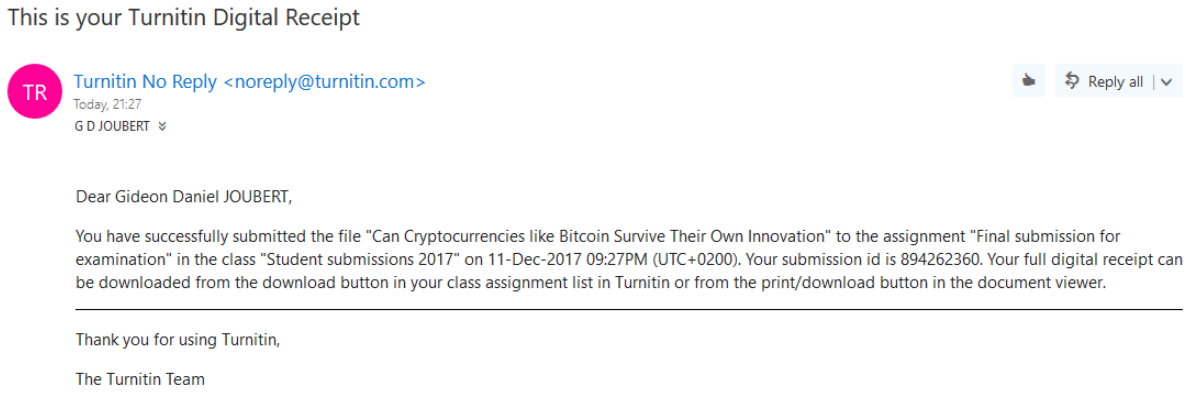
This is your Turnitin Digital Receipt

TR Turnitin No Reply <noreply@turnitin.com>
Today, 21:27
G D JOUBERT

Reply all

Dear Gideon Daniel JOUBERT,

You have successfully submitted the file "Can Cryptocurrencies like Bitcoin Survive Their Own Innovation" to the assignment "Final submission for examination" in the class "Student submissions 2017" on 11-Dec-2017 09:27PM (UTC+0200). Your submission id is 894262360. Your full digital receipt can be downloaded from the download button in your class assignment list in Turnitin or from the print/download button in the document viewer.

Thank you for using Turnitin,

The Turnitin Team

Can Cryptocurrencies like Bitcoin Survive their own Innovation?

Gideon D. Joubert

College of Economic and Management Sciences

University of South Africa

December 2017

Table of Contents

Can Cryptocurrencies like Bitcoin Survive their own Innovation?

Gideon D. Joubert

Abstract

Bitcoin is a decentralised electronic cryptocurrency which makes use of a public ledger system to record transfer of ownership. Since its launch in 2009 it has not been widely adopted for use in transactions, but rather for indulging in speculative activity. Although Bitcoin is a highly innovative creation, its future prospects are shrouded in uncertainty. Bitcoin offers its users numerous benefits, and the blockchain technology powering it may be useful in different applications. It also suffers from potentially serious pitfalls and weaknesses, which could erode and possibly destroy user confidence. If these issues remain unaddressed, they may threaten the continued existence of the platform. The association of Bitcoin with criminal activity and extreme price volatility has brought it to the attention of authorities worldwide that have adopted disparate approaches in regulating it. This paper discusses the strengths and weaknesses of Bitcoin, and what the future may hold for the cryptocurrency and its users. It is therefore difficult to come to any concrete conclusions pertaining to Bitcoin's future prospects. Depending on how the legion of challenges facing the cryptocurrency are dealt with, and whether or not the blockchain technology behind it receives widespread adoption, it can possibly have a very bright (or very bleak) future.

Introduction

The advent of Bitcoin back in 2009 as the first decentralised cryptocurrency was a historic event. The technology behind it is highly innovative to the point of being ground-breaking, and the potential for its use in the traditional banking sector has already been broadly noted. Like all technologies, cryptocurrencies will also continuously evolve and adapt with time as new solutions to existing problems are found.

As pioneering and potentially useful as it is, Bitcoin has also saddled us with an interesting conundrum.

The very nature of the technology and the accompanying anonymity of the userbase presents numerous inherent risks that may negatively affect consumer confidence in the platform, varying from problems involving criminal activity, to regulatory challenges, to consumer protection. Considering the various threats and challenges facing Bitcoin, it is obvious that its future existence is not a matter of certainty. A deeper investigation into existing problems, the current and possible future approaches to solving them, and the impact of this on its future is needed. Will the advantages offered by Bitcoin outweigh its tribulations in the long-run?

The main objective of this research is to investigate Bitcoin's advantages and shortcomings, and the potential effects to its future viability. The discussion begins with a description of Bitcoin and how it works, followed by whether or not it can be defined as money. Threats facing Bitcoin and its users are then dealt with, before moving on to a study of Bitcoin's advantages. Finally, conclusions are drawn regarding the future of Bitcoin after an examination of its prospects and pitfalls.

Literature Survey

Bitcoin's entrance unto the world stage has been a momentous and disruptive event. The cryptocurrency has disciples and detractors from a broad cross-section of society, and the media regularly publishes pieces weighing-up the pros and cons applying to it. The only aspect on which there appears to be unanimous agreement is that Bitcoin, and the technology powering it, is a highly innovative phenomenon with potentially far-reaching implications.

1 What is Bitcoin?

Bitcoin is an Internet-based cryptocurrency that makes use of a decentralised public ledger, known as the blockchain, to record transactions between user addresses. The ledger is decentralised in the sense that users are spread throughout the Bitcoin network. Users are divided into ordinary buyers and sellers of bitcoin and node operators. The latter span the globe and independently work on "assembling" transaction blocks that make-up the blockchain. In order for a block of transactions to be added to the blockchain, there must be a consensus between all the individual nodes that make up the network that the transactions contained within that block are indeed valid and correct. Because the ledger is decentralised, there is no central authority with the final say in validating a new block, which makes fraudulent transactions much more difficult.

Each Bitcoin user address has its own unique public and private key pair, which are used to enhance the safety and anonymity of transferring Bitcoins between transacting addresses. The Bitcoin is in essence a container of value. Each transaction includes a digitally signed hash of the entire transaction history of that particular Bitcoin, which can be used to verify the origin of the spent Bitcoin, and so confirm the transaction's validity. Every transaction is incorporated into a block which is then broadcast to the entire Bitcoin network, and miners then use their computing power to solve a difficult cryptographic problem in order to add the block to the blockchain. The completed block comes with its own hash-based proof-of-work, which is used by the network to publicly verify the validity of the transactions. The miners in turn are rewarded with Bitcoin and any included transaction fees for their labour. A new block is added to the chain every 10 minutes.

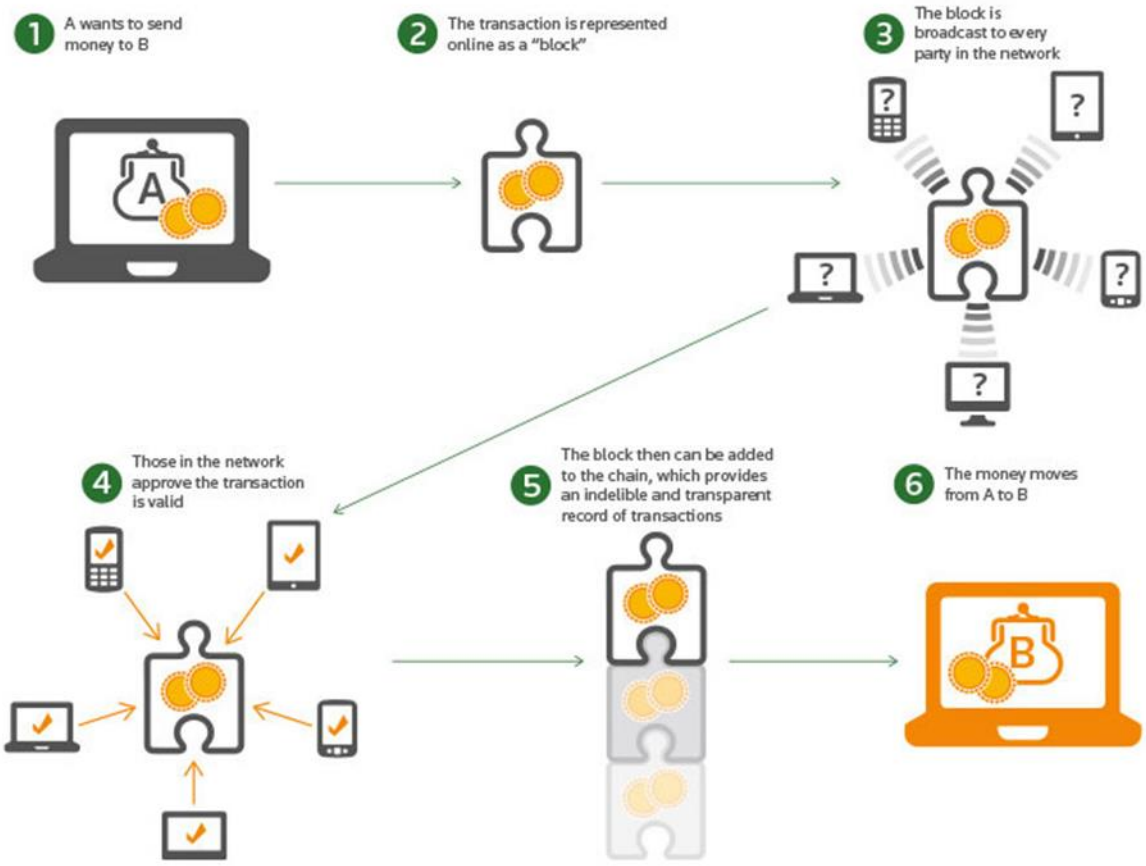

FIGURE 1: HOW THE BITCOIN BLOCKCHAIN WORKS (GRAPHIC SOURCED FROM REUTERS)

Zohar (2016) explains that Bitcoin's core mechanism is governed by two rules: 1) Block creation is designed to be difficult and resource-intensive, and 2) the longest chain must be adopted in order to resolve conflicting transactional histories. For every block that is added to the blockchain, the miner will be required to use a large amount of computing power, which in turn will consume a significant amount of electricity. The two most obvious costs to a miner will be the investment in specialised Bitcoin "mining" equipment (normal desktop computers do not possess the required processing capability to profitably mine Bitcoin), and the significant cost of consumed electricity. The purpose of making blockchain creation difficult and resource-intensive is to limit the ability of any single miner to obtain sufficient computing power which will allow them to influence the network. This prevents malicious behaviour which could compromise the integrity of the blockchain. The reason why the longest chain is adopted in the event of a blockchain fork occurring, is due to the longer chain having a more protracted and consistent history of node consensus: it is more efficient and rational to discard the blocks in the shorter chain, adopting the longer chain, and then adding transactions on the ledger from there onwards.

Bitcoin has a fixed supply of coins that can be mined which is set at 21 million, and the supply will be exhausted in 2040. The potential size of the blockchain is also limited: there is an ongoing wrangle between various camps within the Bitcoin community on the future scaling of individual blocks, and the blockchain itself. This debate, described by the Economist (2017) as a "bitcoin civil war", involves prioritising the security and integrity of the network versus safeguarding future viability. Either way, once whichever limit is reached, it is uncertain what type of incentive system will replace the existing one. This may prove to be a significant challenge to the network, as explained by Evans (2014).

The users of Bitcoin appear to fall into two distinct categories according to Yermack (2013): technology enthusiasts who embrace the platform with the hope that it develops into a sustainable vehicle for online commerce, and those with pseudo-libertarian beliefs to whom Bitcoin's lack of any connection to a central authority or government appeals. We should include two further categories: those who hold Bitcoin for speculative investment purposes, and those who use it for illicit purchases and other criminal activities due to the pseudonymity offered by the platform.

Before any meaningful discussion pertaining to the future of Bitcoin can be had, it is important to answer the question regarding its definition, and whether or not it is money.

2 Is Bitcoin Money?

Considering the controversy surrounding Bitcoin, it should not be surprising that there isn't even agreement as to what it should be defined as. According to conventional economic theory, for something to be defined as money, it must satisfy three criteria: it must be generally accepted as a medium of exchange, it must be suitable as a store of value, and it must function as a unit of account.

Bitcoin currently fails to adequately satisfy all three aforementioned attributes.

2.1 Generally Accepted Medium of Exchange

Money is generally accepted as a medium of exchange when all economic agents, within a specified economic space, accept it in exchange for goods and services. Even though Bitcoin is accepted by an ever-growing number of vendors in exchange for goods and services, its transactional usage appears to be so small as to be negligible. Ali et al (2014) estimate that a maximum of 20 000 residents in the UK have a "significant holding" of Bitcoin, and as few as 300 transactions per day occur. They further calculate that in 2014 there were only about 1 transaction per 65 Bitcoin wallets held at "My Wallet", a Bitcoin wallet-hosting service. According to Ali et al's (2014) research it would appear that the majority of Bitcoin users are holding the cryptocurrency with a speculative motive as opposed to using it for transactions.

Yermack (2013) supports this assertion with the estimate that approximately 80% of activity on the Coinbase digital wallet service is related to speculation. It is derived from this estimate that only about 15 000 daily Bitcoin transactions involve the purchase of goods or services: a minuscule and insignificant amount.

The IMF (2016) notes that the total market value of Virtual Currencies, including Bitcoin, is approximately US$7 billion, which is negligibly small when compared to the amount of US currency in circulation which stands at around US$1,4 trillion.

Work done by Glaser et al (2014) emphasises the high exchange rate volatility experienced by Bitcoin, and that this is indicative of it being held as a speculative asset instead of being utilised as an alternative transaction system.

The research provides strong evidence that new users tend to limit their transactions to trading on Bitcoin exchanges, and so-doing primarily view Bitcoin as an alternative investment vehicle.

2.2 Store of Value

According to Mandjee (2015), for something to be considered a store of value it must "retain its purchasing power over time with a good deal of certainty". A problem faced by Bitcoin in this regard is the extreme price volatility experienced by the cryptocurrency. Bitcoin is described as a fiduciary currency by Velde (2013) since there is no asset backing its value, and it therefore has no intrinsic value. Instead Bitcoin's value derives from the belief that other people will be willing to accept it as a form of payment or otherwise. All fiat currencies are fiduciary currencies, but what is unique about Bitcoin among fiduciary currencies is that it has no statutory backing in the form of being the officially recognized legal tender of some jurisdiction. Bitcoin is not a government-backed fiat currency. As a result, its value is strongly influenced by expectations and opinions about its future demand. Ali et al (2014) explain that these beliefs and opinions make it practically impossible to nail down Bitcoin's value, resulting in significant volatility. The authors argue that Bitcoin's volatility, which has been up to 17 greater than that of the Sterling, makes it a very poor short-term store of value, and that its prospects in the medium and long-term are as of yet unknown. Other issues also come into play in this regard. Yermack (2013) notes that the lack of security and deposit insurance provided by digital wallet services exacerbates Bitcoin's store of value problem, since users cannot be assured that their Bitcoin holdings will be safe from theft.

2.3 Unit of Account

A unit of account is a function of money which provides measurement for defining, comparing, and recording value. At present there is little evidence of retailers quoting their prices in Bitcoin: prices are usually denominated in national fiat currencies and Bitcoin is only used as a payment system, similar to the functioning of credit cards, to facilitate the transaction. Ali et al (2014) assert that retailers who do quote their prices in Bitcoin, would update the prices at high frequency in order to preserve stable prices when they are expressed in fiat currency. This is again a consequence of Bitcoin's extreme volatility.

An additional problem inhibiting Bitcoin's usefulness as a unit of account, described by Yermack (2013), is the relatively high cost of one Bitcoin when compared to the cost of

goods and services. This results in vendors having to quote their Bitcoin prices with up to four decimal spaces, which is grossly impractical.

2.4 Conclusions

It is obvious that Bitcoin fails to meet the requirements of the definition of money. The IMF (2016) states that Bitcoin fails to adequately satisfy both the legal and economic concepts of money. Instead Bitcoin is defined as a digital representation of value, and classified as a so-called Virtual Currency. The SARB (2014) classifies Bitcoin as a Decentralised Convertible Virtual Currency that is not legal tender.

Since Bitcoin is not backed by any government authority or redeemable for any commodity, there exists a problem of trust. Turpin (2014) explains that although it may be difficult to entice users to convert significant amounts of their wealth into Bitcoin for this reason, supporters of the cryptocurrency claim that its intrinsic value is no different to that of government-issued fiat currency, whereby they ignore the fact that fiat money is characterized not only by a lack of intrinsic value but also by being declared legal tender by some government. And the legal tender status of a money is surely a strong foundation for its general acceptance in exchange for goods; people would break the law if they reject it. Proponents like Gavin Andresen (as referenced by Turpin) further argue that Bitcoin is in fact closest to so-called “pure currency” due to its value deriving solely from its suitability as a medium of exchange. As previously noted, this claim appears to be dubious at best. Apart from the difficulties which undermine the potential use of Bitcoin as currency, there are additional threats and risks that impact its users. These hazards serve as further inhibitors of Bitcoin being more widely adopted, and could threaten the long-term existence of the cryptocurrency.

3 Threats and Risks to Bitcoin and its users

Bitcoin’s existence is dependent on maintaining the trust of its users and satisfying the requirements of regulators. In the case of the former, trust can be eroded by excessive value fluctuation, theft and fraud propagated through the platform, or the emergence of superior competitors.

Regarding the requirement of satisfying regulators: if governments believe Bitcoin poses a threat to the effectiveness of their monetary policy, or that it is significantly used to finance illicit activity, it could potentially be regulated into extinction.

Grinberg (2012) discusses numerous threats to user confidence. One such a threat involves the developers using their discretionary authority improperly to change the inflation rate, which can result in users abandoning the platform in panic due to a massive loss of confidence. Other serious threats include a superior competitor emerging from the fold, a crackdown by governments, anonymity failure, theft, and denial of service. All of these can potentially bring the network to its knees if user confidence is sufficiently shaken.

Bitcoin grants its users many potential benefits, but the cryptocurrency also faces numerous serious challenges that not only inhibit its potential acceptance as a fully-fledged digital currency, but that may also prove to be life-threatening to Bitcoin's future existence. These challenges deserve to be discussed in turn.

3.1 Volatility

As briefly touched upon, the extreme price volatility experienced by Bitcoin is a serious inhibitor to its use as currency, but it also poses a definite threat to those who hold it even speculatively. Ali et al (2014) mentioned Bitcoin being up to 17 times as volatile as the Pound Sterling. Yermack (2013) notes that Bitcoin in 2013 experienced 142% exchange rate volatility, which is extreme when compared to other currencies, which typically fall between 7% and 12%, and even gold, which had a 2013 dollar-denominated volatility of 22%. Even though Bitcoin is the most stable public ledger currency, it is still more than 18 times as volatile as the Euro, as noted by Evans (2014).

The causes of Bitcoin's price volatility are myriad, but Turpin (2014) singles out two factors: no widespread adoption by consumers and acceptance by merchants, and high levels of speculative activity. Turpin does note that volatility has been declining, while remaining significant.

A positive correlation between price risk and price development is noted by Glaser et al (2014), which brings them to conclude that the Bitcoin ecosystem is currently experiencing an asset bubble: a potentially very dangerous consequence of the cryptocurrency's volatility.

3.2 Criminal Activity

Due to the pseudonymity features associated with Bitcoin, it is potentially very attractive to criminals. Illicit activity associated with Bitcoin include fraud, money laundering, illicit purchases, and tax evasion.

3.2.1 Theft and Fraud

Users are at risk of having their Bitcoins stolen from both online wallet services, as well as the wallets they store on their personal computers. Turpin (2013) mentions numerous thefts, noting one online wallet service which was robbed of more than $12 000 by hackers due to insufficient security. Even service providers have been guilty of stealing from their own clients, as was the case with Bitcoinica, and Ponzi schemes have tricked many users into parting with their Bitcoin holdings for dubious “investment” purposes, such as the scam perpetrated by BST which misappropriated an estimated 500 000 BTC (Turpin 2013: 347).

3.2.2 Money Laundering

A node is any computer that shares blocks and transactions across the Bitcoin network. Bitcoin consists of a decentralised network of nodes that provide pseudonymity (the addresses of transactions are open for all to see on the public ledger) and does away with the requirement of a trusted third-party (the banking system in traditional payment systems). This results in none of the transactions being overtly tied to any person’s identity, which in turn makes it attractive for criminals to hide money laundering activity as explained by Troeller (2016). In order for money to be laundered, three steps must be followed: 1) placement - the injection of the “dirty” money into the financial system; 2) layering - by transferring or converting the “dirty” money, it is disconnected from its illicit source; 3) integration - the laundered money re-enters the financial system as “clean” money. These money laundering processes are significantly enhanced by cryptocurrency, as explained by Marshall (2016): Bitcoin allows international transfer of money at near-instantaneous velocity at very low cost, whilst allowing the users to remain anonymous. Money launderers can thus move their illicit funds faster, cheaper, and more discreetly than previously. Users can also hide their laundering activity by transferring Bitcoin through endless numbers of nodes before converting it back into fiat currency.

3.2.3 Illicit Purchases

Silk Road, the now-defunct online market for a wide range of illicit goods and services, accounted for a large part of the total Bitcoin circulation. Yermack (2013) estimates up to half of all early Bitcoin transactions went through Silk Road. Drugs, explosives, firearms, child pornography, and other illicit goods and services were purchased on Silk Road in exchange for Bitcoin, which left a stain on the cryptocurrency's reputation that has not as of yet completely vanished. According to Turpin (2014), Silk Road's success was directly dependent on the perceived anonymity its users enjoyed, which was achieved through two technologies: TOR, and online network that hides users' locations and identities, and Bitcoin. The FBI did succeed in shutting-down Silk Road and arresting its founder, Ross Ulbricht, but the agency had to resort to more traditional policing methods and techniques to achieve the result (Turpin 2014: 358-359).

3.2.4 Tax Evasion

Mandjee (2015) elaborates on the possibility that, due to the perceived difficulties of tracing virtual currencies like Bitcoin, they can be used as a sort of virtual tax haven. Franklin (2016: 82) states that Bitcoin presents users with a notable opportunity to perform transactions that are obfuscated from tax reporting. Due to the difficulty of regulatory authorities reaching any sort of consensus regarding the tax status of Bitcoin, there may exist a tax-free arbitrage advantage in making use of Bitcoin.

3.3 Risks to Stability

Bitcoin's lack of any central monetary authority, combined with its finite predetermined amount of mineable Bitcoin, opens the door to the possibility of a deflationary spiral. Turpin (2014) notes that as the rate of Bitcoin mining declines, some holders of the cryptocurrency may decide to hoard them in the hopes of deflation occurring. This hoarding of Bitcoins combined with a finite supply (and Bitcoin being mined at a decreasing rate as time goes on) will lead to a reduced velocity of circulation as users increase. This will in turn lead to deflation, and possibly even a deflationary spiral unless merchants counter it by fixing their prices in other currencies whilst accepting Bitcoin at a fluctuating rate.

The collapse of MtGox, the biggest Bitcoin exchange, in February 2014 resulted in the loss of over 850 000 Bitcoins, valued at approximately $450 million.

Mandjee (2015) notes Warren Buffet's response to the event which was to state that "Bitcoin does not meet the test of a currency." If Bitcoin is to retain the confidence of its users, the collapse of large exchanges must be avoided.

3.4 Collusion Between Miners

Another significant risk is if any single miner achieves 51% or more of the computing power on the network, putting it in danger of a so-called 51% hash power attack. Controlling 51% of the network's computing power allows a miner to create blocks faster than all the other nodes together, which would allow it to alter the blockchain and double-spend any transaction it issued, regardless of how far back down the chain it occurred. Zohar (2015: 109) explains that a miner with such control can cripple the entire Bitcoin network by issuing empty blocks that fill the blockchain, effectively blocking all transactions from taking place. The pooling of computing resources by mining cartels may compromise the integrity of the entire Bitcoin network if any of them come close to controlling 50% of the platform's computing power. GHash.IO is a popular mining pool that on several occasions came close to producing 50% of the network's hash rate, and after a public outcry opted to restrict their computational power voluntarily (Zohar 2015).

Gervais et al (2016) explain that the computing power of dedicated miners far exceeds that of individual users, and that more than 50% of Bitcoin's computing power is concentrated to the three largest mining pools, which are centrally managed entities. Gervais argues that mining and block generation are certainly not the decentralised activities as originally intended. The significance of this is that Bitcoin relies on decentralisation of computing power to maintain the integrity of the system in order to prevent a single miner or cooperative cartel from achieving enough computing power to alter the blockchain - integrity in the sense of resisting double-spending attacks and other forms of dishonesty.

The reason for miners pooling their resources lies in the high cost of participation and the highly competitive nature of the activity, which limits the chances of any individual miner in being successful and receiving a payout.

Gervais estimates that approximately 75% of all computing resources on the Bitcoin network are concentrated in the possession top six mining pools. Collusion and cartel behaviour are therefore certainly not impossible, and may even be plausible.

3.5 Coin Tainting

Due to all Bitcoin addresses being publicly visible, it is possible to track the spending of individual Bitcoins. This attribute allows for any entity with the desire to do so to target a specific set of addresses and "taint" the coins associated with them. Gervais (2016) explains that this is achieved when users stop interacting with a specific address on the network, and in so doing deflate the value of the coins they hold. Even though this process was justifiably employed by MtGox following the theft of 43 000 BTC from Bitcoinica by locking accounts which received tainted coins, there is a danger that government pressure and social activism can result in addresses being targeted for more sinister purposes than enacting justice. Developers also have the ability to block addresses from performing any transactions by hard-coding a list of banned addresses with every Bitcoin address release. Whilst this can be useful in combating criminal activity on the network, it is a double-edged sword which can also be employed arbitrarily with little chance of recourse for affected parties.

3.6 Government Regulation

Governments reserve the right to regulate cryptocurrencies through numerous channels available to them, but regulatory approaches have widely varied between nations.

The IMF (2016) acknowledges that cryptocurrencies do not readily fall into traditional regulatory models, mostly due to their decentralised nature. The central intermediary (the banking system) is traditionally the focal point of any regulation, and Bitcoin has effectively done away with such an entity. This presents a challenge to policymakers regarding who to regulate, and the existing trend is for national authorities to focus on Bitcoin market participants and the financial institutions that interact with them. The IMF (2016) notes that the effectiveness of any regulation will be dependent on how the cryptocurrency market evolves, as well as how policy responses are developed and coordinated internationally. The IMF does not consider cryptocurrencies a threat to monetary policy effectiveness due to them not being widely used as medium of exchange as of yet, and because they will not easily be able to replace the lender of last resort function of central banks. The IMF recommends that any regulation should aim to minimise risks without stifling innovation.

The BIS (2015) mentions that it would require widespread success and acceptance of cryptocurrencies as an alternative medium of exchange, in order for them to threaten monetary policy effectiveness.

The BIS explains that the borderless online nature of digital currencies like Bitcoin serves to complicate the matter of their regulation. Their belief is that regulation should cover three main fields: consumer protection, prudential rules for the different stakeholders, and specific operating rules as payment mechanisms. The BIS has identified 5 categories of regulatory action: 1) moral suasion (like public warnings, buyer information, and research papers); 2) specific stakeholder regulation (regulation of exchanges and administrators, and consumer protection initiatives); 3) interpretation of existing regulations; 4) overall regulation (covering all three main fields); 5) prohibition.

According to Macurak (2014) only four countries have explicitly regulated Bitcoin: China, Japan, Thailand, and Brazil. The responses contrast sharply – in China the cryptocurrency remains in a legal grey area, but the authorities have banned initial coin offerings (ICOs) and cracked down on Bitcoin exchanges since September 2017 (Parker 2017). Thailand has taking a prohibitionist stance and banned banks from using Bitcoin in totality, whilst Brazil have opted to normalise the use of the cryptocurrency. Many European nations subject Bitcoin exchanges to VAT, and Japan considers it a taxable commodity after the collapse of MtGox. Japanese authorities have additionally prohibited banks from trading Bitcoin and securities brokers from brokering on Bitcoin exchanges. Germany and Iceland treat Bitcoin as foreign currency.

US regulations are less clear (Macurak 2014). Regulating authorities appear to have adopted a wait-and-see attitude in order to quantify the long-term effects of Bitcoins existence before formulating explicit policy. The existing federal and state statutes are a quagmire of conflicting interests between the various agencies combined with legal grey areas. The only laws that have been confirmed as being specifically applicable to Bitcoin is the Federal Tax Law and the Bank Secrecy Act. The former requires reporting of any gains made from Bitcoin exchange activities, and the latter pertains to the obligation of exchanges to register with FinCEN, to develop anti-money laundering programs, and to identify all their customers. The fact that there is no clarity regarding the powers existing laws grant regulatory agencies in the United States has led to marked negative effects on Bitcoin users in the county. The development and enforcement of US regulation is still in process and any final outcome is yet to be determined.

Hostile government regulation has the potential to be fatal to Bitcoin's prospects in achieving mainstream success, but it is dubious as to whether regulation will be any more effective at killing the cryptocurrency than existing laws have been at stopping the trade in contraband.

The reality of the situation is that it would be in everyone's best interest for regulations to be workable, equitable, and effective in achieving their desired results.

4 Benefits of Bitcoin

Despite the numerous and significant potential pitfalls suffered by Bitcoin, it does succeed in presenting its users with some noteworthy advantages.

4.1 Lower Transaction Costs

Bitcoin has succeeded in significantly lowering transaction costs: there is no trusted third-party – the banking system in traditional payment systems – that requires compensation for its services, and Bitcoin miners are already rewarded for the work they do.

There is another side to this benefit, however. Turpin (2014) discusses the phenomenon of lower transaction costs drawing new customers into the virtual currency market, but that they may be woefully uninformed about the risks and dangers of putting their wealth into the platform. Kasiyanto (2016) explains that Bitcoin provides its user base with borderless and low-cost transactions, with average costs being merely 0,9% of the transaction value. It is precisely these attributes that make Bitcoin ideal for cross-border remittances, although the degree to which it will be adopted for this role remains to be seen.

4.2 Anonymity

Perhaps one of the most controversial aspects of Bitcoin is the alleged anonymity it offers users. It would be more accurate to refer to it as pseudonymity, considering that there have been successful attempts at identifying Bitcoin users via their public addresses. Glaser (2014) mentions previous work which succeeded in passively mapping Bitcoin addresses and then identifying a large number of users.

Further work by Meiklejohn et al (2016) erodes the perceptions of anonymity even more. They collected data and proceeded to "tag" as many addresses as possible. This was achieved by labeling addresses where the real-world user is readily identifiable. Much of this tagging was achieved by simply transacting with users. Tagged addresses were clustered into groups of shared attributes, like mining pools, wallets, exchanges, vendors, and so on.

Through the use of two heuristics, they managed to identify several users behind supposedly anonymous Bitcoin addresses, including ones involved in illegal activity. This allowed theft of Bitcoin to be tracked, regardless of the sophistication of the techniques employed by criminals in an attempt to hide their activities and identities. Meiklejohn et al (2016) note that, even with their limited time and resources, they managed to achieve astounding success at removing anonymity from the Bitcoin network, and that it would require considerable more effort from users to effectively hide their identities.

It is therefore clear that the perceived anonymity offered by Bitcoin is not as robust as first believed, and that government agencies can certainly defeat it for the purpose of law enforcement by simply devoting sufficient resources to their efforts.

5 Adoption of Bitcoin, its technology, and future prospects

Opinions on what the future prospects of Bitcoin and the technology behind it may be are diverse.

There is little empirical evidence in support of claims that Bitcoin is becoming more widely adopted as a medium of exchange (Evans 2014). It has not exhibited the typical “hockey stick” growth path of its transactions associated with successful platforms like mPesa, a Kenyan person-to-person payment system. Such a growth path would involve slow growth initially until a point of critical mass is reached, upon which growth would rapidly accelerate. Bitcoin’s volume of transactions has remained stable and low since its inception, which ties in to our earlier conclusion that it is primarily held as a speculative asset, and not for transactional purposes.

Evans (2014) argues that it is highly unlikely that distributed public ledger currencies like Bitcoin will evolve into general purpose use, based on several findings. Firstly, the protocols governing coin supply are inflexible and do not adjust supply with demand, and therefore no stable values for the coins can be provided. Secondly, due to the unstable value of Bitcoin, it is unlikely that it will be widely adopted by users for transaction purposes. Lastly, more than five years after inception there is no empirical evidence supporting claims that Bitcoin is generally accepted as a medium of exchange, and its use remains niche.

Kasiyanto (2016) also acknowledges that Bitcoin has a long way to go before it can be considered mainstream. He notes that the two primary inhibitors of Bitcoin’s general adoption

are the security problems affecting it, and the high volatility of its value. In order for Bitcoin to appeal to the mainstream, the platform must provide adequate security in both the technical and perceived realms (the latter referring to the perceptions of users regarding the integrity and security of the Bitcoin network and its exchanges), provide adequate consumer protection, be user- friendly, and address the issue of legal compliance. Kasiyanto notes that Bitcoin's vulnerable ecosystem and unstable price will be difficult to overcome, and that the shallowness of the market and users' dependence on exchanges further exacerbate problems of market and counter-party risk. Notably, 45% of exchanges ceased operations after suffering a major security breach, and 46% of them provided no reimbursement to affected users. Kasiyanto concludes that Bitcoin has incredible potential, but the obstacles the platform must overcome to achieve mainstream acceptance are significant.

There are also other inhibitors to Bitcoin's future success potential. The BIS (2015) lists numerous supply and demand side factors that have potentially negative influence on Bitcoin's future development. Fragmentation, considering that there are over 600 digital currencies in circulation, problems with scalability and efficiency, the hazards of pseudonymity, numerous technical and security concerns, and uncertainty about its business model sustainability in the long-run are all significant obstacles Bitcoin has yet to overcome. They conclude that significant developments are required before any meaningful increase in the use of digital currencies like Bitcoin can be expected.

Not all researchers have as pessimistic an outlook regarding Bitcoin's prospects as a currency. Zohar (2015) notes that early adopters of Bitcoin suffered being on the negative side of the network effect. Network effects are the result of the value of a good or service being dependent on the amount of people using it, and that money's value as a medium of exchange hinges on it being generally accepted by others as payment. This results in users having very few places at which to spend their cryptocurrency. The failure of exchanges and regulatory uncertainty also took their toll, but despite the aforementioned problems there is evidence of Bitcoin acceptance slowly increasing. More exchanges that trade Bitcoin for domestic currency have appeared, ATMs that dispense Bitcoin have popped-up, and digital wallet applications have become more user friendly and widespread.

Regarding the adoption of the distributed ledger technology, the IMF (2016) remarks that there are several emerging uses for the technology. Money-transfer start-ups have been known to embrace the technology, and that even established financial institutions have begun investigating ways in which to apply it to their operations in order to take advantage of the efficiency it offers.

This is due to the advantages offered by distributed ledger technology, such as a notable reduction in cost of international transfers, shortening of the time required to settle securities transactions, and enhancement of the transparency and back-office functioning of securities dealers. Luther (2016: 400-401) mentions that the long-term trend of digital payments increasing their share, and the potential cost benefits of using blockchain technology in payment systems, could make it attractive for financial intermediaries. At this point it is uncertain as to whether or not the implementation of such technology is viable or even advantageous over currently used centralized systems. However, considering that these institutions (including some central banks) are spending resources and time on research and development to adapt blockchain technology to their specific needs, it is likely that there may be noteworthy competitive advantages in implementing such systems. This forms the basis of the IMF's conclusion that distributed ledger technology may cause significant structural shifts in the financial industry.

Ali et al (2014) are of the opinion that many new technologies take a significant amount of time to manifest their productivity gains after first being introduced. They foresee the possibility that the distributed ledger may be applied on a broader scope than just payment systems, and that it is theoretically possible for the existing financial system's infrastructure to be replaced by distributed systems. There is thus reason to believe that the technology may have wider appeal than initially thought, although any significant developments in this regard may take considerable time to come to fruition.

Luther and White (2014) attempt to answer the question of whether or not Bitcoin has the potential to become a major currency. They note that the inelastic supply and volatile demand combined cause Bitcoin to be far more volatile than any other established currency, but that it may be rescued from obscurity and speculators via entrepreneurial innovations, such as market exchange pricing and instantaneous exchange facilities, which would allocate speculative risk to those wishing to hold it whilst enabling Bitcoin to be used as a medium of exchange. Market exchange pricing allows retailers to set their prices in one currency (such as ZAR) while simultaneously displaying them in other currencies (like Bitcoin) at current market exchange rates. Instantaneous exchange facilities in turn allow retailers to have their customers pay in Bitcoin without the vendor having to accept Bitcoin: a payment service provider takes the Bitcoin and pays the retailer in actual currency. Hence the retailer is not exposed to any exchange rate risk.

In later work, Luther (2016) explains that opinions regarding the future prospects of Bitcoin are diverse. Some commentators mentioned by Luther (2016: 397), such as Jennifer Calvery of the Financial Crimes Enforcement Network, believe that Bitcoin can turn out to be a "major player in the financial system." Other observers believe that the blockchain technology employed have far-reaching potential, but aren't overly optimistic regarding Bitcoin's prospects. Still others, such as Paul Krugman, consider Bitcoin as nothing more than a solution to "an interesting information problem", but he has reservations as to whether solving the problem will have "any economic value".

Luther considers the incumbent-monies problem, the fact that everyone is already using money and that switching to Bitcoin represents a cost, as the biggest obstacle to Bitcoin's general adoption. Switching costs and network effects favour the status quo according to Luther. Switching costs pertain to the price paid for switching from incumbent money to Bitcoin, such as menu costs. The fact that incumbent money is government-sponsored legal tender further exacerbates the incumbent-monies problem.

Competition from other cryptocurrencies also present a threat to Bitcoin's future prospects. However, any competitor will have to overcome Bitcoin's first-mover advantage, which is calculated to be quite substantial due to Bitcoin's approximately 85,6% market share. If a competitor is capable of offering a superior product at a lower or similar price, it may allow them to enjoy a second-mover advantage over Bitcoin.

Luther (2016) declines to attempt any prediction of Bitcoin's future, but he does offer a few interesting forecasts. The share of electronic transactions will very likely continue to increase, as smartphones are more widely adopted and innovations allow even small vendors to access electronic payments. Blockchain technology is likely to be adopted more widely in order to process digital payments, considering how it lowers transaction costs and offers a potentially large switching benefit, which is due to the high volume of transactions being processed by each payment processor and that payment processing is a highly concentrated activity. This has already manifested in some businesses taking steps to embracing the technology, such as NASDAQ. Luther notes that Bitcoin will likely only function as niche money, but that it may be widely adopted by the population of countries with a weak currency. Luther concludes that even though he is excited by the prospects offered by blockchain technology, he is not optimistic that Bitcoin itself will manage to achieve widespread acceptance.

My own opinion regarding the future of Bitcoin is a mixed one. I fully appreciate the potential value of blockchain technology, as well as the advantages offered by Bitcoin's low transaction costs and pseudonymous cross-border transfer of wealth. That being said, I harbour serious concerns regarding its recent price movements. In the beginning of 2017 the price of a Bitcoin was just under $1000. As of December 2017 its price has rocketed to more than $16000, with a marked increase in volatility. The price (and its volatility) has potential for further upward surges if the NASDAQ goes ahead with planned Bitcoin futures contract offerings in 2018. Meanwhile, commentators have compared Bitcoin to asset bubbles such as Tulip Mania, the DotCom bubble, and the US Housing bubble. Time will tell if it is indeed an asset bubble waiting to pop, or if we are witnessing the price discovery of Bitcoin's true value. Ironically, the very price increases that are making investors euphoric also serve to inhibit Bitcoin from achieving its designed purpose to become a generally accepted medium of exchange. The challenges that Bitcoin will have to overcome to achieve broad acceptance are certainly noteworthy. However, the fact that large financial institutions have expressed interest in blockchain technology and the use of public ledgers may prove significant.

Conclusion

Since this paper is a literature review, my conclusions flow from what can be intelligently gleaned from the various sources consulted. The most obvious shortcomings of this method are that there are not only numerous other studies that were not consulted, but also that important new developments pertaining to Bitcoin occur almost weekly. This paper attempted to compensate for this backward-looking characteristic by gravitating to what could be considered the main factors that determine the cryptocurrency's future prospects. Bitcoin is an innovative concept. Although it fails to satisfy the requirements to be considered money, it is accepted by a growing number of online vendors as payment for goods and services. However, the vast majority of Bitcoin holders use the currency for purely speculative purposes, an attribute which is both a product and a consequence of Bitcoin's extreme volatility. This volatility, combined with other serious risks to the currency's users like criminal activity and coin tainting, have drawn regulatory attention from authorities. At present there is no uniform approach to how governments are attempting to regulate Bitcoin, with some taking a permissive stance and others a prohibitive one, and the process of choosing a desirable form of regulation is ongoing. It is highly unlikely that Bitcoin would be regulated out of existence, if the IMF's guidelines are adhered to. The most significant threat to Bitcoin's future would be a significant loss of user confidence, either due to the numerous unaddressed

consumer protection and security concerns and extreme volatility, or by the emergence of a superior competitor which relegates it to obsolescence. There are also serious concerns about how it would handle diminishing mining profitability and cartel behaviour, as well as the potential deflationary pressures due to mining activity releasing diminishing numbers of Bitcoin into the network. Since Bitcoin is decentralised, it does not appear to have any obvious capacity to adequately formulate policy in response to these issues. The future of Bitcoin remains uncertain, but the blockchain technology powering it may have a very bright future outside the realm of cryptocurrency as suggested by the fact that financial institutions begin to adapt and adopt it.

References:

Ali, Robleh, John Barrdear, Roger Clews & James Southgate 2014. Innovations in payment technologies and the emergence of digital currencies. *Bank of England Quarterly Bulletin*, 2014 Q3: 262-275. Bank of England.
https://my.unisa.ac.za/access/content/group/ECS4864-17-Y1/Ali.etal.2014.InnovPaymTechDigitalCurrencies.pdf
Last accessed 21 August 2017

Ali, Robleh, John Barrdear, Roger Clews & James Southgate 2014. The economics of digital currencies. *Bank of England Quarterly Bulletin*, 2014 Q3: 1-11. Bank of England.
https://my.unisa.ac.za/access/content/group/ECS4864-17-Y1/Ali.etal.2014.EconomicsofDigitalCurrencies.pdf
Last accessed 21 August 2017

BIS 2015. Digital Currencies. *Committee on Payments and Market Infrastructures*, November 2015. Bank for International Settlements.
https://my.unisa.ac.za/access/content/group/ECS4864-17-Y1/BIS.2015.DigitalCurrencies.pdf
Last accessed 21 August 2017

Blundell-Wignall, Adrian 2015. The Bitcoin Question. *OECD Working Papers on Finance Insurance and Private Pensions*, No 37. OECD Publishing.
http://dx.doi.org/10.1787/5jz2pwjd9t20-en

Evans, David S. 2014. Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. *Coase-Sandor Institute for Law & Economics Working Paper No. 685*. Chicago: University of Chicago.
http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2349&context=law_and_economics
Last accessed 21 August 2017

Gervais, Arthur, Ghassan Karame, Srjdan Capkun & Vedra Capkun 2014. Is Bitcoin a Decentralized Currency? *IEEE Security & Privacy*, Volume 12, Issue 3.
Last accessed 21 August 2017

Glaser, Florian, Kai Zimmermann, Martin Haferkorn, Moritz Weber & Michael Siering 2014. Bitcoin – Asset or Currency? Revealing Users' Hidden Intentions. *European Conference on Information Systems 2014*.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425247
Last accessed 21 August 2017

Grinberg, Reuben 2012. Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal*, Volume 4, p.160.
https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1817857
Last accessed 21 August 2017

IMF Staff Team 2016. Virtual Currencies and Beyond: Initial Considerations. *IMF Staff Discussion Note*, SDN/16/03. International Monetary Fund.
https://my.unisa.ac.za/access/content/group/ECS4864-17-Y1/IMF.2016.VirtualCurrenciesandBeyond.pdf
Last accessed 21 August 2017

Kasiyanto, Safari 2016. Bitcoin's potential for going mainstream. *Journal of Payments Strategy & Systems*, Volume 10, Number 1.
https://my.unisa.ac.za/access/content/group/ECS4864-17-Y1/Kasiyanto.2016.Bitcoin_sPotentialofGoingMainstream.pdf
Last accessed 21 August 2017

Luther, William J. 2016. Bitcoin and the Future of Digital Payments. *The Independent Review*, Volume 20, Number 3.

Luther, William and White, Lawrence C. 2014. Can Bitcoin become a Major Currency? *George Mason University Working Paper*, No.14-17. George Mason University. Last accessed 21 August 2017

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker & Stefan Savage 2016. A Fistful of Bitcoins: Characterizing Payments among Men with No Names. *Communications of the ACM*, Volume 59, Number 4.
https://my.unisa.ac.za/access/content/group/ECS4864-17-Y1/Meicklejohn.etal.2016.FistfulofBitcoins.pdf
Last accessed 21 August 2017

Macurak, Andrew B. 2014. Regulating Bitcoin. *Capstone Strategic Project for the American Bankers Association*, 1 April 2014. Stonier Graduate School of Banking.
http://www.abastonier.com/stonier/wp-content/uploads/2014-Macurak-Andrew.pdf
Last accessed 21 August 2017

Mandjee, Tara 2015. Bitcoin, its Legal Classification and its Regulatory Framework. *Journal of Business & Securities Law*, Volume 15, Issue 2.
http://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1003&context=jbsl
Last accessed 21 August 2017

Marshall, Russ 2015. Bitcoin: Where Two Worlds Collide. *Bond Law Review*, Volume 27, Issue 1.

South African Reserve Bank 2014. Position Paper on Virtual Currencies. *Position Paper*, number 02/2014. South African Reserve Bank.

Parker, Emily 2017. Can China Contain Bitcoin? *MIT Technology Review*
https://www.technologyreview.com/s/609320/can-china-contain-bitcoin/
Last accessed December 2017

Smit, JP, Filip Beukens & Stan du Plessis 2016. Cigarettes, dollars and bitcoins – an essay on the ontology of money. *Journal of Institutional Economics*, Volume 12, Issue 2.
https://my.unisa.ac.za/access/content/group/ECS4864-17-Y1/SmitBuekensDuPlessis.2016.Bitcoin.pdf
Last accessed 21 August 2017

The Economist, 2017. Making Bitcoin Work Better: a Crypto-Currency Civil War. *The Economist*, 27 July 2017

Troeller, Lauren 2016. Bitcoin and Money Laundering. *Review of Banking & Financial Law*, Volume 36, Issue 1. Boston University School of Law.
http://www.bu.edu/rbfl/files/2017/03/DA-13.pdf
Last accessed 21 August 2017

Turpin, Jonathan B. 2014. Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework. *Indiana Journal of Global Legal Studies* 21: 335-368.
http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1557&context=ijgls
Last accessed 21 August 2017

Velde, Francois R. 2013. Bitcoin: A Primer. *Chicago FED Letter No 317*. Chicago: Federal Reserve Bank of Chicago.
https://www.chicagofed.org/~/media/publications/.../cfldecember2013-317-pdf.pdf
Last accessed 21 August 2017

Yermack, David 2013. Is Bitcoin a Real Currency?: An Economic Appraisal. *NBER Working Paper* 19747. Cambridge (MA): NBER.
http://www.nber.org/papers/w19747.pdf
Last accessed 21 August 2017

Zohar, Aviv 2015. Bitcoin: Under the Hood. *Communications of the ACM*, Volume 58, Number 9.
https://my.unisa.ac.za/access/content/group/ECS4864-17-Y1/Zohar.2016.BitcoinUndertheHood.pdf
Last accessed 21 August 2017