar manner that tech companies have to collaborate with the law for criminal matters.

Universe and fair access issues mainly relate to the governance of the systems and how mining operates but also to the technical aspects of software in terms of the consensus mechanisms such as POW which benefit resource density. Likewise the public may benefit or require some institutional support in a manner that enables the trust and confidence of users in the system. This means using some of the benefits of seigniorage profits be reinvested to fund the institutions (new or existing). The wider issue of public benefit needs to be considered in the debate about public versus private money creation. Proposals such as CBDC discussed by Andolfatto (2018), may enable many of the objections of unfairness to be addressed without the need for cryptocurrencies as an alternative to fiat.

**Failures in Cryptocurrency Governance as a Commons**

This section follows on from Table 3 in that it addresses the failure in the governance structure of cryptocurrencies as a form of commons, following the principles to manage a commons as suggested by Ostrom (2005, 2012). Governance remains an important area to address. Knox and Meinzen-Dick (2001) and Sekher (2001) comment about the importance of users being
involved and participating in the governance. Schweik and English (2007) suggests that inadequate monitoring has consequences particularly if the rules are not enforced. This issue is in a DAO who does the monitoring when the only hard enforcement is in software, but the issues arise out of failure to govern that software adequately.

Clearly defined boundaries need to be created to define the mutual obligations for participation in operation of the system for the greater good in exchange for access. Proof of Stake approaches provide some grounding for improving governance but a simple open system without any commitment to the common good is flawed. Proportional cost-benefit equivalence for example and to not allow discretion over transactions processed or any ability to consider the content of transactions prior to processing could improve this for users. Smart contracts could be put in place to recognise the presence of unbalanced interests and be used to constrain individuals or operators rather than implement common rules. In this way as participants come and go, the base line of rules is unaffected.

Collective-choice arrangements require a more disciplined approach to equitable property rights that are established within the system. This means that the rules should be able to be enforced by all users (or their chosen proxy) and balance the interests of operators and users. Furthermore, voting structure based on aggregate economic power should not be allowed to marginalise the vote of smaller users and some limit or governance to absolute aggregation of voting blocks to individuals or entities should be put in place.

The monitoring of behaviour that usurps the commons is pointless unless the monitored breaches are accepted as such and have a consequence. Monitoring ideally should implemented by consensus (and can be external ideally) and given the power to impose penalties. This is in
the context of a better voting structure to implement such rules. Monitoring adds credibility and stability and is akin to regulation that is voluntary and build confidence for users and operators alike.

There is no mechanism for penalty, as suggested by Ostrom (2005) and for most cryptocurrencies other than exclusion from incentives and in some cases a cost-benefit deterrent for malfeasance. There needs to be some form of penalty, proportional to the potential damage to the system, on the basis of agreed rules. These may not be possible in a software sense as monitoring that is external may be required. Ideally if this can be built into the system or by using smart contracts to provide more rapidity would be preferred, rather than system-wide change.

The resolution of conflict is critical to the stability and success of cryptocurrencies as evidenced by the forking experience. This is in part tied to the collective choice arrangements alluded to above. Disputes about breaches or unintended outcomes of embedded rules in software should be arbitrated rapidly and ideally by independent external parties. There are known crypto-technology platforms emerging for smart contract arbitration that could be used to resolve such breaches.

One of the problems with governance of cryptocurrency has been the unfettered right to organise into economic interest groups for voting or pooling resources for mining. Unlike other commons where some freedom needs to be granted by government to operate the commons with variation of rules, under public cryptocurrency there are few if any restrictions. There needs to be some restriction on rights to organise, for example for voting or combining mining power in pools above a certain concentration. This is difficult with external monitoring.
The instances of ‘nestled enterprises’ for mining or operator cooperatives that are created by the supplier of equipment and resources who also provide know how and favourable pricing to attract operators is commonplace. This creates clusters of economic interest that can usurp the goals of the commons. However, there may be situations where due to the diversity of environments (countries) in which cryptocurrencies operate that nested organisations may benefit the common good. This should be done with the caveat that it is constrained to balance the common good.

5 Conclusion

In the foregoing analysis of cryptocurrency, we identified a number of issues arising from failures in terms of manifested features and benefits promised; we also investigated the governance issues from a common’s framework following Ostrom (2012). We find that cryptocurrencies have been promoted from a social commons perspective able to operate independent of the traditional financial architecture of banks and governments. The plundering of the common good at the expense of the commons or people is not a new concept. Bollier (2002) suggests that governments have given away common resources such as mining rights over land, information or even university research to companies at the expense of taxpayers. But cryptocurrencies are proposed on the greater common good, as a ‘social commons’ with benefits that are often not attainable due to the design and or settings and or governance.

Hayek (2001) warns though that social justice is not of ‘innocent goodwill’ but rather an agreeance to the demands of a special interest group. It seems that cryptocurrencies are an example of what Shenfield (1980) suggest where the concept of social justice can be used to
play on our moral sensitivity. So in other words cryptocurrencies as a form of money appear to be operating as a market driven ‘commercial commons’ aiming to give power and profits to a few, and not living up to the claimed benefits of equality, ease of access and lower transaction costs. This equates to capitalism marketed as a social common good.

We analysed cryptocurrency as a common good perspective following (Hardin, 1968; Meyer and Huddon, 2018) and found a number of promises not met, many arising from issues that will effect confidence but most of all they relate to issues surrounding governance. We then considered how the governance and operations of cryptocurrencies that purport to be a form of money for the social commons be improved to operate that way. A fuller analysis of these failures is an area of further research that we suggest is needed but we have made some suggestions on progressing this using the theoretical framework of Ostrom (2005). Notwithstanding the criticisms of government fiscal policies, monetization of debt and management of fiat, future research may also reconsider fiat money as a common good given the shortfalls of the system it operates within by considering initiatives such as Central Bank Digital Currencies (CBDC).
References:


McCallum, T., & van der Laan, L. (2017) The blockchain could have better security than the banks. The Conversation, July 17.


Szabo, N (1994). Smart contracts. Unpublished manuscript


