2016

Bitcoin's Global Potential: Examining the Obstacles to Becoming a Legitimate Financial Tool

Nicholas J. Moorman
DePauw University

Bitcoin's Global Potential:
Examining the Obstacles to Becoming a Legitimate Financial Tool

Nicholas J. Moorman
2016

Larry J. Stimpert, Ph.D.
Sponsor

Jeffrey M. Gropp, Ph.D.
Committee Member

Douglas E. Harms, Ph.D.
Committee Member

Table of Contents

Chapter One
A Primer on Bitcoin

Bitcoin has garnered a great deal of attention in the last couple of years and not all of it good. Associations have been made between Bitcoin and numerous criminal organizations, including (but not limited to) terrorist groups, the Silk Road, and even Wall Street. These associations have not only tarnished Bitcoin's reputation, but increased its notoriety as well. The following section provides an in-depth analysis of the Bitcoin ecosystem.

More than anything, Bitcoin began as an idea in the fall of 2008. While the United States was embroiled in a financial meltdown, Satoshi Nakamato[1] published *Bitcoin: A Peer-to-Peer Electronic Cash System*. From this whitepaper, an idea emerged with potential to change global finance. A working perspective of Bitcoin (the ecosystem) requires an understanding of the relationship between the Blockchain and bitcoin (the currency).

The Blockchain

The Blockchain, considered the "main technological innovation" of Bitcoin, is a general ledger. Distributed across the Bitcoin network, the Blockchain "is downloaded automatically when the miner joins the network" (Swan 10). A blockchain serves the purposes of verifying a transactions over the untrustworthy medium of the Internet. Moreover, it allows for participants to agree on transactions without them needing to meet. In this manner, it decentralizes the entire process of transferring ownership from one person to another and provides a permanent record of transactions over the network. But how can one be sure that the general ledger is accurate and hasn't been tampered with?

[1] The anonymous creator of Bitcoin and author of *Bitcoin: A Peer-to-Peer Electronic Cash System*. While there has been much speculation into his or her identity all attempts in doing so are speculation.

The Byzantine General Problem

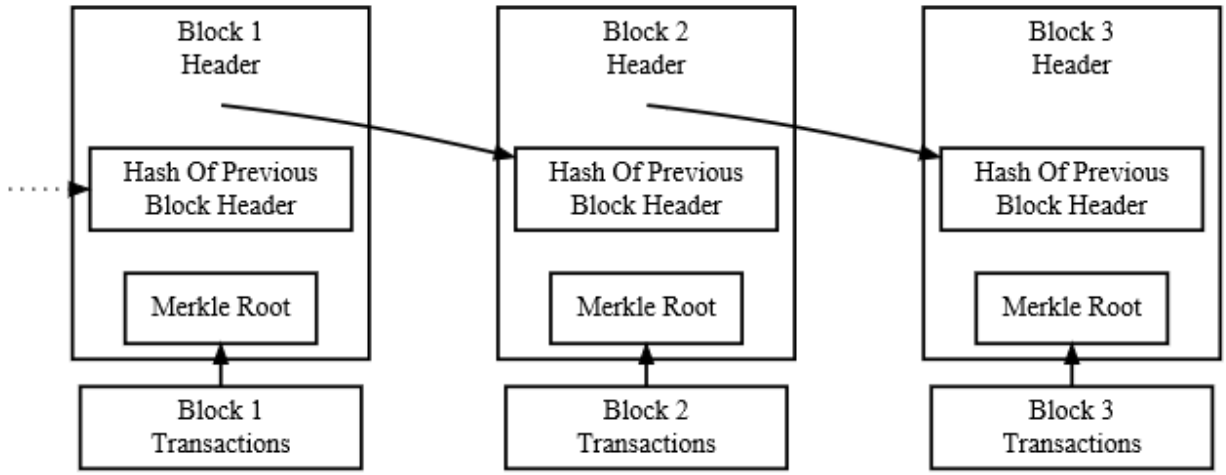
Abstractly, Bitcoin solves the Byzantine Generals problem. Imagine a group of Byzantine Generals camped outside an enemy city (Lamport 1982). They must find a common battle plan of when to attack the city. However, one or more of the generals could be traitors. For this scenario, two conditions have to be met. First, the lead general can only pass along messages through his messenger. Second, any general may be a traitor. So the problem arises, how do the group of generals reach a consensus on battle plans?

Block

From all over the world, transactions flow into the Bitcoin network. A potential problem exists when these transactions appear differently on the network. If transaction A reaches computer 1 at time t = 1 and it also reaches computer 2 at t = 1+X (where X is some additional time) transaction A would appear differently to both user 1 and user 2. To mitigate this problem and maintain an accurate accounting of the transaction, Nakamoto (2008) presented a proof-of-work race.

Recent transactions are broadcasted across the Bitcoin network in a generic list. This long lists of transactions is referred to as a block. On January 3rd, 2009, the genesis block (the first block on the Blockchain) was brought into existence. Blocks of transactions were added to the tail of the genesis block. Image 1 shows the tethering on one block to next. Each block is approximately 1 Megabyte (MB) in size and they have been added to the genesis block in a "linear, chronological order" over time (Swan, 10). However, blocks are not simply added to the existing chain. First, they have to be discovered and this is the job of the Miner.

Image 1: A Blockchain Representation



Simplified Bitcoin Block Chain

Miners

In order to be discovered, Miners take blocks and apply a mathematical equation. This process creates something that is shorter than the original message (the previous mentioned list of transactions) called a Merkle Root.[2] The Merkle Root would appear to be a string of completely random letters and numbers. This is called a Hash or a one-way function. An interesting property of one way functions are that the forward direction is a very easy solution. In this example, taking the data from the block of transactions and finding the hash is the forward direction would take only a matter of seconds (encrypting the data). However, the inverse direction is computationally difficult to compute (decrypting the data).

In order to verify the list of transactions, miners will use additional pieces of data which contains the hash of the previous block of transactions. Image 1 shows this as the Hash of the

[2] Image 1 shows a Block of Transactions being fed in as input and a Merkle root as output. This process would leave the miner with an output of random numbers and letters like:31a87e51bf34a495713016846bcc668ced0b448c7030fffe92d9a637609154b1 called a sixty-four-character digest (Popper, 359). There are 64 characters in the preceding string and a digest is another word for a message. So the process has left the miner with a 64-character message.

previous block header. Since each current block's hash contains the hash from the preceding block, the miner confirms the legitimacy of the older block. This is generically referred to a sealing off a block. For example, if the miner is in the process of confirming Block 2's transactions, the miner is using the hash of Block 1's header. Therefore he or she is necessarily confirming those transactions.[3]

A Solution to the Byzantine General Problem

The lead general now adds two rules that each subsequent general must follow. First, the general must spend ten minutes creating a message for it to be considered valid (a proof-of-work). Second, a history of previous messages must be included with the current message (a distributed ledger). With the addition of these rules, the general can ensure consensus.

The second general receives the attack message from the first general. If they are a honest general, they will spend the ten minutes creating the attack message to send onwards to third general. Conversely if they are a traitorous general, they will try to create a false order. However, the second rule requires them to include a history of all previous messages. Additionally, the first rule requires a valid proof-of-work. That is messages take 10 minutes to create. Thus, the second general cannot create a false message. It would require 20 minutes in total time. 10 minutes to create the false message and 10 minutes to fabricate the lead general's message. The only recourse for the traitorous general, is to admit defeat and accept the first general's orders. Otherwise the third general would notice the delay and the second general would be outed as a traitor.

[3] This is the process of block discovery. It takes approximately 10 minutes to occur. Hard coded into the hash of previous blocks header is a rewarding mechanism. This mechanism awards the miner bitcoin currency. This is often called minting.

In this manner, proof-of-work ensures that a consensus can be maintained. Extending this principle to the blockchain, a public ledger of verified transactions develops. Furthermore, the community can rest assure that this ledger is accurate because of the work done by the mining community. However, processing transactions into the public ledger takes computational work. To compensate miners, Nakamoto (2008) proposed bitcoin.

Bitcoin

Bitcoin has been called a currency, a Ponzi scheme, and even a bubble. In reality, bitcoin shows characteristics of all three.[4] Academics define it by a select group of adjectives: digital, virtual, decentralized, peer-to-peer, electronic, and cryptographic. However, Bitcoin is a "peer-to-peer network that enables the proof and transfer of ownership without the need for a designated third party" (Lo & Wang, 2).[5] The medium through which these transfers occur is the unit of bitcoin (lowercase bitcoin to refer to the individual token). These tokens are highly divisible, to eight decimal places (1BTC = 100,000,000 satoshi and 1 satoshi = 0.00000001 BTC). Milton Friedman's prediction in 1999 resembles the crux of Bitcoin:

[4] One outspoken critic O'brien (2015) calls it a pyramid scheme because Bitcoin produces hoarding in its users. People hold onto their bitcoins in the hope that they will worth more tomorrow than it is today. As he puts it hoarders are "*waiting for some greater fools to push up the price by using theirs"* O'brien (2015). These hoarders then recruit people to use bitcoin. This pushes up the demand for bitcoin and with the price of the coins. Meanwhile, the hoarders' coins are slowing going up in value. Reinforcing O'Brien (2015), Wile (2013) did an analysis of individuals holding bitcoin. He found that: 47 individuals own 28.9% of total bitcoin; 880 owned 21.5% of the total bitcoin. The rest are owned by the masses. If we extrapolate these figures out to today's total 15.4 million bitcoin, we have 47 individuals holding 4,450,600 btc ($1,869,252,000) and 880 individuals holding 3,311,000 btc ($1,390,620,000). This works out to an average holdings of $39,771,319 and $1,580,250 per person in each respective group.

[5] The United States Department of Treasury, the IMF, and the Federal Reserve have all defined the Bitcoin as a decentralized virtual currency (VC). They have expanded the purview to include all virtual currencies. This is much broader and does not provide insight specific to bitcoin. In fact, such a classification would include in game currency. They do submit that virtual currencies have "greater efficiency in making payments" (He et al. 2016, 5). In reality, bitcoin is a decentralized cryptocurrency. The IMF considered the a Taxonomy of VC from broadest defined to most refined: "Digital currencies, virtual currencies (game coins), convertible currencies (web money), decentralized, and cryptocurrencies" (He et al. 2016, 8).

> I think that the Internet is going to be one of the major forces for reducing the role of government. And the one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A, the way in which I can take a 20 dollar bill and hand it over to you and there's no record of where it came from. And you may get that without knowing who I am. That kind of thing will develop on the Internet and that will make it even easier for people to use the Internet. Of course, it has its negative side. It means that the gangsters, the people who are engaged in illegal transactions, will also have an easier way to carry on their business.[6]

Bitcoin has the head start in the "reliable e-cash" race. It is the first decentralized digital currency that has gathered a significant following. A singular bitcoin (BTC or XBT) can be acquired in one of three ways. A BTC can be mined, bought on an exchange, or traded for goods and services. However all three methods require a wallet to store bitcoins.

Wallets

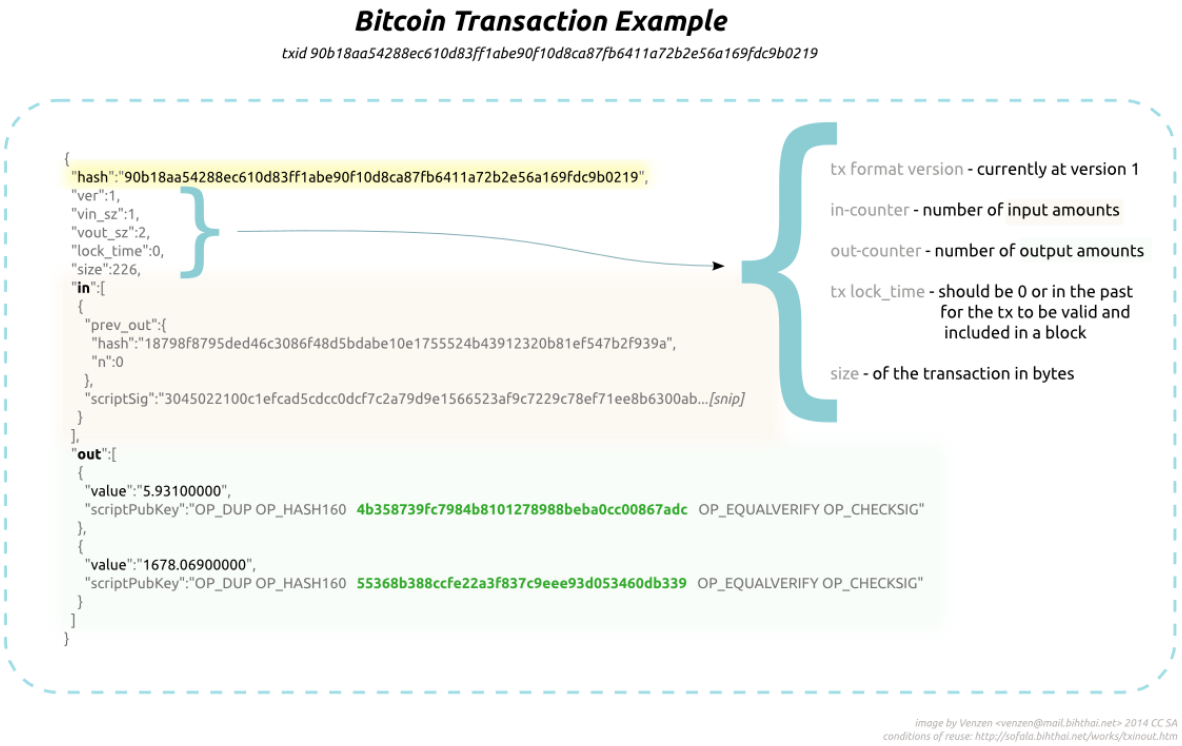
In order to store bitcoin, users have software called a wallet. Like a checking account, a digital wallet will keep current tabs of the level of bitcoin in your account. The *wallet.dat* file is kept on the applications section of a computer.[7] This wallet is important because it holds a user's private key and a public key. This private key is a user's online signature of sorts and it allows the user to verify a transaction. This is of paramount importance as it verifies your expenditure of bitcoins. Conversely, the public address is viewable on the blockchain and allows the user to receive bitcoin. The public address could be compared to your mailing address or a routing number.

---

[6] Milton Friedman's quote was accessed via a Freakonomics Transcript called, "*Why Everybody Who Doesn't Hate Bitcoin Loves It: Full Transcript"*

[7] It is advisable to have a backup copy of the *wallet.dat* file because if a computer is lost or stolen, the wallet.dat file bitcoins on that machine will also be lost or stolen. This brings up an interesting research question: How many bitcoins have been lost? These bitcoins are called zombie bitcoins. Zombie bitcoin are defined "as all bitcoins associated with a public key address which has had no send transactions for over 18 months" (Ratcliff 2014). An interesting question would be gather statistics on which coins have been completely lost compared to which coins are just being hoarded. However, this is beyond the scope of this paper.

Image 2: A Transaction in Bitcoin



Bitcoin transactions (tx) are simply information announce and awaiting verification by the network. All this tx is doing is transferring ownership from individual A to another individual B.[8] Sending Bitcoin, creates a data structure within you *wallet.dat* file. Each transaction has four elements: a unique transaction ID, descriptors and meta-data; inputs, and outputs (Khaosan).[9]

So suppose you created a new *wallet.dat* file called "My Wallet". Four transactions of differing denominations bitcoin are sent to My Wallett: 2 BTC, 0.3 BTC, 0.45 BTC, and 0.1 BTC.

[8] This isn't necessarily correct. Bitcoin is not limited to transactions between individuals. It has the ability to transfer ownership machines to machine or system to system. As long as the other side of the transaction has a Bitcoin address, transfers in Bitcoin can be made to that address.

[9] Khaosan points to four truths about bitcoin transactions: "Any Bitcoin amount that we send is always sent to an address. Any Bitcoin amount we receive is locked to the receiving address – which is (usually) associated with our wallet. Any time we spend Bitcoin, the amount we spend will always come from funds previously received and currently present in our wallet. Addresses receive Bitcoin, but they do not send Bitcoin – Bitcoin is sent from a wallet". From these axioms we can build on our understanding on how transactions work with the *wallet.dat* file. The transactions received do not mix into a singular balance, but rather they remain distinct.

My Wallet's balance would be 2.85 BTC; however, My Wallet does not have 2.85 BTC. Rather it has four unspent transaction outputs (UTXOs) that add up to 2.75BTC.[10] These UTXOs are the output element from the original transaction.

Now suppose you would like to buy a cup of coffee from Peter that costs 0.25 BTC (25 mil satoshi). This will create a new tx data structure called tx1. My Wallet does not have a UTXO that is 0.25 BTC so it will select a UTXO that is larger than the 0.25 BTC.[11] For simplicity, My Wallet will take the 0.3 BTC UTXO and use it as the input element for trx1. Once this occurs the UTXO has been "spent" and is now destroyed. Tx1 will create two distinct output elements. It will create an output element of 0.25 BTC that will be sent to Peter's Wallet. In Peter's Wallet it will sit as a new UTXO of 0.25 BTC. Tx1 will also create a change output element of 0.05 BTC. This will become a new UTXO that will reside in My Wallet. In this manner, My Wallet has been debited 0.25 and Peter's Wallet has been credited by 0.25 BTC.

While these distinctions seem minute, they are incredibly important. By destroying UTXO and creating change, Nakamato (2008) developed a way to tackle the problem of double spending. A bitcoin's transaction history follows it along the public ledger and ensures that bitcoins are not counterfeit.

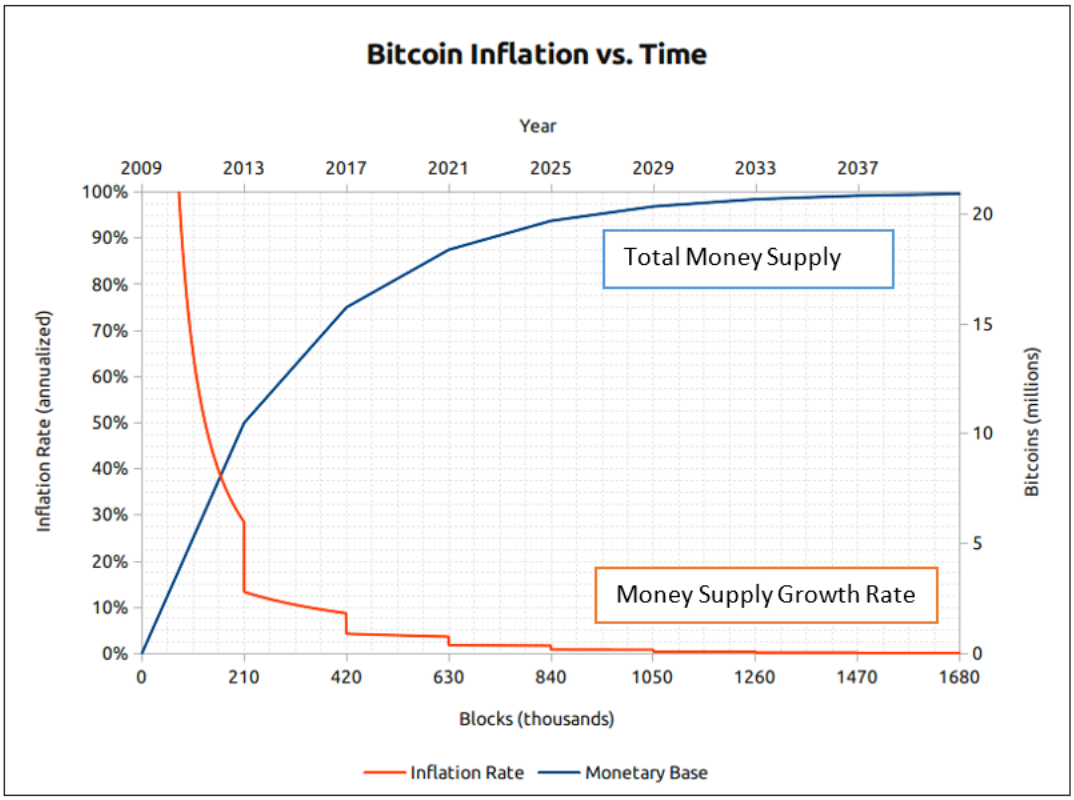
The Minting and Supply of bitcoins

One of the draws of Bitcoin is the capped supply of 21 million bitcoins. The purpose of capping the supply is to introduce scarcity into the market. Moreover, the block discovery reward will reduce by 50% with the discovery of every 210,000 blocks. This decay will follow in this

[10] This difference has to be stressed because it ensures the consensus history of the entire blockchain.
[11] The selection process for UTXOs differ from wallets. Some may select the UTO that is closest in value to the desired amount while others may select the oldest UTO from the bunch. There are merits to all the variety selection systems; however, that is beyond the scope of this paper.

manner: the initial 50 BTC reward, will become a 25 BTC Reward, which will become a 12.5 BTC reward. This decay pattern will continue to zero until 21 M BTC have been distributed. Growth rate halvings occur approximately every four years. Interestingly enough, the next halving is set to occur around July 21, 2016.[12]

Image 3: Bitcoin Inflation versus Time[13]



This minting process seems arbitrary on the face of it; however, it exists for a purpose. Bitcoin arose in response to the perceive fiat debasements of the mid 2000's. Early converts were those seeking monetary restraint. The minting process seems to reflect the works of Milton Friedman. Friedman argued that the "most important magnitude that the monetary authorities can effectively control and for which they have primary responsibility is the stock of money"

[12] Examine http://www.bitcoinblockhalf.com/ this is a clock that is counting down the time until the next halving of Bitcoin.
[13] Source: Bitcoin Inflation versus Time (Bogart 2016, 14).

(88). The money supply is the value that a monetary authority can most directly control. Taking this into account, Friedman prescribes a system where "the stock of money be increased at a fixed rate year-in and year-out without any variation in the rate of increase to meet cyclical needs" (90). This prevents what Friedman describes as "opportunistic tinkering" and would be "an effective insurance against major monetary disturbances" and "a notable reduction in short-term monetary uncertainty and instability" (99). This is what some economists call Friedman's "k-percent rule" (Bohme et al., 233).[14] Although Bitcoin's minting process slightly veers from the program laid out by Milton Friedman, the stock of money is well known. K decreases at a stable rate, every four years until the stock of bitcoin reaches 21 million where k is equal to 0.

Table 1: Bitcoin Scope[15]

	As of March 2015	As of 4/10/16
Total Bitcoin Minted	14 million	15.4 Million
US dollar equivalent @ Mkt Price	3.5 billion	6.5 billion
Total number of Reachable Bitcoin Nodes	6500 nodes	7152 nodes
Total (cumulative) number of transactions	62.5 million	121.7 million
Block Chain size	30.3 GB	64.6 GB
Number of blocks to date	350,000 blocks	406,818 blocks
Estimated Daily Transaction Volume	200,000 BTC ($50 million)	277,000 BTC ($116.6 Million)[16]

[14] The "K-percent rule" fixes the growth rate of the stock of money annually. There are questions that this raises. What happens when the economy outpaces the growth rate? Extending this question to Bitcoin, what happens when the "Bitcoin economy grows faster than the supply of bitcoins" (Bohme et al. 233).

[15] The March 2015 values of this chart were created by Bohme et. al (). I took the values and updated them as of April 10, 2016 through a variety of sources: blockchain.info, bitcoincarts.com, and https://bitnodes.21.co/. BitNodes shows the publically reachable nodes along the Bitcoin network. Of the 7152 publically reachable nodes on 4/10/16, 2495 (34.89%) were in the US; 846 (11.83) were in Germany; 473 (6.61%) were in France; 347 (4.85%) were in the Netherlands; and 269 (3.76%) were in Canada.

[16] Calculated at $421/BTC via blockchain.info

Conclusion

Over the past seven years Bitcoin has grown significantly. Table 1 details the increasing presence of Bitcoin both as a network and as a currency. What many thought to be a passing fad has shown tremendous staying power. In this past year alone, the market capitalization has doubled; the daily transaction volume has doubled; and the number of cumulative transactions has doubled. It is hard to tell if this growth will continue moving forward. Bitcoin's pseudonymous capabilities make it hard to glean accurate information regarding number of users. Experts estimate the number ranging anywhere from 2 to 12 million (Torpey). At time of writing, blockchain.info reports nearly 6.8 million users with over 400,000 unique addresses being used in a day.[17] Measuring the Bitcoin network comes with its challenges. All that we can derive is that the scope of Bitcoin's Network is larger than it was last year.

[17] Users can be using multiple wallets. This is an additional step used for added layers of privacy.

Chapter Two
Examining Bitcoin's Legitimacy as a Currency

Money propelled society out of the barter system and allowed humans to further specialize. Understanding money's characteristics is necessary to assess whether or not bitcoin fulfills those requirements. Without money, people would have to trade goods and services for other goods and services. Currency is a projection of money (Krause, 5). For it to be legitimate, any currency must satisfy three requirements: the currency must act as a medium of exchange, a store of value, and a unit of account.

Amduson and Oner (2012) point to the historical examples of currency over the years like "cowry shells, barley, peppercorns, gold, and silver". The need for money to store its value disqualified the use of perishables as an effective means of currency. People responded by placing their faith in precious metals. These metals were scarce so they would have stable value. Precious metals could be divided and portable making them easier to exchange. Yet, there existed dangers to carrying around ones wealth. Institutions rose up to allow people to deposit their currency with the promise that their gold was kept safely in a vault. When Nixon took us of the gold standard in 1971, this link was severed.[18] The government would issue money by decree or *fiat*. Fiat money as it was coined had the backing of the government that issued it.

[18] Nixon ended the Bretton Woods system, a post-WWII agreement that pegged the U.S. dollar to gold. The U.S. solar was the reserve currency of the world and countries would hold the U.S. dollar which was then convertible into Gold. Once Nixon cut the tie, U.S. dollars would not be exchanged for gold. Proponents of Fiat currency argue that it is more efficient than a commodity backed currency because it is not beholden to the am out of commodity in circulation. And certainly this did contribute to the rise of modern monetary policy; however, it did open up the country to the potential debasement of its sovereign currency.

While 2015 has been a legitimizing year for Bitcoin, Yermack (2013) and Lo and Wang (2014) balk at classifying bitcoin a currency. Their reservations arise from a lack of public trust with bitcoin.[19] Recently the European Union went as far as to recognize the cryptocurrency as a currency (Economist). However, seeing if bitcoin can fulfill currency requirements, is a provocative question that will be addressed with the remainder of this section. Can Bitcoin be considered a legitimate currency?

Currency Evaluation of Bitcoin: A Medium of Exchange

Bitcoin is limited in its ability to be used in transactions. For any currency to be successful, the exchange pool of people using it must be sufficiently large. Bitcoin proponents often site Overstock.com acceptance of the digital currency as a signal that large companies backing the currency are just around the corner. Bitcoin has made traction in enticing substantial companies to accept the cryptocurrency.[20] Limited volume has been a damper on Bitcoin's ability to be medium of exchange. Yermack (2013) cited the daily volume as an important measurement of BTC's exchangeability. In 2013, 70,000 BTC ($29,610,00) were the maximum transacted in one day. That number has tripled and grown to nearly 250,000 BTC ($105,000,000) transacted.[21] However, the volume of bitcoins being transacted is still very small.[22] As Yermack (2013) claims "Bitcoin transactions appear to be rarities, even for the small

[19] The issue of trust is ironic. After all, Bitcoin is the first system that allows trustless transactions over the internet.

[20] Many companies like Amazon, Expedia, Dell, NewEgg, the National Basketball Association, Dish Network, and Virgin Galactic claim to accept the currency. However, these organizations require the assistance of a third party intermediary. For example, BitPay has stepped in an offered solutions to vendors looking to get involved in Bitcoin. Bitpay changes a company's bitcoin to cash immediately. Moreover, companies that are accepting BTC are in the tech sector and are already part of a niche market.

[21] Examine, https://blockchain.info/charts/n-transactions.

[22] An additional area for concern that has not been addressed in transaction volume is speculation. The amount of bitcoin being transacted per day is somewhat misleading because it does not tell whether or not the bitcoins are being bought for speculative purposes. Fred Ersham founder of Coinbase estimated how much of bitcoin being

number of merchants that accept" (10). Though it is hard to know why this is the case, trust still seems to be the main reason why merchants do not accept the cryptocurrency.

This trust issue for both merchants and consumers seem to stem from the fact that a technological barrier exists to getting bitcoin. There are two methods for consumers to get bitcoin. They can either mine it or buy it. The former requires that the consumer has a mining rig, essentially a super computer that is constantly running looking for the solution to complex problems. The latter requires that consumer first, research bitcoin. Second, download a virtual wallet. Third link their bank information to that third party wallet. Fourth, go to an online exchange and purchase bitcoin. Only after these four steps can consumer's engage in the bitcoin system.[23]

However, proponents of bitcoin offer the low transaction fees as reason for large firms and individuals to start switching over to accepting bitcoin (Lo and Wang 7). Most bitcoin transactions do not require transaction fees. Lo and Wang (2014) cite the costs of wiring money as a comparable fee. As they claim "wire transfers can run as much as $30 per transfer domestically and $50 internationally" (7). Bitcoin has no such out-of-pocket fees. Additionally, merchants would not have to deal with interchange fees that credit cards charge (Lo and Wang, 6). Typically, these fees would range anywhere from to 2 to 4 percent and are charged for the convenience they provide to merchants.

bought was for speculation purposes. In 2013, he estimated 95%. That number has since decreased to 80% in 2014. However the number still seems to be very large (Goldman Sachs, 2014).

[23] Both options limit the potential user base. It is a hard ask of consumers to go through this four step process. The draw of bitcoin has to be so enticing that a consumer would go through this time-consuming process.

Currency Evaluation of Bitcoin: A Unit of Account

As Lo and Wang (2014) point out, "Bitcoin's use as a unit of account is so far entirely derived from … its medium of exchange function" (10). The value of a bitcoin is still something that is foreign to the average consumer. For example if good A costs $1.00 and good B costs $2.00, the consumer can readily tell that good B is twice as expensive as good A. When quoting the price of something in Bitcoin, simple comparison would be confusing for the average consumer. Simple items like a cup of coffee would become hard to value if its price was posted in BTC. Consumers would see price quotes like .00529 BTC or $5.255 * 10^{-2}$ BTC for a chocolate bar (Yermack, 12). As a result, merchants would still have to post prices in terms of the local currency (Lo and Wang, 10). Maybe this is just a superficial concern and a reference point can be established that conveys value to the consumers. However, unless a solution to such a problem as simple as price quoting is not found Bitcoin may never gain widespread adoption.

This problem is only exasperated by the price fluctuations that bitcoin experiences. Yermack (2013) took quotes for U.S. dollar prices for one bitcoin from the five most popular bitcoin exchanges and found a 7% bid–ask spread (12). To him and critics alike, this seems to violate the law of one price.[24] So this complicates matters for bitcoin users. If price volatility is high, it becomes harder to establish a reference price which the market could set.

[24] Donald Marron examined the spreads between Bitstamp and the now defunct exchange Mt. Gox and found that a Mt. Gox charged on average a 5% premium for bitcoins. However, the spread has been much larger, and it has even surpassed a 40% spread at times. All of this should be concerning to people wishing to get into bitcoin. Furthermore, the law of one price "is the theory that the price of a given security, commodity or asset will have the same price when exchange rates are taken into consideration" (Investopedia).

Image 4: Bitcoins price over time[25]

A major concern for merchants exists about the oscillating nature of Bitcoin. It requires them to constantly recalculating prices. For example, Overstock.com recalculates it prices in Bitcoin every 10 minutes. If consumers could observe the price fluctuations in such a manner, they may be turned off to using the currency.

However, these problems has been largely corrected by third party money changers like BitPay and Coinbase. Their services provides merchants the peace of mind of never having to be susceptible to the price fluctuations of Bitcoin. Rather, their Bitcoin will be exchanged into the local currency immediately.

Currency Evaluation of Bitcoin: A Store of Value

For a currency to be a store of value, it should maintain its value over some period of time. As bitcoin are not tangible[26], they must be held by third-party wallets. These wallets can be

[25] Source: Blockchain.info

[26] Somewhat true, people have created tangible form of bitcoins. The most popular example is the Casascius coin which has the private key embedded in the coin. Tangible bitcoins are more gimmicky that substantive.

considered like a piggy bank for bitcoin. However, they are subject to hacks and little headway made in insuring Bitcoin. Backed by one-way functions, it would nearly impossible to give restitution to people who have had their bitcoins stolen. This concern can be seen in a statement from Kenya's central bank, "Bitcoin and similar products are not legal tender nor are they regulated in Kenya. The public should therefore desist from transacting in bitcoin and similar products." Bitcoin financial legitimacy could best be described as somewhere in between complete anarchy and the Wild West. Despite this, people still seemed to be enthralled with the cryptocurrency.

Again; however, price volatility seems to be limiting Bitcoin's ability to store its value. It's hard to tell what the price of Bitcoin will be tomorrow, a month from now, a year from now. This does not make it conducive for businesses or individuals to hold for long. Take for example, Dell which claims to accept Bitcoin. "Since Dell began accepting bitcoin through Coinbase in July 2014, bitcoin's value has dropped by over 54 percent. If Dell had actually kept the cryptocurrency it received, its revenue from bitcoin sales would have essentially been cut in half" (Davidson). As Yermack (2013) puts it "Bitcoin's exchange rate volatility in 2013 was 142%, an order of magnitude higher than the exchange rate volatilities of other currencies, which fall between 7% and 12%" (14). For this reason, Bitcoin seems to be something that is more speculative in nature. For this reason, Bitcoin has been given the name "digital gold". People are holding their Bitcoin today on the prospects that it will be worth more tomorrow. 2016 market estimates have the dormant population of Bitcoin being around 80% of Bitcoin's total market capitalization. This approximates to around $4.8 billion worldwide.[27]

[27] http://www.coindesk.com/analysis-around-70-bitcoins-dormant-least-six-months/

Table 2. Characteristics of Currencies: A Comparison[28]

Feature	Bitcoin	USD	Euro	Commodity (Bullion)	Commodity Currency (Coin)	Gold Standard	U.S. Greenback Era (1861-78)
Economic Demand Factors							
Intrinsic Value	None	None	None	Yes	Yes	None	None
Claim to Issuer?	No	Yes	Yes	No	No	Yes	Yes
Legal Tender	No	Yes	No (in the U.S.)	N/A	N/A	Mixed	Yes to public note
Used as a Medium of Exchange	Small, but rising in especially online retail	Yes	Limited (In the U.S.) possibly for more cross-border trade	Yes	Yes	Yes	Yes
Used as a Unit of Account	No	Yes	No (in the U.S.)	Yes	Yes	Yes	Yes (all notes shared "dollar" unit)
Used as a Store of Value	Yes, subject to very high exchange rate risk and sudden confidence shock	Yes, subject to inflation risk	Yes, subject to foreign exchange risk	Yes, subject to commodity price risk/cycle	Yes, subject to dilution of quality (inflation/devaluation)	Yes, subject to devaluation risk	Yes, Subject to inflation risk
Supply Structures							
Monopoly/Decentralized	Decentralized	Monopoly	Monopoly	Decentralized	Mixed	Mixed	Decentralized
Supply Source (public or private)	Private	Public	Foreign Public	Private/Public mining	Mixed	Mixed	Public and private
Supply Quantity	Inflexible	Flexible	Flexible	Inflexible	Inflexible	Inflexible	Flexible
Supply Rule	Computer Program	Rule-Based (Inflation Target	Rule-Based (Inflation Target)	Opportunity Cost for Mining	Tied to Commodity in Bullion	Tied to commodity by reserve ratio	Private note subject to reserve requirement
Supply Rule Change	Yes (With Agreement of majority of miner	Yes	Yes	No	Quantity of minted coins can be diluted	Reserve ratio can be changed and economized	No for private banks
Cost of Production	High (electricity cost for computation)	Low	Low	Very High (Mining)	Medium	Low	Low

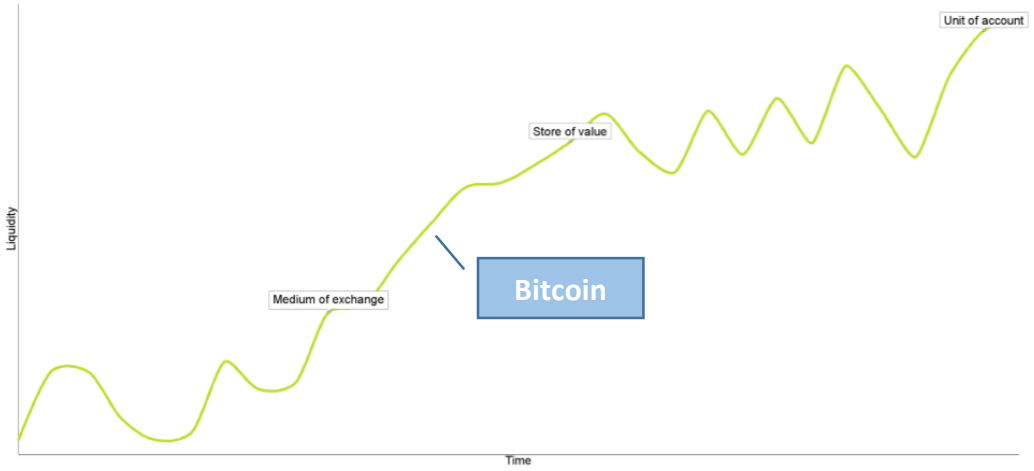
Austrian Theory of Money

Peter Surda (2012) did a currency analysis on Bitcoin from the Austrian perspective. As Surda posits, the Austrian school maintains that the primary function of money is the use of a medium

[28] Source: IMF Report Virtual Currencies and Beyond: Initial Considerations

of exchange (25). The secondary functions of money being a unit of account and store of value comes over time and as liquidity increases.

Image 5: Austrian Perspective of Money[29]



Coupled with Table 4, we are able to position bitcoin placement on an Austrian framework. Currently bitcoins use is as a Medium of Exchange; however, it is gathering characteristics of a store of value. Though this placement of Bitcoin is a controversial one; over time and as bitcoin's liquidity increase, bitcoin has the ability to gather characteristics of a Unit of Account (Surda, 26). The leap to bitcoin being a legitimate money cannot be made via the classical money framework. However, bitcoin does fulfill the primary function of money from an Austrian perspective.

Conclusion

Critics seek to discredit bitcoin as a legitimate currency via the three factors of the classical currency framework. Yermack (2013) and Lo and Wang (2014) argue that one or all of these criteria are being violated by bitcoin. Bitcoin it current form may not satisfy all three

[29] Source: (Surda 25).

characteristics of a currency perfectly. However, it is a budding technology. We are witnessing a living social experiment that has paradigm shifting potential. As its volume and trustworthiness increases, BTC will become more stable.

Image 6: Potential Price Consolidation[30]

Evidence of this can be seen in image 6. Jenn (2016) shows a potential convergence in the price of bitcoin over the past four months. Stability has been something that has escaped the bitcoin markets. If this trend continues, trust in bitcoin will deepen.

[30] Source: Sarah Jenn's Bitcoin Price Technical Analysis for 03/31/2016 – Symmetrical Triangle Intact

Chapter Three
Internal Threats to Bitcoin's Stability

There exist some debate as to whether or not bitcoin (BTC) can be considered a currency. However, there is little debate as to the fact that BTC is rooted in cryptography. The cypherphunks[31] picked up on this idea once the Bitcoin Network was implemented in 2009 Coined a "crypto currency," BTC is a decentralized network that relies on the faith of its users to persist in the ether of the internet. As it is both decentralized and open sourced, BTC has significant security demands. To insulate itself from hacks the blockchain, a public log of all transfers from one person to another in BTC, was developed in order to verify transactions.[32] Directly, BTC "operates as a p2p file sharing protocol it is based on the SHA-256 algorithm" Courtois et al. (n.d.).[33] SHA-256 is a block cipher hash function referencing the Davies-Meyer construction Courtois et al, (n.d). Miners are tasked with solving cryptographic puzzles. When they discover a block:

> a 32-bit value which, when hashed together with data from other transactions with a standard hash function gives a hash with a certain number of 64 or more leading zeroes (Courtois et al.).

These solutions are then linked to one another in a chain, the block chain.[34] The block chain verifies the previous transactions and is as result constantly evolving. As Swan posits, "The blockchain allows the disintermediation and decentralization of all transactions of any type

[31] "Cypherphunks advocate for the use of cryptography and similar methods of a way to achieve societal and political change" (Assange et al., 2012). The term cypherphunk is the union of cipher and punk.

[32] The public log can be hacked and some of these ways will be discussed later on in this chapter.

[33] The United States government transferred from SHA-256 to SHA-3. Although SHA-256 is still a popular encryption algorithm, this could be viewed as a blow to BTCs security. In the future, a better encryption algorithms may be necessary. As of now, SHA-256 should be adequate it is stronger than SHA-128 but weaker than SHA-512. The use of super computers could a potential area of concern moving forward. Computers that guess billions/trillions of times a second could break the strength of SHA-256.

[34] The block chain can be viewed here: *https://blockexplorer.com/*

between all parties on a global basis" (Swan 2015). As a result of the block's discovery, the miner is rewarded with a certain amount of BTCs.

However for BTC to move beyond a social-experiment and become a legitimate financial tool, certain security flaws have to be addressed within the block chain. This section will look at examine unique internal threats to BTC and the blockchain and it will address two in particular. First, the selfish miner threat will be examined. Then, the threat of double-spending will be addressed. Both of these threats have the potential to bring BTC to ruin; however, solutions to these threats will be presented.

Vulnerabilities to the Bitcoin and Blockchain

There are certainly security concerns attributed to BTC. As table 3 shows there are multiple points along the transaction lifecycle that can be attacked. Most notably, third party wallets can be especially vulnerable through DDoS attacks (Vyas & Lunagaria 2014). However, the main concern are threats to the Blockchain which is the featured security to BTC. If the securitization method of BTC is delegitimized the system as a whole will be compromised. The work done by Selfish miners in particular is most concerning.

Table 3: Major Attack/Threats and their Targets[35]

Attack	Target
Attacks on Wallet File	Coins of Users stored in online wallets
DDoS Attack	Online Cloud-based exchanges and wallet services for Bitcoin
Timejacking	Transaction Process, Mining Process
>50%	Mining Process
Double-Spending	Transaction Process
Selfish-Mining	Mining Process

[35] Source: Vyas & Lunagaria (2014) pg. 12.

Selfish Miners

The mining process of the blockchain in part has potential corruption that must be addressed. In particular, selfish miners have the ability to disrupt the security of the blockchain by ignoring some of the blocks. This should be examined in conjunction with the >50% attack. In short, a cartel of miners collects more than 50% of the "computing power in the mining process" (Vyas & Luanagaria 2014).[36] These miners can reveal blocks after the fact of discovery, a revision of transaction history. An alternate, private blockchain is produced by selfish miners in order to fork the chain. As new blocks are published, a subsequent block race starts to solve the next cryptographic puzzle and publish the next block. Selfish miners seek not only to capture the mining reward but increase the length of their private chain. This attack ruins the security of the blockchain by centralizing authority to the selfish miners. If they have the majority of mining capability, they then can mine more BTC than the rest of the honest community. Moreover, it increases transaction times and inject the possibility of double-spending into the network. One solution to this attack is to adopt an unforgeable timestamp or the freshness preferred method Heilman (n.d.). The idea would alter the blockchain protocol so that the most recent block created is preferred. Selfish miners have withheld discovered blocks and freshness preferred would penalize the selfish miners.[37]

Goldfinger Attack

Named after the Bond villain, a sub set attack of the 51% is the Goldfinger attack. Introduce by Kroll, Davey, and Felten (2013) the adversary seeks to ruin the "Gold-backing" of the bitcoin.

[36] It has recently been shown that not even 50% is necessary to capture the lion share of the mining process. Some scholars have shown that as little as 25%-32% is necessary to have an advantage over other miners [3].
[37] It is important to note that the introduction of timestamps would increase the overhead of transacting. However, this penalty should be weighed against reducing the centralization threat of selfish miners. [3]

Kroll et al. (2013) hypothesized three perpetuators of such an attack: a government that is displeased with Bitcoin; a "non-state attacker"; and an attacker that gains financially from the destruction of Bitcoin (13). The first option would be the most plausible avenue for attack. Bitcoin has already classified as illegal in the countries of Iceland, Vietnam, Bolivia, Ecuador, and Kyrgyzstan. The appeal to use such an attack is that current law enforcement techniques have trouble cracking down on Bitcoin (Kroll et al, 13).[38] In reality, the Bitcoin Network has the collective computing power beyond most super computers. As Bogart (2016) states "to 'hut down' Bitcoin would require shutting down the thousands of globally distributed computing nodes that run the Bitcoin protocol" (7). Over 7,000 nodes to be precise. But if anyone had the computing power to do it, it would most likely be a state-sponsored attack.

Double-Spend Attack

The issue of double-spending is particularly damaging to BTC because it destroys the legitimacy of the entire cryptocurrency. Currencies have certain value; however, if that value can be applied more than once an individual engaging in exchange will be cheated. The goal of the double-spend attack is to invalidate legitimate transactions by using a BTC for more than one transaction Vyas & Lunagaria (2014). The attacker creates two transactions: the malicious transaction (TR_a) and the legitimate transaction (TR_v). The transactions share the same BTCs serial numbers; however, the receiving address in TR_v is altered to a falsified addressed that the attacker controls. TR_a is the sent out into the network to be verified while TR_v is sent to the Vendor. If this attack is propagated through a zero-confirmation fast payment transaction of

[38] Chapter 4 will have more on the obstacles to regulating Bitcoin.

bitcoins[39] they"succeed with overwhelming probability" Karame et. al (2012). Fortunately Courtois and Bahack were able to increase detection times dramatically by immediately forwarding all double-spend attempts to the p2p network.[40] Many agree Vyas & Lunagaira (2014), Karame et al. (2012) that the main avenue to reduce these type of attack is to insert an "observer" node into the blockchain. These nodes would be introduced by the third party to intercept TR_a. Since multiple transactions will be not be accepted, in theory the malicious transaction TR_a will be rejected.

Ransomware

Ransomware per say isn't an immediate threat to the stability of Bitcoin; however, it could irreversibly damage the image of Bitcoin by further associating it with criminal activity. Ransomware is a particularly strain of malware that installs itself onto a user's computing systems. This malware then encrypts a user's data. A technical blogger writes, "The encryption can be removed by using a related decryption key in the possession of the attacker. The only way to gain back access to these files is by sending the ransom in bitcoin in exchange for the decryption key"[41] Users will be prompted to pay a fee or risk jeopardizing their systems. Usually the amounts are small; however, ransomware can have major implications. A recent strand of ransomware is thought to be targeting the MedStar Washington Hospital Center

[39] Normally, a BTC transactions are confirmed by at least 6 confirmations. However in the desire to increase transacting speed, zero-confirmations are applied to fast transactions. Fast payments are required when speed of transacting is necessary. Typically, it takes less than 30 seconds for the BTCs to transfer from one party to another. However as this process lacks multiple confirmations, it is inherently more risky to partake in [1,2]. This is a considerable obstacle to the legitimacy of BTC. As one would imagine, if transactions in a certain currency were found to be illegitimate, it would be a serious blow to the faith within that currency.

[40] Dramatically, constitutes a 100% detection rate. However, this should be couched as this was done manually by the researchers. Their average transaction time in this study was 3.354 seconds [2]. Additionally, a low-tech solution to double-spend attempts is simply to apply a listening period. For example, a vendor should wait some time before they complete transactions. This would allow miners the necessary time to verify transactions.

[41] http://www.newsbtc.com/2016/03/25/whats-first-bitcoin-ransomware/

(Buntinx). This attack coupled with the recent attack on Hollywood Presbyterian Medical Center in Los Angeles have both been linked to Bitcoin. Hollywood Presbyterian had to pay out a reported $17,000 in bitcoin to unlock their systems (Barrett). While it is not clear whether the same strand of Ransomware was used, this threat may have lethal consequences.[42] Hospitals and medical facilities are ideal targets for hackers because of lack of preparedness by the staff and the wealth of patient information (Zetter). A hacker knows that a hospital is more likely to pay the ransom because it can be a matter of life and death.

External Threats to Bitcoin's Stability

The Bitcoin ecosystem is threaten by computational, legal, economic, and geopolitical pressures. It is impossible to tell which of the following issues are most pressing; however, they must all be addressed in some form or another. What ties all these threats together are their ability to destroy confidence of Bitcoin. If the public does not trust Bitcoin, will be hard pressed to continue its innovation.

Anti-Money Laundering and Terrorist Financing

The United States Department of Treasury is worried of virtual currencies like Bitcoin. Milton Friedman recognized this fact about his reliable e-cash "It means that the gangsters, the people who are engaged in illegal transactions, will also have an easier way to carry on their business are appealing for illicit activities." Friedman's analysis is spot on as Bitcoin makes perpetuating illicit activities easier for a number of reasons:

- Enables the user to remain relatively anonymous;

[42] To mitigate the effects of the infection, all systems interfaces were forced to shut down. This caused delays in lab results and could potentially bring treatment to a standstill. MedStar operates over 250 facilities in the Washington D.C. area and presumably they use similar systems. (Buntinx) This could be another salvo of cyber terrorism. However, if the link to Bitcoin is confirmed this only harms the public's opinion of the cryptocurrencies.

- Is relatively simple for the user to navigate;
- May have low fees;
- Is accessible across the globe with a simple Internet connection;
- Can be used both to store value and make international transfers of value;
- Does not typically have transaction limits;
- Is generally secure;
- Features irrevocable transactions;
- Depending on the system, may have been created with the intent (and added features) to facilitate money laundering;
- If it is decentralized, has no administrator to maintain information on users and report suspicious activity to governmental authorities;
- Can exploit weaknesses in the anti-money laundering/counter terrorist financing (AML/CFT) regimes of various jurisdictions, including international disparities in, and a general lack of, regulations needed to effectively support the prevention and detection of money laundering and terrorist financing[43]

In fact, Bitcoin was used as the vehicle for exchange in the illicit marketplace called the Silk Road. Nathaniel Popper (2015) argues throughout his book the early adoption of Bitcoin in part was caused by the success of the SilkRoad.

While this concern is warranted, the actual use of Bitcoin and other digital currencies to launder money has not been realized. A National Risk Assessment report out of Britain found that the threat level of digital currencies in money laundering and terrorist financing was low. In fact, more established institutions like money changers and banks were classified at a higher risk level. The report goes on to say:

> *There is little evidence to indicate that the use of digital currencies has been adopted by criminals involved in terrorist financing, whether as a means by which to raise funds (crowd funding etc.), to pay for infrastructure (e.g. server rental), or to transfer funds* (National Risk Assessment, 87)

However, we should not be fooled into thinking that Bitcoin does not host money laundering

[43] This information was gathered from Shasky Calvery (2013) Statement to Committee on Banking, Housing, and Urban Affairs.

and terrorist financing efforts. There are a slew of applications that when used in conjunction with Bitcoin make it virtually impossible to track. Virtual Private Networks (VPNs), TOR (anonymous networking), and Dark Wallets are all added measures that could obscure online identities.

Deflationary Spiraling

Barber, Boyen, Shi, and Uzun (2012) present an interesting scenario for Bitcoin in the coming future. Barber et al. (2012) claim that because the supply of Bitcoin is capped at 21 Million BTC should appreciate against the dollar as marginal acceptance increases (6). Therefore, the real purchasing power will necessarily increase over time. Interestingly enough, this appreciation could severely hamstring the system through deflation.

A moral hazard of hoarding could sent in. The value of Bitcoin is dependent on its ability to garner the trust of the public. If BTC appreciates as expected against the dollar, the average user would prefer to save (hoard) their bitcoin rather than spend it. That is because a bitcoin today (t) would be worth more in real purchasing power than a bitcoin in the future (t+1, t+2,…,t+X). This hoarding behavior could result in a loss of circulating bitcoin, transaction volume decrease. Moreover, the mining new Bitcoin could become less profitable resulting in the miners no longer working on block discovery (6). With less miners verifying transactions in the market, further consolidation of the mining community could occur. This could lead what Barber et al. call a "History revision attack"[44] (6).

[44] See Chapter 3

To combat the potential deflationary spiral, Barber et al. (2012) propose "organic inflation" (6). This inflation target would be used to incentivize miners continue to verify transactions via block discovery. However, this is simply thinly veiled inflation targeting.

Regulations

The regulating nightmare that is Bitcoin can be exemplified by the different definitions that government agencies used when talking classifying bitcoin. For tax purposed the IRS defines Bitcoin as property. The SEC maintains that Bitcoin is a security. Finally, FinCen considers Bitcoin a currency. Erik Voorhees spoke to the regulatory nightmare:

> Bitcoin businesses are literally at the edge of law, not because they are doing anything wrong, but because Bitcoin enables new activities and behaviors and recategorizes money in such a way as to enable it to transcend current statutes. This is both exciting, and scary, because we're breaking amazing ground and we'll inevitable be in the crosshairs for doing so. (Popper 224).

The thing that makes Bitcoin incredibly hard to regulate, is that its meaning can be different to different people. To the miner, it is a source of income. To the casual investor it is a commodity to be traded.

A technology lawyer claims that to regulate Bitcoin in its current state could be an "exercise in futility" (Cameron-Huff). As the current market capitalization of Bitcoin pales in comparison to the trade in any specific commodity or currency, regulators time would be better spent on the current. The blockchain is in its infancy. Overregulation is a considerable concern that could stifle innovation. This can be seen in the New York BitLicense fiasco. The New York Department of Financial Services (NYDFS) issued a regulatory framework to handle issues with virtual currencies including bitcoin. Introduced in August of 2015, this framework require a

license to operate within the state of New York.[45] In response to the potential regulations, Bitcoin startups migrated out of New York for less regulated locales (del Castillo). Startups are finding that the costs outweigh the actual benefits of receiving a BitLicense. As a result, only larger and more established firms have the resources to within New York.

BitLicense can be seen as a microcosm for what future attempts to regulate Bitcoin might look like. As more cities, nations, and the world seek to apply regulations onto Bitcoin, innovation and development in Bitcoin may be stifled. The need to regulate cannot be ignored. However, current and future attempts at regulating complex technologies could be creating "hollow laws" (Cameron-Huff). These laws would pile up in sedimentary layers as Bitcoin development quickly outpaces its legal constraints.

Taxation

Virtual currencies can be used to evade national taxes. With the emphasis on anonymity, users of Bitcoin do not need to share their identity. The ability to attribute transactions to specific individuals is limited. Moreover, the ability of Bitcoin to be nearly frictionless affords the users of Bitcoin to find a tax situation that is marginally beneficial. The IMF is already questioning how to effectively enforce taxation (He et al. 2016, 30).

Some countries have already created policies directed at VC's like Bitcoin. As the IMF states, "most countries that have addressed the issue have determined that VC's will be treated for income tax purposes as non-currency" or property. (30). However, Bitcoin taxation is

[45] The application for the license is 30 pages long and cost $5000. Moreover, the costs of applying could range upwards of $100,000 for a company (Perez). However, the costs of the application are not limited to dollars and cents. As Michael del Castillo writes, "Not only do the BitLicenses require companies share in-depth information about their own operation, but there are ongoing Know Your Customer (KYC) requirements designed to prevent money laundering". Bitcoin's draw is in part rooted in an ideology. Many consumers of Bitcoin do not trust the government and the big banks.

incredibly nuanced. For example, the selling of Bitcoin for a capital gain differs from the reward of Bitcoin through mining processes which differs from an exchange of Bitcoin for goods or services. These issues must be addressed before Bitcoin can become legitimate.

The IMF in their discussion on bitcoin addressed the taxation issue. For example, The United States implements a fair market value at the time of mining for income generate through mining activities. This differs greatly from the policies of Australia, which taxes miners once BTC are transferred. The United Kingdom implements other forms of taxation like a VAT and Sales tax. Per the U.K.'s policy, "(i) use of VC's in purchase of any good or services will be treated in the normal way for VAT, with the value being the sterling value of the VC at the time the transaction takes place; (ii) income from mining activities will be outside the scope of VAT; and (iii) exchanges of VCs for British or foreign currency will not be subject to VAT on the value of currency itself, nor on any fees or charges for arranging the transactions. (IMF, 30). However, these differing tax policies are playing catch up to VCs. Additionally, they require significant documentation request to enforce. For example, the U.S. policies will require reports of gains and losses of BTC transactions. Complicating the entire process, this would require the convergence of multiple reports from multiple Bitcoin exchanges. And all of this is supposed to be done by the taxpayer?

Consumer Protection

The Mt. Gox causes financial harm to many of Bitcoin's users. The entire system is vulnerable to the threats enumerated earlier in chapter 3. Moreover, the laws and regulations are being written on Bitcoin in real-time. The system depends on unregulated third party wallets, exchanges, brokers, and clearing houses (He et al. 28). Transactions are one-way functions making them irreversible. For example, "users cannot reclaim payment for erroneous

transactions given that decentralized VCs lack a central intermediary as well as clarity regarding the counterpart" (IMF 29). This opens up the entire industry to scams. The idealistic creators of Bitcoin hoped that the community would be made up of honest users; however, in application dishonest users are out there. Currently, people transact in Bitcoin at their own risk. Many sites include warnings about the potential for loss of principal when engaging in Bitcoin activities.

Many of the issues revolving around Bitcoin occur because it has not been defined. It does not fall into a singular regulatory category but rather has elements of many categories. It could be considered under three financial categories: investment contracts; as a note or security; or a commodity. Defining regulation is necessary for the future stability of Bitcoin.

Scalability

Individual blocks on the blockchain are considered by the Bitcoin community to be too small to the handle the amount of transaction needed. The 1 MB limit currently in place translates to "roughly 200,000 transactions a day, or approximately 3 per second" and some believe "a higher limit" is necessary to ensure longevity of Bitcoin. For parity, "the bitcoin network currently does about seven transactions per second. PayPal does 100. And Visa does 4,000" (Metz). Gavin Anderson believes that "the availability of convenient, attractive, secure, lightweight wallet software and the general trend away from computing on desktop computers to mobile phones and tablets" has burdened the Blockchain.

Some proposals on the table are to increase the block size to 8MB, by doubling the blocks every two years until they reach 8MB. This 2-4-8 plan is being pushed by Bitcoin

Fundamentalists, Gavin Andresen and Jeff Garzik.[46] A consensus; however, needs to be implemented by the mining community in order for any changes to occur to the system. Miners are taking sides on the matter.

A fork in the road seems to be on the horizon for Bitcoin. Literally, the community has been developing forks away from the Bitcoin Core chain. A fork is essentially a copy of the original version with some added software (Kroll et. al. 17). A fork to Bitcoin XT[47] would increases the block size and allow for more transactions to be verified in a single block. The argument for doing so is that increasing the transaction volume constraints would allow for more people to adopt BTC. This, in turn, could lead to a more robust network with nodes running in more political jurisdictions" (Andresen).

However, the increase in block size could have unintended consequences. In response to a 2-4-8 system, miners will seek to consolidate further. The cost announcing larger blocks cost computational resources of low-latency and high-bandwidth. As block size increases, the bandwidth required to announce block discovery increases. Consolidation will push miners out, and cause the development of a very small number of very large miners" (Andresen). This seems to be at odds with the ideological sentiment of Bitcoin.

Mike Hearn a Vanguard member of Bitcoin, officially declared the system dead. The incentives to switch to the necessary 2-4-8 system are off. As Hearn suggests, "the miners [of Bitcoin Core] refuse to switch to any competing product, as they perceive doing so as 'disloyalty' —and they're terrified of doing anything that might make the news as a 'split' and

[46] This would increase blocks to 2MBs immediately. In a year, blocks would increase to 4 MBs. Finally, block size would settle at 8MB.
[47] The higher block size plan laid out.

cause investor panic" (Hearn). Astonishingly, the Chinese Miners could actively be suppressing the spread of Bitcoin. The Great Firewall of China seriously inhibits the ability of data to transport across linked systems. As a result, Chinese Bitcoin miners are in a quandary. As Hearn posits:

> Right now, the Chinese miners are able to — just about — maintain their connection to the global internet and claim the 25 BTC reward ($11,000) that each block they create gives them. But if the Bitcoin network got more popular, they fear taking part would get too difficult and they'd lose their income stream. This gives them a perverse financial incentive to actually *try and stop Bitcoin becoming popular.*

The Bitcoin community is treading into unknown waters on this. Many are calling this a schism others are calling it a civil war. However, Bitcoin is at a crossroads where it either must evolve to higher block size or risk a slowdown in operations.

Consolidation amongst Mining Pools

In order to increase the chances of discovering the next block in the chain, Miners will pool computational resources into mining pools. Miners will then split the reward amongst all those engaged in the pool. "Bitcoin mining in pools began when the difficulty for mining increased to the point where it could take years for slower miners to generate a block" (Bitcoinmining.com). This consolidation is an example of the principal of economies of scale at work.

Mining pools were an important development in Bitcoin because they allowed for individual miners to receive consistent returns. Individual miners would need to devote incredible amounts of computational power and even then the chances of block discovery were very variable. The individual miner would then present evidence of computational work performed (proof-of-work) and a share of the discovery reward would be awarded to them. In the context of mining pools, a share is simply a portion of the overall solution. Specific mining

pools have a variety of ways in which they calculate a miner's share. Pay per Share Method is a popular methods because it "shifts the risk to the mining pool" and "guarantee[s] payment for every share you contribute." (Bitcoinmining.com) However, there exist a variety of payment methods and they differ with each different mining pool.

Image 7: Mining Pool Hashrate Distribution

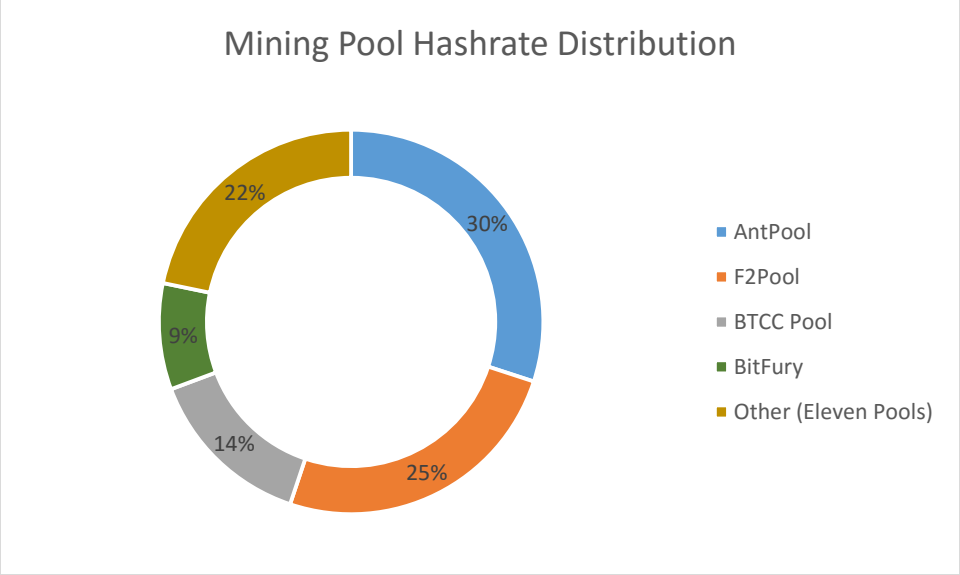


Image 7. shows the hash rate of mining pools for the past four days (April 9, 2016). Ant Pool and F2Pool discovered 30% and 25% of the nearly 600 blocks added in the past four days. While this still is far from the threshold for a 51% attack, it should be cause for concern. As Heilman (n.d.) pointed out, 25% to 32% could be the theoretical floor to a mining pool centralizing the mining process.[48]

Potential for Break in Anonymity

Users are mistaken in thinking that Bitcoin is completely anonymous system. A better characterization of Bitcoin would be pseudo anonymous. A motivated attacker can use basic

[48] What should be a far greater cause for concern is the location of these mining pools. Antpool and F2pool are both located in China. It is not hard to imagine further consolidation between these two pools that would take the market over the 51% threshold.

data analysis techniques to break user anonymity Reid and Harrigan (2012). The public log of all transactions made in Bitcoin is a treasure trove of information. When coupled with external "off network information", Reid and Harrigan (2012) were able to form linkages that threaten the anonymity of users (15). This type of "off network information' includes but is not limited to twitter, Bitcoin exchanges, public directories, and Bitcoin forums. More disturbingly, Reid and Harrigan (2012) were able to leverage the information on Bitcoin Faucet.[49] Using basic web scraping they were able to associate public-key information with certain IP addresses. They were then able to geolocate these IP addresses (16). Information also leaks through the TCP/IP layer and Dan Kaminsky was able to exploit this information and map all the public-keys on the Bitcoin Network to IP addresses, by opening a connection to all public users (Kaminsky). If a user does not take steps to anonymize their web use (via TOR or a VPN), hackers can form extensive data linkages.

The threats revealed by Reid and Harrigan (2012) and Dan Kaminsky (2011) should be alarming. A motivated attacker, armed with extensive "off network information" like that available on a Bitcoin exchange, can observe with whom and where Bitcoin users are transacting. In the future, it is not hard to imagine an Ashley Madison like data breach involving the Bitcoin community.

Competitor captures the market

Although many other cryptocurrencies do exist (they are called altcoins and examples include i.e. Litecoin and Dogecoin), Bitcoin "is the de facto standard" (Swan, 10). To date, Bitcoin is the

[49] "The Bitcoin Faucet is a website where users can donate Bitcoins to be redistributed in small amounts to other users" (Reid and Harrigan, 15). This website now appears offline; however, while it was operational it did include a list of IP addresses of those who received bitcoins.

most successful virtual currency. While Bitcoin's first mover advantage is considerable, it may not insulate Bitcoin from a superior competitor capturing market share. Over 275 virtual currencies exist in some form or another (Marshall 90). Cryptocurrencies at the time of writing had a market capitalization of over eight billion dollars. Table 4 illustrates the top ten cryptocurrencies as of April 7, 2016:

Table 4: Top Ten Crypto-Currency Market Capitalization[50]

Rank	Name	Market Cap	Price ($)	Available Supply	Volume (24h)	%Change (24h)
1	Bitcoin	$ 6,521,612,319	$ 423.34	15,405,250 BTC	$ 56,287,200	-0.14 %
2	Ethereum	$ 805,680,261	$ 10.22	78,856,061 ETH	$ 13,869,500	-5.92 %
3	Ripple	$ 237,861,720	$ 0.006907	34,439,870,367 XRP *	$ 1,442,500	-5.78 %
4	Litecoin	$ 147,061,244	$ 3.25	45,259,501 LTC	$ 1,095,380	-0.17 %
5	Dash	$ 44,691,332	$ 7.03	6,358,180 DASH	$ 154,782	-0.26 %
6	MaidSafeCoin	$ 34,421,272	$ 0.076060	452,552,412 MAID *	$ 100,878	-0.06 %
7	Dogecoin	$ 21,982,583	$ 0.000212	103,821,697,300 DOGE	$ 137,699	-1.93 %
8	Monero	$ 17,792,959	$ 1.54	11,531,630 XMR	$ 256,667	-0.27 %
9	BitShares	$ 15,108,208	$ 0.005921	2,551,420,000 BTS *	$ 120,330	-2.55 %
10	Factom	$ 13,447,045	$ 1.54	8,753,219 FCT *	$ 193,602	-0.45 %

The most recent competitor, Ethereum, rivals Bitcoin and is making a considerable push for market share. Ethereum, seeking to revolutionize the smart contract concept, has some perceived advantages over Bitcoin that should not be underestimated. First, it has the advantage of time over bitcoin. Bitcoin introduce in January of 2009 could be battered, broken, and beyond repair. Ethereum introduced in July of 2015, has six years of learning from the mistakes of Bitcoin. Second, Ethereum will transition to a proof-of-stake method to achieve the consensus along its blockchain. Proof-of-stake method for consensus means that owners of Ether (ETH), the crypto assets of Ethereum, only have to prove their stake in terms of Ether. From a cost perspective, proof-of-stake improves on the proof-of-work method because proof-

[50] http://coinmarketcap.com/

of-work requires energy consumption. Proof-of-Stake is simply more cost effective. Third, Ethereum ensures that the rewards for block discovery will be constant over time. Unlike Bitcoin, inflation of the digital currency will be zero. Fourth, Ethereum has not capped the supply of Ether. Fifth and finally, Ethereum has serious clout with powerful businesses. As of March 2016, Microsoft, JP Morgan Chase, and IBM had introduced or are in development of applications running on the Ethereum platform (Popper 2016).

Ethereum currently stands as the most competitive altcoin. However, this does not necessarily take away from Bitcoin. Bitcoin has some significant advantages over Ethereum. First, the Ethereum platform is more complex than Bitcoin. Code complexity leaves Ethereum with higher potential exposure with security flaws. Bitcoin has seven years of tested resilience. Additionally, "the novel design of Ethereum may also invite intense scrutiny by authorities given that potentially fraudulent contracts…can be written directly into the Ethereum system" (Popper 2016).

Conclusion

There is a full court press on Bitcoin from a variety of sources. Externally, regulators fear the Bitcoin's potential as vehicle for money laundering and terrorist financing. Lacking a viable definition for Bitcoin, regulators naively define it as either a commodity, a currency, or a security. In reality, Bitcoin has aspects of all three. Seeking to steal market share, competitive altcoins like Ethereum are gaining considerable ground on Bitcoin.

BTC and the blockchain are subject to a multitude of internal security threats. In particular, the ability for individuals to spend one BTC more than once and the ability to withhold blocks from the blockchain must be addressed. If not, the entire system will become centralized and corrupted. This would defeat the entire purpose of having a decentralized

currency in the first place as volatility would almost certainly ensue. BTC has made global transactions easier and has potential to revolutionize global monetary problems. The blockchain has been lauded as a means of ensuring data integrity through cryptography.[51] However, these inherent internal flaws must be addressed before Bitcoin can be adopted as a legitimate financial tool. If neglected, these external and internal threats could create a crisis of confidence for Bitcoin.

[51] The Blockchain can be extended to all forms of data management. It has been linked to developments in financial services, communication networks, and crowdfunding. Some argue that it can even be a pathway to an eventual artificial intelligence (Swan 2015).

Chapter Four
Predications on the Future of Bitcoin

The time is ripe to make predictions about the future demand for Bitcoin. In the short term, we should necessarily see the price of bitcoin increase. This is because the rate of supply should decrease with the halving in mid-July. The rate of bitcoin growth will decrease as discovery rewards decrease from 25BTC to 12.5BTC. Holding everything constant, the reduction in supply will cause an upward pressure on price. Theoretically we should therefore see an appreciation of bitcoins to other currencies.[52] Daniel Masters, co-founder of the bitcoin hedge fund Global Advisors, drew a parallel to the oil industry "If OPEC (Organization of the Petroleum Exporting Countries) came out tomorrow and said, 'in six months' time, we're going to halve oil production', the price of oil would instantaneously react" (Reuters). It is impossible to tell whether or not bitcoin will react like oil in the presence of a supply shock. What can be done; however, is make inferences based empirical data and other external pressures that could affect the price of bitcoin.

Bitcoin's exchange rate to US dollars seems to be standardizing. In Image 6, Sarah Jenn highlights consolidations of BTC/USD since December of 2015. If this pattern continues, it could alleviate the concerns of some Bitcoin price volatility. Moreover, people in the Needham group feel that the current level of Bitcoin are undervalued significantly. They feel that in the next five years the price of Bitcoin will rise to a value of $655/BTC (Bogart). While this may seem like

[52] This assumption's counter is quite easy to understand. Perhaps, 12.5 btc is not enough of a reward to justify the expenditure on mining. The individual miner is then left with two foreseeable choices: pack up their rig and leave the market or continue to mine at pre halving levels. In the short term, the reward is less appealing than the previous 25 btc. If the appreciation does not justify the mining costs, we could witness miners leaving the market in droves. Well established mining pools should naturally exploit the exodus of firms and reinforce their advantages. This could lead to a further centralization of the mining community. However, the Bitcoin community had already through a halving process in 2012 and little

a pie in the sky assessment of future Bitcoin prices, upon further examination of the fundamentals about the Bitcoin ecosystem and global economy could cause this to occur. So what could be drivers to the increase in stability and trust in the Bitcoin system?

Further Internet Penetration

The world is becoming increasingly interconnected. As the internet of things expands throughout the world, Bitcoin could witness a spike in popularity. The rise of smartphones could be a catalyst for this potential growth. Fred Wilson argues that a second spike in smartphones in the developing world will promote mobile applications for health services, finances, transportation, and other essential services that are lacking in emerging markets. By 2020, nearly 65% of the global population will have smartphones with access to the internet (Evans). Riding this "mobile revolution" could be Bitcoin.

Developing Bitcoin Financial Architecture

As Bitcoin develops, necessary infrastructure will develop along with it. All of this will decrease the technological barrier that currently shrouds Bitcoin. As third parties enter the ecosystem, they provide services that not only increase the visibility of Bitcoin but also increase its overall stability. While Bitcoin remains on the financial frontier, old world financial services firms are staking their claims. New technologies are popping up along the transaction cycle and these will further drive down price volatility. Already there are numerous examples of this developing architecture.

Bitcoin ATM's

One of the most visible extensions of the Bitcoin ecosystem are the Bitcoin ATMs. Since 2013, these machines have been installed all around the world at increasing rates. There are two types of machines a one-way and a two-way machine. The one-way machine (60% of the

machine population) allows for purchases of bitcoin to be made whereas two-way machines (remaining 40%) allow for both the purchase and sale of bitcoin. Currently, there are over 600 of these machines globally.[53] While the industry average transaction fee is over 7%, these are the most visible form of the Bitcoin economy. Bitcoin ATMs have the potential to increase the user base of bitcoin. It will be interesting to see if this technology has staying power over the next couple of years.

Digital Wallets

The original generation of *wallet.dat* files were technologically cumbersome. The average user would be expected to possess a level of computing acumen to be able to navigate the Bitcoin ecosystem. To expand to a larger public, developers started to create second generation of wallets. These wallets would be hosted online. This offers some improvements over the original wallets. First, there is a significant reduction of overhead. First generation wallets were nodes to the entire Bitcoin network and they required up-to-date access to the Blockchain (Khaliq). Second, online wallets are an easier overall experience to use.

However, there exist some disadvantages to using an online wallet service. First, you are giving up the autonomy of a first generation wallet. Administrators of the site are in control of a user's account and by extension their bitcoin. Second, online wallets like Coinbase further centralize the process. Third, certain online wallets collect more information on their users. For instance, Coinbase has acquired a BitLicense from NYDFS and this had "Know Your

[53] These machines are predominately located in North America with 284 of 619 in the United States and 104 of 619 in Canada. The rest are scattered throughout the globe. However, 1.43 new ATMs are being installed per day (Coin ATM Radar). However, Greece has shown significant interest in expanding these numbers. As Katy Barnato reports, "BTCGreece, which bills itself as the country's first bitcoin exchange, plans to eventually install 1,000 ATMs nationwide, in partnership with European bitcoin platform, Cubits". Again only time whether the ATM bitcoin angle has staying power.

Customer" requirements.[54] This makes them an appealing target for potential attack like the one laid out by Reid and Herrigan (2013). Therefore, a tradeoff between security and convenience when using an online. If users are convinced that the measures taken by online wallets like Coinbase, they should use the services.[55]

Coinbase exemplifies how these online wallets can expand the industry boasting: 3.6 million users, 5.3 million wallets, 42,000 merchants, and 8000 developer applications (Coinbase). These services are increasingly becoming popular avenues for people looking to get into Bitcoin. As they gain this popularity, this should put upward pressures on the demand for Bitcoin.

Bitcoin Debit Cards

Another highly visible extension of Bitcoin are the new Bitcoin debit cards. These cards would operate like current debit cards and enable users to spend money directly from their Bitcoin wallets. Moreover, these cards immediately transfer your bitcoin to the local currency making them acceptable to most merchants. Xapo is widely considered the forerunner of the bitcoin debit card market. Their card is partnered with Visa and is accepted at any location that accepts Visa (Xapo). However, the Xapo card has limits and fees just like any other debit card.

Investment Vehicles

Barry Silbert has launched the first venture into digital currencies for investment called Digital Currency Group (DGC). One of the subsidiaries of DGC called Greyscale Investments created

[54] Many consider this selling out by Coinbase. However, there are some built in consumer protections that come along with holding a BitLicense.

[55] Coinbase claims to keep 85% of their total bitcoins in cold storage. This obviously increases the friction in the market. The purchase of bitcoin on Coinbase requires time for it to settle in the Coinbase online clearing house. It seems that the nearly instantaneous transaction time still needs time to further develop.

the first investment vehicle involving cryptocurrencies called Bitcoin Investment Trust (GBTC). In March of 2015, GBTC received approval by the FINRA.

Image 8: A Quote of GBTC

Although this is only one security, GBTC shows a movement towards legitimacy for Bitcoin. This further reduces the obstacle to owning bitcoin. As Grayscale submits, "The BIT [Bitcoin Investment Trust] enables investors to gain exposure to the price movement of bitcoin through a traditional investment vehicle, without the challenges of buying, storing, and safekeeping bitcoins". With the BIT leading the way, we could be seeing future bitcoin-backed securities hitting a variety of markets.

Currency Exchanges

The ability to transact from one individual to another is of paramount for currencies. Bitcoin relies on currency exchanges to perform these functions. Through these exchanges, an individual can trade currencies either traditional or virtual for Bitcoin. (Bohme et al 220). In addition, these exchanges allow buyers and sellers of Bitcoin to transact in bitcoins. Like other

markets, buyers buy for as low as possible and sellers sell for as much as possible, this is the bid-ask spread. On top of these transactions, exchanges will apply a small commission.

In 2014, the Mt Gox exchange failed located in Tokyo, Japan. This was considered by many to be the death blow to the Bitcoin ecosystem. At the time nearly 754,000 customers had their bitcoins on the exchange. This loss of BTC amounted to nearly $450 million lost. (Bohme et. al, 220). Nearly 80 percent of all transactions in Bitcoin were handled on this one platform.

The Mt. Gox failure, actually strengthened the Bitcoin ecosystem. It allowed for more exchanges to enter the market and handle transactions. As Bohme et al. posit listed the seven largest bitcoin exchanges as: BTC China, OKCoin, Huobi, Bitfinex, LakeBTC, Bitstamp, and BTC-e, which jointly serve more than 95 percent of all bitcoin trade from October 2014 to March 2015" (220).[56]

However, in 2016 it seems that the exchanges are becoming less diverse. The 2 largest exchanges Huobi and OkCoin now handle 92% of Bitcoin trades. (Bitcoinity.org). Although this is much better than the 80% of the now defunct Mt. Gox, it still makes these two exchanges appealing targets for future attacks.[57]

[56] This can be considered misleading to a certain extent. In May of 2015, Coinfox published an article addressing the dominance of Chinese Bitcoin exchanges. According to Coinfox, "Three of the biggest Chinese digital currency exchanges dominate the sector globally, with BTCChina, OKCoin, and Huobi market shares reaching 33.01%, 32.38%, and 14.78% respectively." At the time of publishing, 80% of transactions were handled on these platforms. Since, BTCCHina has seemingly been squeezed out.

[57] This presents a few questions that are out of the scope of research: why is so much volume being handled by the Chinese; what problems could arise; and will a challenger arise? Does this even matter? What if it was US based exchanges that traded over 90% of the world's total BTC? We do know that Chinese miners have considerable mining pools. Could this be an explanation?

Further Adoption in Emerging Markets

For citizens of countries with relatively stable fiat currencies, it is hard to realize the advantages of a substitution towards bitcoin.[58] Bitcoin's potential rise could be sparked by those living in emerging markets. Much of the world developing does not have access to bank accounts and the demand for financial security is apparent.[59] The beauty of Bitcoin is that it allows individuals to keep their money more safe than keeping it on hand. Particularly, Bitcoin's appeal is on center stage in Latin America where many countries are suffering from dysfunctional monetary policy.[60] The monetary outlook for 2016 will not be kind to Latin America:

> The International Monetary Fund (IMF) predicts a 720 percent inflation rate for Venezuela during 2016. The Brazilian economy has entered a recession that, according to the IMF projections, will be the longest since 1930-31. Argentina's Minister of Finance in Argentina predicts a minimum of 25 percent inflation, and analyst projections estimate that 2016 inflation could be as high as 38 percent, with a 30 percent devaluation of the Argentine Peso against the U.S. dollar (Sing & Vega 2016)

Seeming to crystalize the link between increase inflation rates is a study by Makari Krause (2015). His findings seem to indicate "that bitcoin is in fact being used as a safe haven asset for those confined to inflationary currencies and that a small increase in inflation can lead to a

[58] I believe this is the answer for why so much of Bitcoin transactions are being handled by Chinese exchanges. Bitcoin is popular in China precisely because it is not the Chinese Yuan. Although, the Chinese government is against Bitcoin, the people value it as a more stable currency. Of course this is conjecture, but monetary policy by the Chinese Central Bank i.e. flooding the market with cheap Yuan makes this a plausible answer. Therefore, I surmise that Chinese citizens are substituting away from the debased Yuan and towards bitcoin.

[59] Some of the draw of this can be seen through the Example of M-Pesa in Kenya. M-Pesa designed originally for the propulsion of microloans, has been leverage by the bulk of the Kenyan population. The economist reports, that over "17 million" Kenyans use this mobile application to move money. Additionally, has led to an increase in incomes from anywhere from 5% to 30 %.

[60] Bitpay, a payment processor for Bitcoin, reports that merchant transaction in Bitcoin have increased by 1747% in 2015 over 2014. https://blog.bitpay.com/understanding-bitcoins-growth-in-2015/

profoundly large increase in bitcoin adoption" (Krause, 29). Although this does not provide insight into adoption rates in developed markets, global demand should increase altogether.

Increase in Remittances

Bitcoin also has the potential to shake up the remittance market. Remittances are "the funds an expatriate sends to their country of origin via wire, mail, or online transfer" (Investopedia). The price of these transfers can be very costly. Bitcoin has the unique opportunity to decrease the costs of these transfers. Table 5, shows the transaction cost of sending $200 dollars home through a variety of payment processors. Individuals using bitcoin to change their money are saving by an order of magnitude. Bitcoin has the ability radically reduce the price of remittances globally.

Table 5: Remittance Fees associate on a transfer of $200[61]

Remittance Corridor	Money Transfers Operators	Banks	Bitcoin
Australia–Papua New Guinea	15.3%	18.1%	0.02%
Germany-Serbia	6.6%	20.9%	0.02%
Japan-Brazil	10.1%	18.1%	0.02%
Malaysia-Indonesia	1.9%	7.1%	0.02%
New Zealand–Tonga	9.4%	18.2%	0.02%
Russia-Ukraine	2%	—	0.02%
South Africa-Mozambique	11.8%	22.4%	0.02%
South Africa–Zimbabwe	15.8%	19.2%	0.02%
Saudi Arabia–Pakistan	3.3%	3%	0.02%
United Arab Emirates–India	2.5%	13.1%	0.02%
Australia–Papua New Guinea	15.3%	18.1%	0.02%
Germany-Serbia	6.6%	20.9%	0.02%
Japan-Brazil	10.1%	18.1%	0.02%
Malaysia-Indonesia	1.9%	7.1%	0.02%
New Zealand–Tonga	9.4%	18.2%	0.02%

Increasing Injections of Capital

Big venture capital firms are injecting serious capital into bitcoin and blockchain startups. To date, $1.1 billion has been invested into bitcoin related ventures.[62] These include injections of capital all along the transactions chain. While this table only includes publically announced investment; there is significant interest in bitcoin products and services. Over half of the capital

[61]Source: Table was compiled from Ratha (2012) and Bogart (2016).
[62] Source: http://www.coindesk.com/bitcoin-venture-capital/

invested in these technologies has been within 2015. Big banks seem to be interested in blockchain technologies and the draw of trustless operations offered by decentralized distributed ledgers.

Table 6: Venture Capital Investment in Bitcoin Technologies

	Investment by Year	Percent Change
TOTAL - 2012	$2.13	-
TOTAL - 2013	$95.05	4362%
TOTAL - 2014	$361.53	280%
TOTAL - 2015 YTD	$651.17	80%
TOTAL - ALL TIME	$1,110.37	-

Distributed Ledgers

The finance system requires the use of ledgers to settle payments. When individuals and financial institutions seek to move money from one place to another the internal ledgers are either debited or credited. These ledger underpin modern finance to ensure parity between accounts. A problem that these ledgers prevent is double accounting. For example, an individual should not have the ability to sell security A to both person B and person C. Preventing double spending is the first obstacle that any currency must overcome.

When considering this in the development of Bitcoin, Nakamato presented two solution to the problem of double spending. One solution would be a central authority that mints the money and ensure the legitimacy of all transactions. However, such a system is dependent on the central authority or as Nakamato places “the fate of the entire money system depends on the company running the mint” (2). Trust is the undercurrent to such a system and “the stability of the system depends on the trust vested in the central bank as an honest broker and its ability to safeguard the central ledger from tampering or failure” (IMF 18). Typically, most

central authorities maintain the health of their currency. However, there are examples of this not occurring i.e. Weimar Republic and Zimbabwe.

The second solution, is a publicly announced system. In this system "a single history of the order[s] in which they were received" are distributed to all users. The benefits of these system are pervasive. Not only would there be reduced time in financial transactions, there could exist reduce cost. A distributed ledger reduces the time necessary to verify transactions and ensures that records are kept accurately. Thereby, implementation of a distributed ledger would increase efficiency. Some areas of improvement include: reduction in time and costs of international remittances; reduction in settlement times of security trades; and a revamp of online contracts of international remittances; reduction in settlement times of security trades; and revamp of online contracts.[63]

Conclusion

In the short term, Bitcoin has a bright future ahead of itself and we should witness an increase in the price of bitcoin. There are two primary drivers of these short term increases bitcoin. First, those in the developing will shift to bitcoin as a store of value. In particular, we can look to the Latin American nations to adopt bitcoin. The presumed response of Venezuelans, Argentineans, and Brazilians is a substitution towards bitcoin. Second, old financial firms and venture capital has been increasingly investing capital into Bitcoin technologies. In particular,

[63] The IMF addressed the cost of remittances. They claim that the "global average of sending small remittances is 7.7 percent." Conversely, future remittances that use Bitcoin are estimated to be only 1% (21-22). Trading in securities requires the use of clearing houses and can take up to three days. Goldman Sachs has applied for a patent on a "blockchain based settlement system." Blockchain technologies are being used in like manner to develop smart contracts and these "could further enhance the efficiency of transactions and settlements in the security industry" (22). An additional area for growth is land registry. Blockchain-based technologies can be used to ensure that the seller of a property holds the title (19). These are just a few examples; however, the surfaces is just being scratched with what can be accomplished by leveraging blockchain technology.

they are looking at use cases of blockchain technology. The financial driving force could provide the necessary long-term stability to Bitcoin and with could ensure Bitcoin's legitimacy.

Yet, the future is uncertain. The short-term price driver of developing countries demand could only garner a temporary appreciation of bitcoin. However, the perceived long-term driver of interest in the blockchain could spell Bitcoin's doom. It is foreseeable that corporations will take the heart of Bitcoin (the decentralized transferring of property over the internet) and scrap the body (bitcoin the currency itself).

Conversely, bitcoin could take off like a rocket. Developing nations demand; coupled with better financial architecture; further interconnected systems; and increasing capital flows could explode the price of bitcoin. We could be witnessing a paradigm shift in global finance. More money would be in the pockets of the individual as less money is taken out in transaction fees and by third parties.

Closing Remarks:

In an interview with Nathaniel Popper, Benjamin Bernanke lauded Bitcoin by describing, "long-term promise" of "a faster, more secure and more efficient payment system".[64] However, Bitcoin is much more than just an "efficient payment system", it is an extension of one's property in an increasingly globalized and interconnected world. It is one of those technologies that is disruptive and unapologetic about it. It represents creative destruction.

However, my worry is that this is all that will come of Bitcoin. A marginal improvement in payment systems while the large banks will continue to reign. While this is a step forward in the short-term, Bitcoin will not reveal its full paradigm-shifting potential.

That being said, a second thought should be given to bitcoin as a currency:

> Bitcoin is the first time in five thousand years that we have had something better than gold. And it's not a little bit better, it's significantly better. It's much more scarce. More divisible, more durable. It's much more transportable. It's just simply better (Wences Caseres)

The desire to legitimize Bitcoin reintroduces the friction and fees that plague the current financial system. Third-parties are collecting the personal information of customers to satisfy the desires of regulators. They use national security as a boundless warrant to increasingly overreach into our daily lives. Benjamin Franklin once said, "those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety". When did it become the norm to track the transactions between two consenting individuals? Where did the presumption of innocence go?

[64] September 6, 2013 letter to senate committee on homeland security and governmental affairs

My frustrations reside in the fact that Bitcoin is simply a tool. This tool has given individuals the ability to trust counterparties over an inherently untrustworthy system, the Internet. This tool has the power to enable individuals to transact freely. But why is it that is now considered a privilege? The ability to transact freely should be considered a fundamental right. A case can be made that it is even more important than the right to free speech. As Julian Assange said, "where you put your money is where you put your power" (102).

Therefore, it should not come as a shock that some of the most oppressive regimes are the largest detractors of Bitcoin. Totalitarian states like China come out against Bitcoin publically, while its citizens flock to it privately.

The truth is that many fear Bitcoin's potential.

References:

Amundson, I. & Oner, C. (2012). *Back to Basics: What is Money?* International Monetary Fund, Finance & Development. Received from http://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm

Andresen, G. (2015, June 22). *Increase Maximum Block Size*, BIP 101, GitHub Repository. Retrieved from https://github.com/gavinandresen/bips/blob/fd99a8ce04dbad96fb275e0300a7ee669e70f418/bip-0101.mediawiki

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in bitcoin. In *Financial Cryptography and Data Security* (pp. 34-51). Springer Berlin Heidelberg.

Assange, J., Appelbaum, J., Muller-Magnum, A., & Zimmermann, J. (2012). *Freedom and the Future of the Internet*. New York, NY: OR Books.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better—how to make bitcoin a better currency. In *Financial cryptography and data security* (pp. 399-414). Springer Berlin Heidelberg.

Barnato, K. (2015, August 19). *Greece could soon get 1,000 Bitcoin ATMs*. Retrieved from http://www.cnbc.com/2015/08/19/greece-could-soon-get-1000-bitcoin-atms.html

Barrett, B. (2016, February 16). *Hack Brief: Hackers are holding an LA Hospitals Computers Hostage*. Retrieved from http://www.wired.com/2016/02/hack-brief-hackers-are-holding-an-la-hospitals-computers-hostage/

Bello Perez, Y. (2015, August 13) *The Real Cost of Applying got a New York BitLicnese*. Retrieved from http://www.coindesk.com/real-cost-applying-new-york-bitlicense/

Bitcoin ATM Radar (n.d.) Retrieved from http://coinatmradar.com/charts/#fees

Bitcoin Community War. (2016, February 28). *How a Peaceful Bitcoin Community Turned to Savage War*. Retrieved from http://www.blockcy.com/how-bitcoin-community-turned-to-war#

Bitcoin Mining Pools. (n.d.). Retrieved from https://www.bitcoinmining.com/bitcoin-mining-pools

Bogart, S. (2016). *Bitcoin Investment Trust (GBTC): Byte-ing Down Barriers with Bitcoin*. Needham & Company.

Bohme, R., Christin, N., Edelman, B., & Moore, T. (2015). *Bitcoin: Economics, Technology, and Governance*. In Journal of Economic Perspectives. Vol 29(2).

Buntinx, J. P. (2016, March 29). *MedStar Washington Potentially Affected by Bitcoin Ransomware.* Retrieved from http://www.newsbtc.com/2016/03/29/medstar-washington-affected-bitcoin-ransomware/

Cameron-Huff, A. (2016, April 9). *Regulating Blockchain would be an Exercise in Futility*. Retrieved from http://www.coindesk.com/dont-need-blockchain-regulation/

Chepel, A. (2015, May 1). *Chinese bitcoin exchange market continues to grow: BTCChina, OKCoin, Huobi*. Retrieved from http://www.coinfox.info/news/reviews/1958-chinese-bitcoin-exchange-market-continues-to-grow-btc-china-okcoin-huobi

Courtois,N., Grajek, M., & Naik, R. (2012) "Optimizing SHA256 in Bitcoin Mining"

Courtois, N. & Bahack, L. (2014). *On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency*

Davidson, J. (2015, Jan 9). *Businesses like Microsoft, Dell, and Expedia say they accept bitcoin as payment*. But that's not quite accurate. Retrieved from http://time.com/money/3658361/dell-microsoft-expedia-bitcoin/

Das, S. (2015, December 23). *Reuters: Bitcoin Price Likely to Scale to Record Highs in 2016*. Retrieved from https://www.cryptocoinsnews.com/bitcoin-headlines-reuters-publishes-a-bitcoin-price-article-predicting-record-highs-in-2016/

Del Castillo, M. (2016, March 30). *Microsoft adds Ethereum to Windows Platform for over 3 Million Developers*. Retrieved from http://www.coindesk.com/microsoft-ethereum-3-million-developers/

Del Castillo, M. (2015, August 12). *The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem*. Retrieved from http://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.html

Evans, B. (2014) "How Mobile is Enabling Tech to Outgrow the Tech Industry" Andreessen Horwitz

Friedman, M. (1960). *A Program for Monetary Stability*. New York, NY: Fordham University Press.

Goldman Sachs Investment Research (2014). "Interview with Fred Ersham," Top of Mind 21, 8, March 11.

Hajdarbegovic, N. (2014, November 24). *Analysis: Around 70% of Bitcoins Unspent for Six Months or More*. Retrieved from http://www.coindesk.com/analysis-around-70-bitcoins-dormant-least-six-months/

He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., ... & Verdugo-Yepes, C. (2016). *Virtual Currencies and Beyond: Initial Considerations* (No. 16/3). International Monetary Fund.

Hearn, M. (2016, January 14). *The Resolution of the Bitcoin Experiment*. Retrieved from https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.6d7jkxesw

Heilman, E. *One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner*.

Jenn, S. (2016, March 31). *Bitcoin Price Technical Analysis for 03/31/2016 – Symmetrical Triangle Intact*. Retrieved from http://www.newsbtc.com/2016/03/31/bitcoin-price-technical-analysis-03312016-symmetrical-triangle-intact/

Kaminsky, D. (2011). *Black Ops of the TCP/IP Presentation*. Black Hat, Chaos Communication Camp, 2011 Received from https://dankaminsky.com/2011/08/05/bo2k11

Karame, G. O., Androulaki, E., & Capkun, S. (2012, October). Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 906-917). ACM.

Kenya Mobile Money. (2013, May 27). *Why does Kenya lead the World in Mobile Money?* Retrieved from http://www.economist.com/blogs/economist-explains/2013/05/economist-explains-18

Khaliq, A. (n.d.). *10 Best Bitcoin Wallets for Secure Bitcoin Storage*. Retrieved from http://www.hongkiat.com/blog/bitcoin-wallets/

Khaosan, V. (2014, June 8). *How a Bitcoin Transaction Works*. Retrieved from https://www.cryptocoinsnews.com/bitcoin-transaction-really-works/

Krause, M. (2016). Bitcoin: Implications for the Developing World.

Kroll, J., Davey, I., & Felten, E. (2013). *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries.* In Proceedings of WEIS 2013.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, *4*(3), 382-401.

Lo, S., & Wang, C. (2014). Bitcoin as Money? *Current Policy Perspectives* Vol 14(4), 1-28.

Market Cap (n.d.) *Crypto-Currency Market Capitalizations*. Retrieved from http://coinmarketcap.com/

Marron, D. (2013, September 3). How Bitcoin spreads violate a Fundamental Economic Law. Retrieved from http://www.forbes.com/sites/beltway/2013/09/03/how-bitcoin-spreads-violate-a-fundamental-economic-law/

Marshall, R. (2016). Bitcoin: Where two worlds collide. *Bond Law Review*, *27*(1), 5.

Metz, C. (2016, February 11). *The Schism over Bitcoin is How Bitcoin is supposed to Work*. Retrieved from http://www.wired.com/2016/02/the-schism-over-bitcoin-is-how-bitcoin-is-supposed-to-work/

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

O'brien, M. (2015, June 8). *Bitcoin isn't the future of money – it's either a Ponzi scheme or a pyramid scheme*. Received from https://www.washingtonpost.com/news/wonk/wp/2015/06/08/bitcoin-isnt-the-future-of-money-its-either-a-ponzi-scheme-or-a-pyramid-scheme/

Popper, N. (2016, March 27). *Ethereum, a Virtual Currency, Enables Transactions that Rival Bitcoin's*. Retrieved from http://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables-transactions-that-rival-bitcoins.html?_r=1

Popper, N. (2015). *Digital Gold: Bitcoin and the Inside Story of The Misfits and Millionaires Trying to Reinvent Money*. New York, NY: HarperCollins Publishers.

Ratcliff, J.W. (2014, June 22). *Rise of the Zombie bitcoins*. Retrieved from https://letstalkbitcoin.com/blog/post/rise-of-the-zombie-bitcoins

Ratha, D. (2012). *Remittances: Funds for the Folks Back Home*. International Monetary Fund, Finance & Development. Received from http://www.imf.org/external/pubs/ft/fandd/basics/remitt.htm

Reid, F., & Harrigan, M. (2013). *An analysis of anonymity in the bitcoin system* (pp. 197-223). Springer New York.

Sanchez, D. (2015, December 16). *Technophobia or Prohibition? Kenya Says No to Bitcoin*. Retrieved from http://afkinsider.com/108568/technophobia-prohibition-kenya-says-no-bitcoin/#sthash.DGHFBjGh.dpuf

Shasky Calvery, J.(2013, November 19). *Statement to the United States Senate, Committee on Banking, Housing, and Urban Affairs.* Retrieved from https://www.fincen.gov/news_room/testimony/html/20131119.html

Sing, S., & Vega, A. (2016, March 16). *Why Latin American economies are turning to* Bitcoin. Retrieved from http://techcrunch.com/2016/03/16/why-latin-american-economies-are-turning-to-bitcoin/

Surda, P. (2012). *Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold* (Doctoral dissertation, Diploma thesis submitted at WU Vienna University of Economics and Business).

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O'Reilly Media, Inc.

The trust Machine: The technology behind bitcoin could transform how the economy works (*2015, October 31*). *The Economist.*

Tepper, F. (2015, October 27). *Barry Silbert Launches Digital Currency Group with Funding from MasterCard, Others*. Retrieved from http://techcrunch.com/2015/10/27/barry-silbert-launches-digital-currency-group-with-funding-from-mastercard-others/

Torpey, K. (2015, November 30). *Gyft's Vinny Lingham: Growth of New Bitcoin Users has Slowed*. Retrieved from http://insidebitcoins.com/news/gyfts-vinny-lingham-growth-of-new-bitcoin-users-has-slowed/36043

Vyas C. & Lunagaria, M. (2014). *Security Concerns and Issues for Bitcoin.*

Wilson, F. (2016, March 13). *The Second Smartphone Revolution*. Retrieved from http://avc.com/2016/03/the-second-smartphone-revolution/

Yermack, D. (2013). *Is Bitcoin a real currency? An economic appraisal* (No. w19747). National Bureau of Economic Research.