COMPLICATIONS OF CRYPTOCURRENCY: FINANCIAL AND CYBERSECURITY RISK IN THE AGE OF BITCOIN

by

Jolana Kubicek

A Capstone Project Submitted to the Faculty of

Utica College

April 2018

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

Abstract

Bitcoin, the forerunner of cryptocurrencies, was coincidentally introduced at a time when the global financial marketplace was in the midst of a crisis. The decentralized, pseudo-anonymous financial system presented an alternative to the status quo. While shaking up the concept of currency, this alternative financial system has not taken popular hold. The purpose of this study was to investigate the intricacies of Bitcoin and how financial and security concerns have slowed widespread investment. This research examined limitations of the Bitcoin system to assist in interpreting the scope of financial and security risks inherent in the market.

This research discovered how the Bitcoin system innately fosters financial risk. In the cryptocurrency market, trust is essential to maintaining value and Bitcoin's price volatility brings economic risk to investors. The lack of price stability and lack of complete anonymity restrict wider adoption of the cryptocurrency. Security breaches also undermine user confidence in Bitcoin. Online criminals are lured in by the same features that draw investors, decentralization and ease of access. While the Bitcoin system itself is highly secure, third-party intermediaries, that Bitcoin users rely on, have become points of failure.

This research recommended, while prices remain volatile, investors secure themselves by limiting large investments in Bitcoin. The research pointed to a need to increase user confidence by stabilizing Bitcoin prices, but how remains elusive. Expanding Bitcoin as a method of payment among businesses could lead to potential users. Improving security, through cybersecurity self-awareness and via cryptocurrency advisors, would reduce vulnerability to Bitcoin theft and loss. For the first time, investors are their own bank.

Keywords: Cybersecurity, Professor Donnie Wendt, Satoshi Nakamoto, digital currency, blockchain, decentralization, digital fortune.

Acknowledgements

I found that juggling the demands of graduate school, along with parenthood, can be a struggle. The biggest challenge to writing a master's thesis was the change in life patterns which resulted in more hibernation, lack of use of my gym membership, and a reliance on my young sons to peacefully play, on some demanding weekend afternoons. Hopefully, to my sons, I was a role model in how to work hard to achieve your goals, especially with regards to academics.

I would especially like to thank my professors at Utica College for persevering and being supportive, when diligence was required, and for having faith in seeing my master's thesis to the end. This was a stimulating project, for its contemporary relevance, and my own curiosity regarding Bitcoin. As the research began, the more apparent became the complexities of cryptocurrencies. Perhaps you will find me in line to buy Bitcoin…will you be joining me?

Table of Contents

List of Illustrative Materials

Introduction

"Bitcoin is a form of digital currency, created and held electronically. No one controls it. Bitcoins aren't printed like dollars or Euros - They're produced by lots of people running computers all around the world, using software that solves mathematical problems. It is the first example of a growing category of money known as cryptocurrency" (Williams, 2014, para. 7).

The Meaning of Currency

In most of the 19th and 20th centuries, currencies were transferrable into gold or other precious metals (Yermack, 2013). The connection between currency and gold created confidence in the value of the currency (Yermack, 2013). Between the 1920s and 1970s, the gold standard was replaced by paper fiat currency for almost every major economy, due to economic growth (Yermack, 2013). The value of fiat currency is based on the public belief that the government, or central bank, will not overproduce the supply of banknotes (Yermack, 2013).

All types of currencies share common problems of stability, control, and susceptibility to inflation (Martins & Yang, 2011). Over time, the value of a currency \will depreciate, as prices increase (Martins & Yang, 2011). If governments are too strained by public finances, their fiat currencies can deflate to worthlessness (Yermack, 2013). Problems can also arise if prices rise beyond the means of the people. The currency should also not be susceptible to great swings in exchange rate fluctuations, particularly under the control of one single party (Martins & Yang, 2011). The creation of Bitcoin, a cryptocurrency, tried to address weaknesses found in both fiat and gold-based currencies (Yermack, 2013).

Cryptocurrencies

Cryptocurrencies, also known as virtual or digital currencies, are electronic currencies designed to be secure and intended to enable anonymous transactions (Field & McGoogan, 2017). The currency uses cryptography to convert information into almost uncrackable codes, for tracking transactions (Field & McGoogan, 2017). The two major differences between cryptocurrency and traditional currency are that cryptocurrencies are not issued by a government, and the total amounts in circulation are designed to be limited (Tillier, 2018). Cryptocurrencies can be bought in online marketplaces, be sent to digital wallets in exchange for online goods and services or be used to buy goods and property. The first cryptocurrency on the market was Bitcoin. Currently competing with over one thousand other cryptocurrencies, Bitcoin has maintained the position as the leading form of cryptocurrency in the world (Gandal, Hamrick, Moore, & Oberman, 2018).

Bitcoin is a decentralized, peer-to-peer (P2P) electronic cash system that was designed, and introduced, in a self-published paper in October 2008, by an unidentified person, using the pseudonym Satoshi Nakamoto (Nakamoto, 2008). The key innovation of Bitcoin is decentralization, as one sole entity does not control the money (Dziembowski, 2014). Transactions, designed to be irreversible, occur directly between peers and are verifiable through network nodes (Corbet, Lucey, & Yarovaya, 2017). Assumptions within Bitcoin are that a majority of network nodes are honest, to prevent double spending and for dispute resolution (Barber, Boyen, Shi, & Uzun, 2012).

Traditionally, online financial transactions have relied on a third-party, such as a bank or credit card company, to ensure the electronic transfer of money (Martins & Yang, 2011). There is an element of trust in the third-party institution, that the third-party verifies ownership of

assets prior to transfer. The third-party also assumes the risk of fraud, chargebacks, and assumes the cost of collecting information, to safeguard the system's security. Establishing an electronic, trust-based system without a governing body to regulate, and secure, transfers is challenging. Rather than rely on trust, Bitcoin relies on proof, which is similar to how cash transactions are handled (Martins & Yang, 2011). Bitcoin's cryptography relies on authenticating coin ownership. A significant distinction between the digital currency and traditional, fiat currency is that Bitcoin's authenticity can be confirmed (Martins & Yang, 2011).

Public interest in cryptocurrencies, including Bitcoin, began gradually. Bitcoin's initial introduction was, coincidentally, during the time of the global financial crisis in 2008-2009 (Yermack, 2013). But Bitcoin did not begin to be seriously considered in world financial news until 2013 and the beginning of 2014, about five years following its initial release in 2009 (Yermack, 2013). At its onset, Bitcoin was trading at fewer than five cents in 2010 (Yermack, 2013). In February of 2018, the market capitalization of Bitcoin had grown to approximately $180 billion and over 198, 455 transactions were estimated on February 19th, 2018 (Blockchain, 2018; CoinMarketCap, 2018).

Bitcoin interacts with the traditional banking system, and the economy, and is changing how users think about currency. Although coined a cryptocurrency, economists have questioned whether using the term currency for Bitcoin is misleading, as it affects legal considerations such as taxes and insurance (Yermack, 2013). To economists, currency typically must have three attributes: functions as a medium of exchange, stores value, and is a unit of account (Yermack, 2013). According to the standards of many economists, Bitcoin fails to meet all the criteria (Yermack, 2013). Although Bitcoin transactions are increasing for alternate forms of payment, early retailers who adopted digital currencies have tapered off (Mulqueen, 2018). Price quotes in

Bitcoin typically refer to an amount of conventional currency, making economists consider Bitcoin as a payment platform, rather than currency (Boehme, Christin, Edelman, & Moore, 2015). Economists tend to believe Bitcoin functions more like a speculative investment, which is also how most users treat Bitcoin, rather than as a method of payment (Boehme et al., 2015; Yermack, 2013).

By design, the amount of Bitcoin to ever be accepted into cryptocurrency is fixed, to 21 million Bitcoin, and the last Bitcoin will be released in 2140 (Yermack, 2013). As of March 12th, 2018, there were nearly 17 million Bitcoin already in circulation (Blockchain, 2018). This makes Bitcoin the first monetary design to have an absolute scarcity of money supply (Boehme et al., 2015). The market value of Bitcoin is determined by the supply of circulating Bitcoins and the desire for users to hold or trade the currency (FBI, 2012). The circulation of Bitcoin cannot be affected in the same way as the U.S. dollar currency, as Bitcoin is tied to mathematics and cryptography and, in general, U.S. regulators have been relatively benign towards the cryptocurrency (Yermack, 2013).

Bitcoin seemed to answer traditional impediments to digital payments, via online banking, such as the need for a trusted server for transactions, high transaction fees and a lack of anonymity (Dziembowski, 2014). Bitcoin does not utilize a trusted server, so money is allowed to circulate, uses low fees and is pseudo-anonymous (Dziembowski, 2014). The irreversibility of transactions has attracted vendors to Bitcoin, whose concerns are over credit-card fraud and chargebacks (Barber et al., 2012).

Initial interest in Bitcoin was primarily among the Information Technology (IT) community, but spread in 2010, so that Bitcoin was being traded on the Japanese-based online exchange known as Mt. Gox (Yermack, 2013). The first purchase of commercial goods, using

Bitcoin, was for two pizzas in 2009, by way of a third-party broker who purchased the pizzas for 10,000 Bitcoins. At the current exchange rate, that many Bitcoins would be valued at over 87 million USD (Coindesk, 2018). This is characteristic of Bitcoin commerce, in that middlemen facilitate the exchange of Bitcoins into conventional currency, and how Bitcoin exchange rate fluctuations can make the prices of goods vary (Yermack, 2013).

There are multiple reasons for the appeal to Bitcoin, from ideology, timing in the market, pseudo-anonymity for trading illegal goods, low transaction fees, to hype and popularity, particularly in some non-democratic nation-states (Dziembowski, 2014). The Silk Road, an online market place where contraband items could be bought only by Bitcoin, enabled the spread of Bitcoins and connected the idea of Bitcoins to the underground community (Yermack, 2013). Bitcoin has appealed to technology aficionados who believe Bitcoin's value will rise due to its advantages in online commerce, libertarian political believers who prefer the lack of government involvement and strengthened financial self-empowerment, to users who anticipate Bitcoin's role in an oncoming monetary revolution (Clinch, Davies, Khairuddin, & Sas, 2016; Yermack, 2013). Important to the motivation for using and buying Bitcoins is the perceived social and future financial impact it will bring (Clinch et al., 2016). An online survey in 2013 revealed the average Bitcoin user was 32.1 yrs. old, male (95.2%), libertarian/anarcho-capitalist (44.3%), non-religious (61.8%), employed full-time (44.7%), and in a relationship (55.6%) (O'Malley & Presthus, 2017).

Background: Making Sense of Bitcoin

Satoshi, as the community refers to Satoshi Nakamoto, envisioned the P2P electronic cash system of Bitcoin would generate new Bitcoins by computer users who would solve complex, mathematical problems (Yermack, 2013). Miners, as these initial owners are referred

to, are incentivized for their work by receiving a reward of transaction fees and new Bitcoins, which are appended to the blockchain using a proof-of-work (Corbet et al., 2017; Dziembowski, 2015). This reward system provides incentives to be a miner and for new blocks to be announced, as soon as they are discovered (Dziembowski, 2015). On average, this occurs approximately every ten minutes (Kelly, 2017). Since Bitcoin is limited to 21 million Bitcoins, the expansion of the currency is controlled, to prevent devaluation. Each Bitcoin can be further divided into Satoshis. One Bitcoin is equivalent to 100,000,000 Satoshis (Bulgakov, 2014).

As the price, and demand, of Bitcoin has risen, the mathematical problems automatically become more complex, in computing power and electricity needs (Boehme et al., 2015). After Bitcoin is mined, the Bitcoin is added to the public transaction ledger, known as the blockchain, which tracks the exchanges of every Bitcoin, so the quantity and growth rate of Bitcoins are visible to all the users (Yermack, 2013). Every new transaction posted to Bitcoin is periodically grouped into a block of recent transactions, which verifies the transaction is final (Boehme et al., 2015).

The new block is then compared to the most recently posted block, which enables users to verify the authenticity of previous transactions, as shown in Figure 1 (Boehme et al., 2015). Figure 1 illustrates transaction flow and validation, amongst miners and peers, in Bitcoin. The recommendation is to consider a Bitcoin transaction final after six confirmations, to assure the transaction is permanently in the blockchain (Boehme et al., 2015). Each Bitcoin can be traced back through all its previous transactions, to the onset of its circulation, and all transactions are transparent to the users, along with the public keys (Boehme et al., 2015). The veracity of the blockchain is the core of the Bitcoin network.

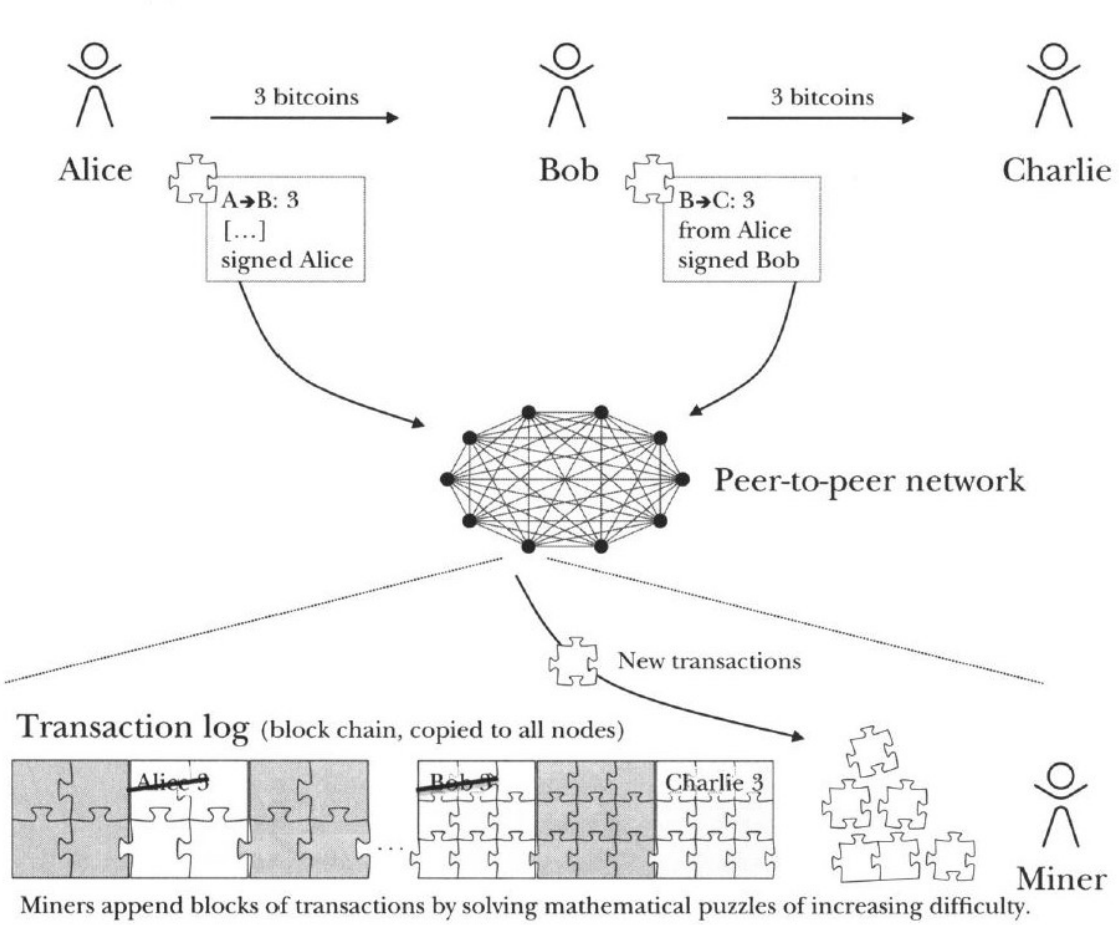


Figure 1. Bitcoin's transaction flow and validation. Adapted from "Bitcoin: Economics, Technology, and Governance," by R. Boehme, N. Christin, B. Edelman, and T. Moore, 2015, *The Journal of Economic Perspectives*, p. 216. Copyright 2015 by the American Economic Association.

Digital Wallets

To use Bitcoin, the user initially needs to download and install the free Bitcoin software (FBI, 2012). Using Public Key Cryptography (PKI), also known as asymmetric encryption, the application will create a Bitcoin address, which is a 36-character alphanumeric password, used for sending or receiving Bitcoins (FBI, 2012). Instead of being deposited into a bank account, the Bitcoin address is stored in the user's digital wallet, on their file system (FBI, 2012). Digital wallets hold Bitcoin accounts, a record of transactions, and the cryptographic keys for

transactions (Boehme et al., 2015). Once the digital wallet and Bitcoin address are created, the user has a node in the P2P Bitcoin network and access to the blockchain (Boehme et al., 2015). As of February 20th, 2018, the blockchain was over 157 GB (Blockchain, 2018).

Public-private key cryptography stores and spends Bitcoins, while cryptography, using digital signatures, validates the transactions (Boehme et al., 2015). Each Bitcoin address is connected to a pair of private and public keys (Miller, 2015). In the blockchain, no two addresses hold the same private and public keys (Miller, 2015). A user can generate multiple public keys, whose addresses can also be associated with multiple wallets (Conti, Kumar, Lal, & Sushmita, 2017).

To send Bitcoin, users input the Bitcoin address where they want it sent and the amount to transfer (FBI, 2012). After confirming a transaction request with a user's private key, which is used as a digital signature, the transaction is declared to the P2P network with a public key, for verification, as shown in Satoshi's depiction in F (Conti et al., 2017). Figure 2 illustrates the progression of ownership, and transfer of public and private keys, in Bitcoin transactions. The P2P network verifies the ownership of the Bitcoins, which prevents double spending (FBI, 2012). Once the irreversible transaction is validated by the Bitcoin network, the receiver can spend the Bitcoins. The private key is necessary to spend, and transfer, Bitcoins from one wallet to another (Conti et al., 2017). Bitcoins whose private keys are forgotten, or destroyed, can never be replaced, which shrinks the available Bitcoin base (Barber et al., 2012).

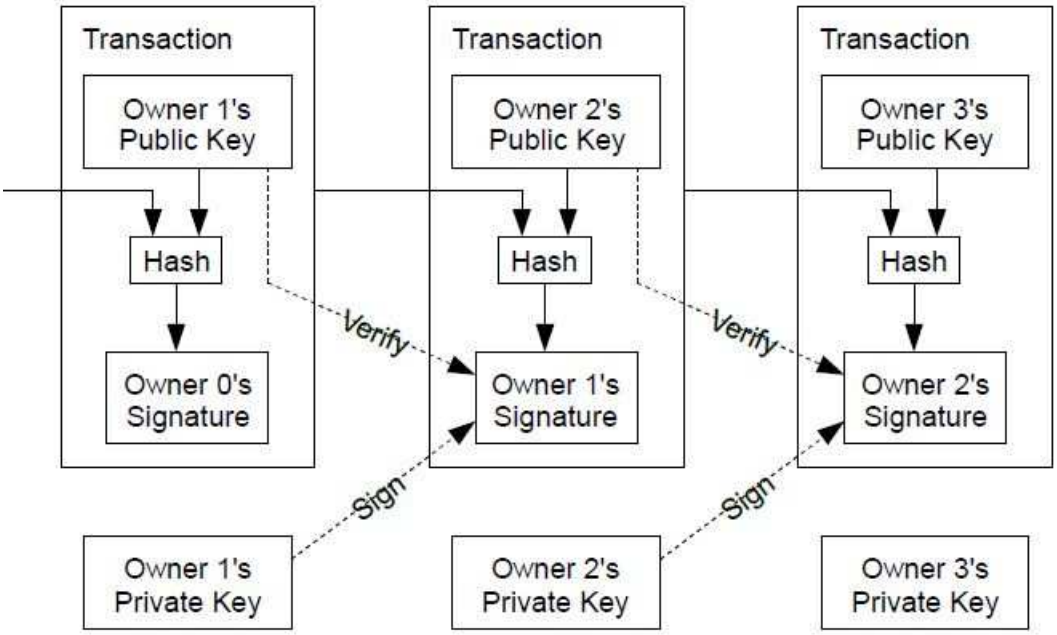


Figure 2. The chain of ownership. Adapted from "Bitcoin: A Peer-to-Peer Electronic Cash System," by S. Nakamoto, 2008, *www.bitcoin.org*, p. 2. Copyright 2008 by bitcoin.org.

Popular among Bitcoin users is to use a digital wallet service, which provides access on a shared server, via the Internet or phone-based applications (Boehme et al., 2015). For users to trade Bitcoins to traditional currency, from their digital wallet, users must also use currency exchanges, which charge a commission (Boehme et al., 2015). The use of digital wallet services, in turn, increases centralization.

Statement of the Problem

Cryptocurrencies are virtually transforming the financial landscape. In 2008, Satoshi Nakamoto's vision of a P2P electronic cash system, or Bitcoin, strived for an advantage in allowing online transactions, while bypassing trusted, third-party financial institutions (Nakamoto, 2008). Relying on cryptography over trust would enable a flow of ecommerce to pass simply between two parties, negating the ability to dispute transactions and protecting sellers from being deceived (Nakamoto, 2008). But, there were concerns over privacy as Bitcoin involved public transactions. Satoshi upheld public keys would be anonymous and created for each transaction, so transactions could not be linked to individuals (Nakamoto, 2008).

Today, Bitcoin is the leading type of cryptocurrency in the world (M., 2017). However, this has not stopped its uncertainty and volatility, as Bitcoin hinges upon participant belief in its value (Clinch et al., 2016; Dziembowski, 2014). Without that faith, Bitcoin has no value. Bitcoin is a highly speculative investment, as returns have been estimated to be 26 times more volatile than the S&P 500 index (Corbet et al., 2017). The year 2017 was particularly a year of volatility for the cryptocurrency. On Jan 1, 2017, Bitcoin was trading at $960.79 per coin and on Dec 4, 2017, around $11,500 per coin (Heath, 2017). This is a price increase of over 10 times, in less than one year (Heath, 2017).

Not only are Bitcoin users vulnerable to the volatility of the cryptocurrency market, but also to security risks. Security is a concern, and weakness, for Bitcoin. The first concern regards privacy, as Bitcoin indirectly enables identification. Bitcoin is not anonymous, as Satoshi envisioned, but technically pseudo-anonymous, as every transaction is public and visible to others on the shared, cryptographically protected ledger called the blockchain (Field & McGoogan, 2017; Jordan, Levchenko, McCoy, Meiklejohn, Pomarole, Savage, & Voekler,

2013). The level of pseudo-anonymity is maintained merely by the ability to link a person with their Bitcoin wallet, which is essential for transactions (Steadman, 2013). Transactions can also be successfully linked to the user when Bitcoin is bought, or sold, for legal tender on the currency exchange (Bonneau & Goldfeder, 2017).

The second security concern regards malicious hackers. Prior to the explosion in Bitcoin's value in about 2016–2017, Bitcoin plunged in 2014, when Mt Gox, the Bitcoin exchange which handled 70 percent of Bitcoin transactions, shut-down after reporting $450 million worth of Bitcoin was stolen by malicious hackers (Dziembowski, 2014; Morris, 2017a). The online environment of Bitcoin, as well as Bitcoin's decentralization, make Bitcoin appealing to malicious hackers. A positive facet of Bitcoin's decentralization is that Bitcoin facilitates transactions, but the transactions cannot be reversed, nor are the transactions regulated (Dziembowski, 2014; Nakamoto, 2008). The criminal element takes advantage of the pseudo-anonymity of Bitcoin, for payments, and Bitcoin's decentralized nature, which forces users to seek out potentially insecure third parties to manage their Bitcoin. Criminal hackers have targeted individuals, to steal their Bitcoin, by utilizing methods such as social engineering, stealing passwords through storage devices, exploiting browser security flaws, spam mail campaigns that spread malware and smartphone exploits, among others (Dascalescu, 2017; Roberts, 2017). Blockchain tracking company Chainalysis estimates over three million Bitcoins have been permanently lost, which is approximately 14 percent of the currency (Nova, 2018).

Purpose of the Study

The purpose of this study is to identify, and discuss, financial and cybersecurity aspects of the cryptocurrency market, specifically concerning Bitcoin. This research will examine key, financial risk factors of cryptocurrency markets that differentiate Bitcoin from traditional,

financial markets. The research will study the limitations on anonymity in the Bitcoin market and the cybersecurity vulnerabilities caused by the lack of privacy. This research will also investigate cyber threats from the online environment, as well as threats that make Bitcoin particularly appealing, and susceptible, to malicious online users. This research will examine supporting literature, to decipher to what extent financial and cybersecurity risks can be mitigated, and to recognize how cybersecurity measures can be applied for user protection in navigating the vulnerable, cryptocurrency market of Bitcoin.

Research Questions

This research will address four key questions related to Bitcoin:

Q1. What elements of the unpredictable Bitcoin market bring financial risk to the user?

Q2. To what extent is Bitcoin anonymous and what risk does the lack of anonymity bring to the user?

Q3. What are the cybersecurity threats to Bitcoin, caused by those typically found in the online environment, as well as online threats specific to cryptocurrency?

Q4. What protective, cybersecurity measures can users implement to mitigate risk?

Literature Review

"Virtual currencies, perhaps most notably Bitcoin, have captured the imagination of some, struck fear among others, and confused the heck out of the rest of us" - Thomas Carper, U.S. Senator of Delaware (Ivanecky, 2018, para.15).

The general perception of Bitcoin is that it is a highly secure, decentralized type of virtual currency which is supported by strong, military-grade cryptographic algorithms (Merkle, 2017). But vulnerabilities in the Bitcoin system are prevalent, especially for novices to cryptocurrencies. The opportunities for making a fortune in Bitcoin are alluring to novices, enticing users who are unprepared for the financial and cybersecurity risks involved. This study has included research from numerous sources, including scholarly journal articles, research findings, conference proceedings, industry reports, and online news coverage, to review elements of the cryptocurrency market that make Bitcoin investors vulnerable.

This study begins with an analysis of the financial risk involved in the Bitcoin market. As a cryptocurrency, this research analyzes how value is determined by a financial system that seems abstract to users familiar with only traditional, financial markets. A cursory glance at the reaction of financial markets to the rise of Bitcoin is discussed. This research evaluates how Bitcoin price is largely determined and covers various, scientific perspectives on why the Bitcoin market is so unpredictable and volatile.

This research then explores the cybersecurity aspects of Bitcoin. The public nature of the blockchain, in Bitcoin, poses a threat to privacy and this study discusses methods in which that threat has been exploited and how investors can mitigate online exposure. Cybersecurity risks in Bitcoin will be discussed, such as why malicious hackers find the Bitcoin market particularly appealing, methods by which malicious hackers have stolen user accounts, and system structures

in Bitcoin which make it vulnerable to attack. This study will end by discussing protective, cybersecurity measures investors can implement to safeguard themselves against theft or loss of Bitcoins.

Prospects of Digital Gold

"You can't have a business where people can invent a currency out of thin air and think that the people who are buying it are really smart," - Jamie Dimon, Chief Executive Officer (CEO) of JPMorgan Chase & Co (Hickey, 2017, para. 1).

The cryptocurrency market is appealing for its innovative concepts, simplicity, transparency, and rise in popularity (Katsiampa, 2017). Bitcoin did not emerge out of cryptocurrency competition, but became dominant, as a pioneer, in the cryptocurrency market. In March of 2018, Bitcoin dominance in the cryptocurrency market was nearly 40 percent (Harper, 2018). As the most successful cryptocurrency through March of 2018, Bitcoin's innovation has provided challenges, and opportunities, to policymakers, economists, financial advisors, and consumers (Katsiampa, 2017).

While security experts and programmers have focused on security issues, policy administrators, as well as bankers, are concerned with the impact of Bitcoin on the global, financial system (Iwamura, Kitamura, & Matsumoto, 2014a; Iwamura, Kitamura, Matsumoto, & Saito, 2014b). In today's economy, the influence of the digital market on financial services is negligible (Committee on Payments and Market Infrastructures, 2015). But, as Ben Bernanke, chairman of the Federal Reserve Board commented, there could be profound impacts on the payments system in the long-run (Iwamura et al., 2014a).

Although termed a *currency,* Bitcoin does not meet the three criteria for standard currency: medium of exchange, unit of account, and store of value. Bitcoin is minimally

accepted as a medium of exchange, for example, purchasing products online (Bariviera, Basgall, Hasperuéb, & Naiouf, 2017). Bitcoin imparts risk to businesses that accept it for transactions, as with any other currency (Yermack, 2013). Major companies that typically deal with more than one currency, such as multinationals, can protect themselves against risks related to currency changes, which is not possible in the Bitcoin market (Yermack, 2013). Bitcoin transactions are also risky, due to the absence of basic consumer protection, such as refunds (Yermack, 2013). In addition, there is no Federal Deposit Insurance Corporation (FDIC) to protect assets, in case of loss or theft. The wild fluctuations in value and issues of privacy are also limiting factors (Sabin, 2018).

Medium of exchange indicates payment for items and that the value is trusted (Thompson, 2017). Although Bitcoin automated teller machines (ATMs), which allow cryptocurrency to be exchanged for cash, have appeared, people still view Bitcoin as a very risky currency for normal transactions (Alvarez-Ramirez, Ibarra-Valdez, & Rodriguez, 2018). In comparison to traditional currencies, there are large price jumps and excessive volatility. Bitcoin cannot function currently on a national scale, due to the limited transactions per minute the Bitcoin system can support (Sabin, 2018). While Bitcoin can handle only seven transactions per second, VISA's credit card network can handle 65,000 transactions per second (Sabin, 2018). Bitcoin is still mainly viewed as an asset, rather than currency (Katsiampa, 2017).

Bitcoin is not used as a unit of account, as there are no financial statements valued in Bitcoin (Bariviera et al., 2017). Unit of account indicates income can be measured in fiat currency (Thompson, 2017). Lastly, volatile price swings, in the Bitcoin market, prevent Bitcoin from being considered suitable to be a store of value (Bariviera et al., 2017). Store of value indicates dollars, or money, can be in a wallet and will not *go bad* (Thompson, 2017).

Bitcoin and the financial sector. In December of 2017, the U.S. commodities regulator, the U.S. Commodity Futures Trading Commission (CFTC), issued a customer advisory to alert the public to the risks related to investing, or speculating, in virtual currencies, including the most recently initiated Bitcoin futures and options trading (U.S. Commodity Futures Trading Commission, 2017). Bitcoin became more mainstream in the financial sector, when the Chicago Mercantile Exchange and Chicago Board Options Exchange received approval from the CFTC to begin trading Bitcoin futures (Nova, 2017b).

The launch of Bitcoin futures is expected to make the market less volatile and could also be the next step towards Bitcoin being established as a legitimate asset class (Cheng, 2017). The Nasdaq Stock Market will also start a Bitcoin futures site in 2018 (Heath, 2017). The CFTC does not consider virtual currency, such as Bitcoin, to have the status of legal tender, but rather to be a commodity cash market (CFTC, 2017). However, the U.S. Securities and Exchange Commission (SEC) leans towards classifying Bitcoin as a security, trying to push towards regulation (Duggan, 2017).

When investors purchase stocks, bonds, debt, and interest, in companies or governments, the investments are securities (Thomson Reuters, 2018). When investors purchase natural resources, such as oil, gas, coal, and agricultural products, the investments are commodities (Thomson Reuters, 2018). Purchasing stock buys a share in a corporation's ownership, while purchasing commodities entails purchasing goods, at a set price, prior to their existence (Thomson Reuters, 2018).

In contrast to typical commodities, however, cryptocurrencies have zero intrinsic value (Committee on Payments and Market Infrastructures, 2015). The value in cryptocurrencies is derived only from the users' expectations that they might be exchanged for other goods or

services, or a certain amount of currency, at a later date (CPMI, 2015). Bitcoin is mainly used for investment, and investors hope for huge financial potential in the Bitcoin market is what drives up Bitcoin prices.

Not surprisingly, the financial community has high-profile skeptics on whether Bitcoin holds any value. Known as one of the most successful investors of all time, Warren Buffet, famously called Bitcoin a "mirage" (Duggan, 2017, para. 11) and stated cryptocurrencies would "come to a bad ending" (Forbes, 2018; Kharpal, 2018, para. 9). JPMorgan Chase & Co. CEO Jamie Dimon called Bitcoin a "fraud" (Duggan, 2017, para. 11), while UBS Group AG coined Bitcoin as the "biggest speculative bubble in history" (Liedtka & Schatzker, 2017, para. 6). Deutsche Bank cited a crash in the Bitcoin price as a risk to the stock market in 2018, while other top European economists do not think Bitcoin is, nor will become, a threat to stability in the financial system (Duggan, 2017; Morris, 2017b). The CTFC states Bitcoin is risky for various reasons. Bitcoin's lack of regulation, lack of basic cash market system safeguards, lack of consumer protection, volatile cash market price swings, cash market manipulation and cyber vulnerability to hacking, place consumers at a disadvantage in the cryptocurrency market (CFTC, 2017).

The larger the Bitcoin market becomes, the more impact it could have on the global, financial system. David Yermack, chairman of the finance department at New York University's Stern School of Business, says the blockchain is so secure that it reduces the cost of verifying transactions, so banks are looking into adopting blockchain technology in the future (Sabin, 2018). In 50 years, Yermack affirms, cryptocurrencies could be used as national currencies (Sabin, 2018). Despite the risk, Bitcoin is viewed as an opportunity to make money. Since 2012, Bitcoin has been the fastest growing area for funding for venture capitalists (Miller, 2015).

Value. Bitcoin had a rough beginning. In its early phases, the bankruptcy filing of Mt. Gox, in 2013, dropped Bitcoin prices from $1,000 per Bitcoin to $180 per Bitcoin (Alvarez-Ramirez et al. , 2018). The bankruptcy eroded customer trust in cryptocurrencies, amongst evidence of hacking, as well as suspicious trading activities (Alvarez-Ramirez et al. , 2018). Bitfinex stepped into becoming the most dominant Bitcoin exchange trading and currency-storage platform by focusing on improving information security and reducing security risks from criminal hackers (Alvarez-Ramirez et al. , 2018). The consequent resurgence in Bitcoin interest led to the rise of diverse exchange platforms and the rise of other, alternative virtual currencies. Bitcoin, in particular, spread in popularity because it is viewed as the *reserve currency* of the cryptocurrency market, similar to the U.S. dollar (Thompson, 2017).

Investors in initial coin offerings (ICOs), or token sales, which raise funds for new cryptocurrencies, first convert cash into Bitcoin (Thompson, 2017). With Bitcoin, investors buy digital tokens in the new cryptocurrency (Thompson, 2017). In 2017, over $1.7 billion was raised through ICOs (Malanov, 2017). The Securities and Exchange Commission (SEC) has warned ICOs can be used to improperly entice investors with promises of high returns, despite the lack of guarantee (CFTC, 2017). Also, in 2017, criminal hackers impersonated ICOs with fake websites, persuading millions of dollars of funds to be sent (Roberts, 2017). China declared ICOs illegal in September of 2017, ordering a stop to fundraising using digital coins (Dunkley, 2017).

Despite the enthusiasm for Bitcoin, one of the problems with Bitcoin is the instability of its market value (Iwamura et al., 2014b). The lack of relying on a central bank's policies means the Bitcoin market is sensitive to macroeconomic factors such as economic, social, and political news, as well as rumors (Alvarez-Ramirez et al. , 2018). Since it is a network, the number of

Bitcoin users is a key determinant of value to the users (Corbet et al., 2017). People's beliefs and economics determine when an item has value (Miller, 2015). An object's worth is determined by the value held by society, as well as rules that govern commerce (Miller, 2015). The perceived value of Bitcoin is important in the market, as the value can affect price bubbles.

A price bubble is when the price of an asset diverges from the asset's value (Corbet et al., 2017). Studies have shown that Bitcoin is vulnerable to significant bubbles, particularly prior to major events affecting the Bitcoin market (Corbet et al., 2017). More recent studies have also shown evidence of spillover from rival cryptocurrencies, such as Ripple, to Bitcoin, aggravating price falls in the Bitcoin market (Corbet et al., 2017).

Contradictory studies have found evidence suggesting Bitcoin returns are driven internally, by buyers and sellers, not by external, economic factors (Corbet et al., 2017). The lack of stable pricing makes it difficult to assess the real value of Bitcoin and increases the risk of loss for investors, which has kept potential users at bay (Bulgakov, 2014). This factor alone makes Bitcoin, and other cryptocurrencies, unlikely to fully replace currencies provided by central banks (Iwamura et al., 2014b).

The Bitcoin system controls the rate of Bitcoin creation, but the market value is determined by the supply of Bitcoins in circulation and users' rate of holding, or trading, Bitcoins (FBI, 2012). The limit of 21 million Bitcoins prevents inflation (FBI, 2012). While the Federal Reserve can increase the number of dollars in circulation, to accommodate for economic growth, the only channel for growth in Bitcoin is for the currency to appreciate (Barber et al., 2012). Due to the potential to appreciate, Bitcoins tend to be saved rather than spent (Barber et al., 2012). As saved Bitcoins disappear out of circulation, transaction volume decreases and block creation becomes less profitable since there are fewer fees to collect (Barber et al., 2012).

See Figure 3 for a graphic depiction of Bitcoin distribution over time, starting at its onset in 2008.

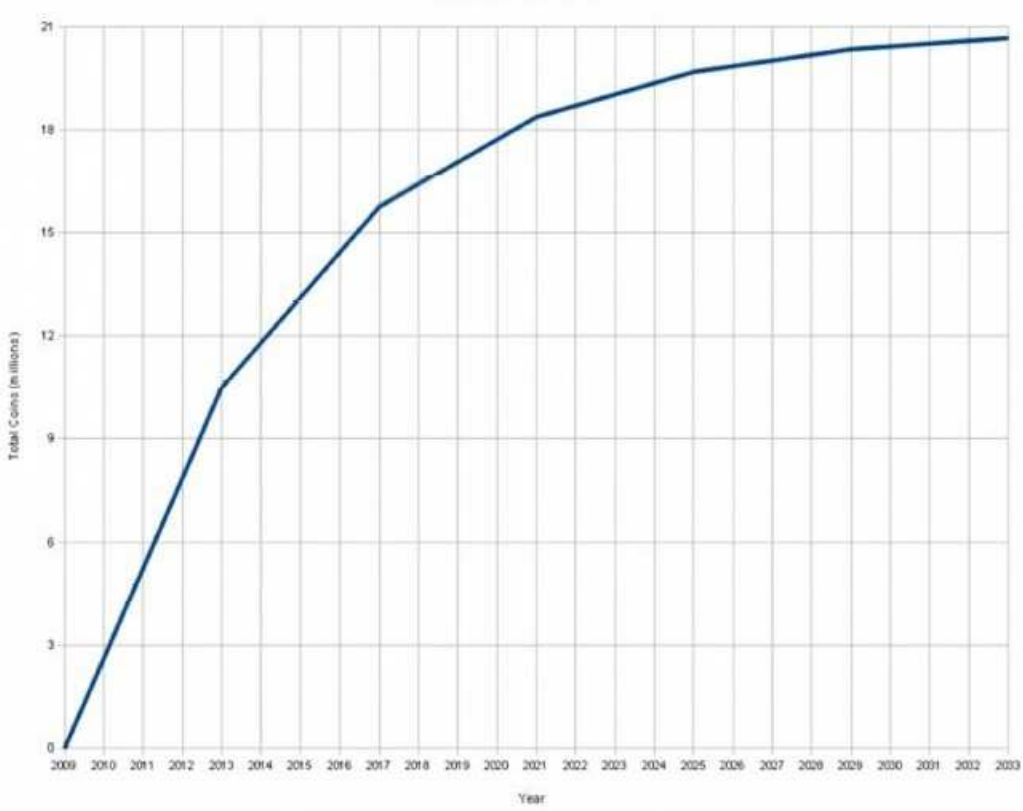


Figure 3. Total bitcoins over time. Adapted from "(U) Bitcoin virtual currency: Unique features present distinct challenges for deterring illicit activity," by FBI Directorate of Intelligence, 2012, *FBI Intelligence Assessment,* p. 14. Copyright 2012 by FBI.

Bitcoin circulation decreasing too much can result in a loss of interest in the system to a point where the Bitcoin system can become too weak to sustain itself (Barber et al., 2012). Some economists theorize the planned, finite supply of Bitcoin will hit a deflationary spiral, as Bitcoins are lost over time and the supply diminishes (Bonneau & Goldfeder, 2017). Other economists believe that if Bitcoin ever gained more than a peripheral acceptance, the limited, built-in supply would appreciate tremendously (Barber et al., 2012). The only outlet for growth would be for the currency to appreciate (Barber et al., 2012).

Volatility. The Bitcoin system manifests instability from two main sources (Iwamura et al., 2014b). Some economic studies have assessed market price instability to be a result of the lack of flexibility in the Bitcoin supply production (Iwamura et al., 2014b). The price volatility of Bitcoin may reflect a naïve understanding by the designer of Bitcoin, in interpreting the monetary value would stabilize, by a fixed supply of Bitcoin (Iwamura et al., 2014b). There is no other mechanism in place to stabilize prices (Iwamura et al., 2014b). The demand for Bitcoin, regardless of the motivation for holding it, increases as the price decreases, and vice-versa (Iwamura et al., 2014b). See Figure 4 for a depiction of the volatility in Bitcoin price over a six-month period, from September 23rd, 2017 to March 21st, 2018.

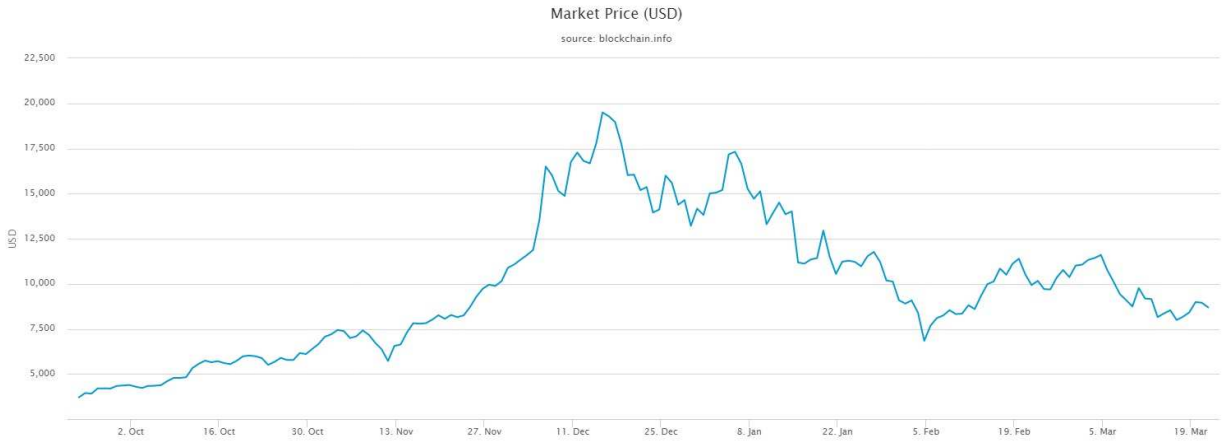


Figure 4. Market price of Bitcoin from 3,703 USD to 8,690 USD (9/23/17 to 3/21/18). Adapted from "Confirmed transactions per day," by Blockchain.info, 2018.

The second risk of instability in the Bitcoin market, Iwamura assesses, comes from the risk of price drops affecting the sustainability of mining for new blocks on the blockchain (Iwamura et al., 2014b). If Bitcoin prices fell below average operational costs, miners could stop mining for new Bitcoin, placing the entire Bitcoin system at risk of collapse (Iwamura et al., 2014b). As rewards for Bitcoin miners are phased out, computer scientists are apprehensive if

transaction fees will be sustainable enough for new block creation in the future (Bonneau & Goldfeder, 2017).

Some studies have indicated the dynamics of Bitcoin price is dependent on price directionality. When Bitcoin prices are decreasing, the returns are random, with a more efficient market (Alvarez-Ramirez et al. , 2018). When Bitcoin price is increasing, there are wild fluctuations, contributing to its unpredictable nature (Alvarez-Ramirez et al. , 2018). Bitcoin prices were sampled, at an hourly frequency, from May 8th to June 3rd, 2017 (Alvarez-Ramirez et al. , 2018). In one week, the price had an increase of 60 percent, from $1,700 per Bitcoin to $2,760 per Bitcoin (Alvarez-Ramirez et al. , 2018). Similar to how financial bubbles fluctuate, the price suddenly dropped to $2,043 per Bitcoin in 1.5 days (Alvarez-Ramirez et al. , 2018). This type of fluctuation indicates Bitcoin is vulnerable to high volatility.

The promised potential of large returns in this non-mature, emerging market attracts speculative investors, which amplifies market volatility even more (Alvarez-Ramirez et al. , 2018). However, contradictory studies have indicated speculative trading does not drive the presence of excess volatility (Blau, 2017). In 2013, when Bitcoin lost nearly 60 percent of its value, studies indicated speculative trading was not excessively high during that bubble period (Blau, 2017). The lack of speculation is puzzling and suggests that factors other than just speculation are at play.

Some authors have argued the Bitcoin market is converting to market efficiency, as more investors are attracted and capitalization is growing (Alvarez-Ramirez et al. , 2018). Others have disputed that market efficiency is not feasible under current market conditions, since the Bitcoin market is still susceptible to price rallies, or periods of sustained price increases (Alvarez-Ramirez et al. , 2018). Although Bitcoin still succumbs to large, volatile dips, there have been

signs the volatility is decreasing over time (Bariviera et al., 2017). The reason for that trend is unknown, since Bitcoin price is not connected to market fundamentals (Bariviera et al., 2017).

The variability of uncertainty in the Bitcoin market is an obstacle to a wider base of adoption (CPMI, 2015). The introduction of traditional, financial regulations in the cryptocurrency market would reduce bubbles, but the nature of the cryptocurrency market does not allow for such a possibility (Alvarez-Ramirez et al. , 2018). The more recent, explosive rise in Bitcoin prices has not been consistently accompanied by sustained signals of a bubble (Corbet et al., 2017). However, there is evidence to support the view that the Bitcoin market is currently in a bubble phase, since the period the price rose above $1,000 per Bitcoin (Corbet et al., 2017).

Cash market manipulation. Since the protection most investors would have on a stock market is not present, Bitcoin owners need to know how to buy, sell, and store Bitcoin properly, not to risk losing their investment (Hickey, 2017). About 40 percent of Bitcoin is owned by about 1,000 investors, which means those investors can send prices plunging if they sell large portions of their investment (Kharif, 2017). In comparison to securities markets, where everything has to be disclosed, there is a lack of transparency in the Bitcoin market (Kharif, 2017).

Since Bitcoin is a digital currency, and not a security, members can share information about anticipated Bitcoin sales, which is likened to *pump-and-dump* schemes (Kharif, 2017). As with other asset classes, large institutional, or individual, holders can collude to manipulate the price, although it is questionable Bitcoin holders would not rather wait on the long-term potential of the market (Kharif, 2017). Bittrex, one of the digital currency exchanges, warned its users their accounts would be put on hold if they organized *pump groups* to manipulate prices (Kharif, 2017).

The CFTC has received complaints from multiple victims of the traditional, financial pump-and-dump fraud schemes occurring in the cryptocurrency market (CFTC, 2018). On February 15th, 2018, the CFTC issued a customer protection advisory regarding cash market manipulation in the unregulated, virtual currency market (U.S. Commodity Futures Trading Commission, 2018). The CFTC warned customers that pump-and-dump schemes could occur in public chat rooms or via mobile messaging apps, particularly those that offer a wide variety of coin pairings (CFTC, 2018). This type of market manipulation typically occurs in unregulated cash markets, particularly thinly traded markets, and takes advantage of traders by creating phony demand, so customers sell quickly (CFTC, 2018).

Bitcoin as an investment. Surveys indicate the vast majority of bitcoin owners are buying and holding onto Bitcoin to exchange them for dollars. Bitcoin, and other cryptocurrencies, are not real investments such as a home, real estate, stocks, bonds, mutual funds, or other tangible assets that can experience genuine price appreciation (Singletary, 2018). To such investors, the short-term buying and selling of Bitcoin are seen as typical of the cryptocurrency market, gambling in the pursuit of quick riches.

Before Bitcoin has a chance to mature, investing in cryptocurrency has been likened to investing in a start-up. “"Ninety percent of your investments will be lost, and 10 percent could show returns," said Christian Catalini, who studies cryptocurrency at the Massachusetts Institute of Technology (MIT) (Nova, 2017a, para. 16). Financial advisors state Bitcoin is too risky to treat seriously for investment purposes (Nova, 2017a). Some consultants even liken Bitcoin to a Ponzi scheme, in that those who created the cryptocurrencies will have profited, at the expense of those who are holding the currency, when it eventually collapses (Singletary, 2018). The lack

of available information regarding certain Bitcoin exchanges raises more concerns about possible Ponzi schemes (Bariviera et al., 2017).

Bitcoin use triggers tax risks, as Bitcoin has been declared property by the Internal Revenue Service (IRS), like stocks, and taxes them accordingly (Williams, 2014). Unlike currency, consumers that use Bitcoin can be subject to the additional capital gains taxes. This tax stance provides incentives to hoard Bitcoin and not use it for transactions, reducing liquidity in the market (Williams, 2014). As Bitcoin rises in value, so will the incentive rise for theft (Barber et al., 2012).

A Matter of Privacy

The more popular Bitcoin becomes, the more value it generates to existing, as well as new, potential users (O'Malley & Presthus, 2017). For Bitcoin to gain in popularity, users are waiting for non-users to join in on the technology (O'Malley & Presthus, 2017). A survey on non-users of Bitcoin stated the elements which Bitcoin lacks are: "stability, security, must see value, usefulness, and ease of use" (O'Malley & Presthus, 2017, p. 94).

In addition, concerns over privacy have been cited (O'Malley & Presthus, 2017).

It is questionable if Bitcoin provides more privacy than traditional banking, due to the possibility of linking user pseudonyms together, by studying patterns in the blockchain. Bitcoin offers poor anonymity, which fundamentally is pseudo-anonymity (Jordan, et al., 2013). Security issues with Bitcoin are closely tied to the transaction privacy and user pseudo-anonymity (Conti et al., 2017).

Bitcoins are not really stored in the wallet, but *exist* in the blockchain, which is the public transaction ledger (Miller, 2015). The Bitcoin transaction log shows each transaction, from payer to payee, along with the public keys, which serve as pseudonyms (Boehme et al., 2015).

Trading Bitcoins entails transferring Bitcoins in the ledger to another address in the ledger (Miller, 2015). If a user wants to transfer Bitcoins, the transaction is broadcast into the P2P network, proving ownership of the Bitcoins (Jordan, et al., 2013). The transaction reaches a miner, who works on finding the right data to find a new block, who then broadcasts it to their peers (Jordan, et al., 2013). When another block is formed after the current block, the previous block is considered officially part of the blockchain (Jordan, et al., 2013).

Bitcoins are associated with the address, not the wallet (Miller, 2015). Users can have more than one address, which is recommended, to enhance security and pseudo-anonymity (Miller, 2015). Each address is linked to a distinct pair of private and public keys, which do not protect the privacy of the user (Miller, 2015).

Security in the Bitcoin system relies on the underlying cryptography. The blockchain system, in Bitcoin, allows entities to transact securely, and directly with one another, through asymmetric cryptography (Prpic, 2017). Asymmetric cryptography systems work by issuing a pair of keys to members, a public and private key (Prpic, 2017). For privacy purposes, the sender encrypts the message with the public key of the recipient and sends the message directly to the recipient, who decrypts the message with their private key (Prpic, 2017). For authentication purposes, the sender encrypts the message with their private key and makes the encrypted message public, through the use of a digital signature (Prpic, 2017). The individual who controls the private key controls the Bitcoins, from the address linked with that private key (Miller, 2015). Keeping the private key secret, and secure, is crucial to preventing theft (Miller, 2015). Satoshi's original vision was that privacy would be sustained by keeping public keys pseudo-anonymous (Nakamoto, 2008).

Through public key cryptography, the blockchain creates a publicly shared, collected, and verified record of transactions (Prpic, 2017). Since the blockchain, or transaction ledger, is public, the pseudo-anonymity only comes from the fact that users are using pseudonyms, in the place of real names. However, the use of pseudonyms does not provide complete privacy protection. Analysis of the blockchain can reveal who is using Bitcoin and for what purposes (Conti et al., 2017).

Cybersecurity issues in Bitcoin are closely linked to transaction privacy and user pseudo-anonymity (Conti et al., 2017). In Bitcoin's current state, users are not completely anonymous and linking seems to be unavoidable with multi-input transactions (Nakamoto, 2008). In Bitcoin, the public blockchain reveals all transaction data, to any user connected to the network. Privacy is maintained up to a certain point, by keeping public keys pseudo-anonymous (Conti et al., 2017). The transaction is visible, but identifiable information linking the transaction to a particular person, is not (Conti et al., 2017). To enhance user privacy and prevent linkage to a specific user, it is recommended to use a new key pair for each transaction, as Satoshi envisioned (Conti et al., 2017; Nakamoto, 2008; Scheuermann & Tschorsch, 2016). Using multiple keys helps to achieve better pseudo-anonymity, without being a true remedy.

Linking is still possible with multi-input transactions, which reveal inputs that were owned by the same owner (Conti et al., 2017). If the owner of the key is revealed, then there is a possibility the link could reveal other transactions belonging to the same user (Conti et al., 2017). Bitcoin's pseudo-anonymity enables the possibility of linking multiple transactions to an individual user, by tracking the movement of money through the blockchain (Conti et al., 2017).

De-anonymization. Complete anonymity in Bitcoin is complicated. Bitcoin users can generate multiple Bitcoin addresses and Bitcoin stores only the mapping information of the user,

to the Bitcoin addresses on their device (Conti et al., 2017). De-anonymizing a user requires linking the user and the associated addresses (Conti et al., 2017). Various companies are specializing in Bitcoin blockchain analysis, to help identify Bitcoin users of illicit activities (Conti et al., 2017).

If a user purchases an item by paying with cryptocurrency, an adversary can identify the transaction by using third-party trackers (Conti et al., 2017). These transactions can be linked to the user cookies, then be linked with the real identity of the user, and their recent, or past, purchase history (Conti et al., 2017). If the tracker can link two purchases to the same user on the blockchain, using blockchain analysis, it can further identify the user's entire cluster of Bitcoin addresses and transactions (Conti et al., 2017).

Transactions and addresses of users can often be linked together by analyzing the transaction graph in the blockchain (Grossmann, Henze, Klaus, Matzutt, & Ziegeldorf, 2018). For the protection of users' identities, Internet protocol (IP) information is never stored in the Bitcoin system (Koshy, Koshy, & McDaniel, 2014). However, Bitcoin addresses have even been linked to IP addresses, which completely deanonymizes users (Conti et al., 2017). While a transaction is broadcast on the network, the node leaks the IP address (Conti et al., 2017). Linking Bitcoin users' public keys to IP addresses has been shown to be effective at about 30 percent (Conti et al., 2017).

Internet anonymity services, such as Tor, provide a solution to de-anonymization, by concealing the originating IP address (Scheuermann & Tschorsch, 2016). If users do not anonymize their IP address, the individual's physical location can be determined (FBI, 2012). The ability to identify users, through their transactions on the blockchain, has made users regard Bitcoin's promise of financial privacy as broken. To re-establish financial privacy, users could

generate unlinkable addresses, but transferring funds will link the address back to the user (Grossmann et al., 2018).

Mixing up privacy. Although anonymity increases by using a different public key for each transaction, the only means to send funds from a deanonymized address to a new address in an unlinkable manner, is to use a secure and anonymous mixer. Mixers are anonymous services that try to obscure the trail of transactions, by breaking down client funds into smaller parts and mixing them, randomly, with parts from other clients, to end up with new coins (Conti et al., 2017). There are a variety of mixers, but all share the common goal of a truly anonymous transaction in Bitcoin (Miller, 2015). The user sends the Bitcoin funds to the mixing service, which, for a fee, will mix funds with the funds of other random users and send the mixed currency to the recipient (Miller, 2015).

To preserve privacy, mixers pool sets of transactions into unpredictable combinations when mixing Bitcoins (Boehme et al., 2015). Some mixers split transactions into smaller pieces, from multiple addresses (Miller, 2015). Mixers make it very difficult to separate the original sender from the distraction, but the degree of anonymity largely depends upon the number of users (Conti et al., 2017; Miller, 2015). The mixer needs to ensure timing does not reveal clues about money flow (Boehme et al., 2015). Even mixing services can be vulnerable to distributed denial of service (DDoS) attacks (Conti et al., 2017). During DDoS attacks, multiple attackers launch a denial of service, at the same time, to cause disruption to a network (Conti et al., 2017).

The first generation of mixers has had problems. Users had to blindly trust the mixer operators not to steal their funds, as there have been allegations of theft (Grossmann et al., 2018). In addition, if mixing services kept transcripts of how funds were mixed, the services were

susceptible to being breached, or could be forced to be revealed to third parties (Grossmann et al., 2018).

New mixers have promised stronger security and anonymity. Mixing transactions have been issued into one large transaction, to prevent peers from aborting after they received funds, leaving their peers unpaid (Grossmann et al., 2018). However, group transactions were still easily distinguishable in the blockchain, which means the user's anonymity is set to the number of users participating in the mix (Grossmann et al., 2018). More secure, multi-party mixers have been proposed, but each has disadvantages (Grossmann et al., 2018). Proposals have included methods to make users anonymous, even amongst mixing peers, and methods to make mixed and non-mixed transactions indistinguishable (Grossmann et al., 2018).

Bitcoin Under Cyberattack

"One of bitcoin's strengths - the most important in my opinion even - is the low degree of trust you need in others" - Pieter Wuille (Lopp, 2016, para. 4).

Venturing into Bitcoin is considered a high-risk transaction, due to volatility, but that unease has also spread to security. Forty-four percent of Bitcoin holders "routinely worry about the technological security of their investments" (Nova, 2017b, para. 5). Traditional banking systems have currencies that are protected by regulation, deposit insurance, and international treaties (Yermack, 2013). Although cryptocurrency exchanges may seem to function as virtual banks, they do not have the added protection. There is no depositor's insurance to absorb the loss, although exchanges function much like virtual banks. By eliminating financial institutions as middlemen, legal protections in the cryptocurrency market are also eliminated. Without such an infrastructure, Bitcoin is vulnerable to fraud, theft, and being undermined by malicious hackers (Yermack, 2013).

The lawless nature of cryptocurrency markets seems to lure cryptocurrencies into facing threats of attack. Criminals intending to steal Bitcoins can target, and exploit, third-party Bitcoin services and individual Bitcoin wallets, since there is no central Bitcoin server (FBI, 2012). Through malware and other hacking practices, personal computers and accounts can be compromised (FBI, 2012). Other techniques involve using botnets to compromise victim computers, to mine bitcoins (FBI, 2012). Particularly appealing to cybercriminals is the lack of recourse if the virtual currency is stolen. These factors have combined to make the Bitcoin system an ideal target for cybercriminals.

Bitcoin has had a negative public perception regarding security, although Bitcoin transactions sent from one party to another, through the system itself, has not been compromised (Kshetri, 2017). Hacking attacks have occurred only in other systems that hold, and store, Bitcoin private keys (Kshetri, 2017). Proponents of blockchain technology, on which Bitcoin is based, argue the technology is secure by design (Kshetri, 2017). Transaction records are on multiple, interlocked computers that hold identical information. Hacking of the entire network would require over 50 percent of systems in the network to be hacked (Kshetri, 2017).

Internet commerce has relied on financial institutions to function as trusted, third parties for electronic payments (Nakamoto, 2008). Bitcoin was Satoshi's answer to the trust-based model (Nakamoto, 2008). Buying, selling, or trading Bitcoins must be done with third-party businesses outside of Bitcoin's P2P system (FBI, 2012). Bitcoin requires individuals to use third-party services, such as currency exchanges, to trade Bitcoins for fiat currency (FBI, 2012). Digital currency exchanges allow users to buy, and sell, Bitcoins for fiat money, or altcoins, and can hold a significant amount of coins in storage (Scheuermann & Tschorsch, 2016). The exchanges also serve as wallet providers in that users, who wish to trade, need to provide a

deposit (Scheuermann & Tschorsch, 2016). The wallet-service middlemen can become points of failure for the system (Scheuermann & Tschorsch, 2016).

Magnet for fraud. The only means by which Bitcoin can be stolen is for a thief to trick the user, trick a third party the user relies on into getting access to the Bitcoin, or for the third party to be compromised (Roberts, 2017). Bitcoin's reliance on third-party intermediaries can become a point of failure, as that reliance makes the system vulnerable. Trends have shown that, as the value of Bitcoin rises, so does the number of viruses designed to steal Bitcoins (Cobb, 2018).

Big currency exchanges that hold customer deposits are a big target for malicious hackers. From Bitcoin's creation, in 2009, to March 2015, 33 percent of all operational Bitcoin exchanges were hacked (Reuters, 2016). Not necessarily triggered by cyber-attacks, the rate of closure for Bitcoin exchanges was near 48 percent at that time (Reuters, 2016). Exchanges have lost Bitcoins and declared bankruptcy due to external or internal theft, or technical blunders (Conti et al., 2017). In comparison, only one percent of U.S. banks experienced a data breach during that same period (Reuters, 2016). The latest survey of 46 securities exchanges revealed over half had experienced some form of cyber-attack (Reuters, 2016).

In 2016, almost 120,000 Bitcoins, worth around 78 million USD, were stolen from Hong Kong-based Bitfinex, one of the most popular cryptocurrency exchanges (Hickey, 2017). The theft resulted in a 20 percent drop in the value of Bitcoin with Bitfinex investors receiving back only partial reimbursement (Hickey, 2017). Information technology security is an issue for any industry that uses technology. Bitcoin, as well as all virtual currencies, rely exclusively on the digital domain.

Bitcoin itself is considered secure, but the security problem lies in the businesses involved in cryptocurrencies, including the digital wallets where Bitcoin is stored (Hickey, 2017). A vital distinction among digital wallet services is whether the service knows the user's private key (Boehme et al., 2015). If not, the user maintains responsibility for the identity of the key. Theft, or loss of private keys, which is essentially a signature forgery, equates to a loss of money (Barber et al., 2012). If the service stores the private key, the risk of the digital wallet service being compromised increases (Boehme et al., 2015).

Rising values have made cryptocurrency exchanges particularly appealing targets for criminal hackers, especially in Asia. After being hacked into on December 19th, 2017, South Korean Bitcoin cryptocurrency exchange YouBit filed for bankruptcy because the hacking caused the exchange to lose 17 percent of its assets (Dunkley, 2017). The attack occurred eight months after a previous cyber breach on YouBit, in April of 2017 (Dunkley, 2017). In July of 2017, South Korean exchange Bithumb was hacked, resulting in the theft of personally identifiable information of over 31,000 customers (Trend Micro, 2017). In August of 2016, Hong Kong-based Bitfinex was hacked for 70 million USD (Dunkley, 2017). On December 7th, 2017, Slovenia-based, cryptocurrency-mining marketplace NiceHash was breached, and payment system compromised, with losses near 64 million USD (Trend Micro, 2017).

Threat of double spending. Bitcoin's digital currency has prominent market capitalization value, so the motives for exploiting weaknesses in the system are substantial (Scheuermann & Tschorsch, 2016). The main attack vector for cybercriminals entails key theft, although the threat of double spending is always a consideration (Scheuermann & Tschorsch, 2016). Double spending is, and always will be, possible with Bitcoin (Scheuermann & Tschorsch, 2016).

Double spending is when a person simultaneously issues two separate transactions, to two different receivers, for the same coin, at the same time (Scheuermann & Tschorsch, 2016). Bitcoin attempts to address this by letting the entire network verify the legitimacy of transactions, so other participants notice the double spending (Scheuermann & Tschorsch, 2016). If the Bitcoin user uses the rule of thumb, waiting for six confirmations before accepting a transaction, it minimizes user risk of double spending (Scheuermann & Tschorsch, 2016). Since every user of Bitcoin technically is a bank, it is on their onus to prevent circumstances such as double spending. Beyond double spending, attack vectors include key recovery and a variant on double spending, transaction malleability (Scheuermann & Tschorsch, 2016).

Digital wallet types. Aside from double spending, Bitcoin attack vectors include wallet attacks: client-side security; network attacks, such as DDoS; and mining attacks, such as the 51 percent attack (Conti et al., 2017). Unlike traditional online payments, which require a login and password, Bitcoin relies on public key cryptography. To use Bitcoin, the user needs a digital wallet, which holds the set of public and private key pairs. It is necessary to secure the keys properly, as compromising, or losing, the keys results in instant, and unalterable, monetary loss. If Bitcoin users do not backup their wallet to a hard drive or phone's flash memory, and a hardware failure occurs, the Bitcoins would be lost if the private keys are gone (Miller, 2015). Thefts of digital wallets have mainly occurred due to hacked computer systems, faulty software, or poor configuration of systems (Scheuermann & Tschorsch, 2016).

Digital wallet providers must provide a good blend of usability and security (Conti et al., 2017). Digital wallet types can range from software, hardware, paper, brain, to online wallets (Scheuermann & Tschorsch, 2016). One of the most common ways to use Bitcoin is with a software wallet (Scheuermann & Tschorsch, 2016).

A software wallet requires a locally running Bitcoin instance, which can be found online (Scheuermann & Tschorsch, 2016). Online wallets, such as Coinbase, are popular (Scheuermann & Tschorsch, 2016). The online wallet either manages the Bitcoins centrally, or in a hybrid manner, the wallet is stored and encrypted, while most operations are on the client side, in the browser (Scheuermann & Tschorsch, 2016). Coinbase is particularly popular because of desirable features such as a web interface; accessibile via browser and Internet; mobile app, access not requiring client software, an independent setup, and moderate security and privacy (Conti et al., 2017). Other digital wallet types are more secured than online wallets.

All software and online wallets are prone to security vulnerabilities because an attacker gaining access to a Bitcoin user's computer gains access to the user's wallet (Scheuermann & Tschorsch, 2016). Online wallets are more vulnerable to theft than hardware wallets. However, the trade-off is the lack of usability with hardware wallets.

A hardware wallet uses a separate device that usually operates offline (Scheuermann & Tschorsch, 2016). Since the device is not connected to the network, it is much harder for an attacker to gain access (Scheuermann & Tschorsch, 2016). Even more secure methods to store user keys are the paper and brain wallets. A paper wallet stores the keys holding coins, offline, as a physical document (Scheuermann & Tschorsch, 2016). In a way, this is similar to cash. A brain wallet relies on the user to store the keys in their brain, by memorizing a passphrase, or a sequence of words to control access (Scheuermann & Tschorsch, 2016).

Other users may prefer to keep their Bitcoins stored on an online currency exchange. However, this makes the user vulnerable to the security of the exchange system, which can never be fully avoided or mitigated, although currency exchanges and mining pools are much more likely to have DDoS protection (Conti et al., 2017; Moore, Thornton, & Vasek, 2014). In 2014,

around 20 percent of online Bitcoin services had anti-DDoS protection, with such protection more prevalent in certain categories (2014). About one-third of exchanges and pools had anti-DDoS protection, with shops that accepted Bitcoin less likely to have protection (2014). Those services that have been previously attacked are more than three times as likely to buy anti-DDoS services than those that have not been (2014). Financial firms and eWallets frequently utilized anti-DDoS protection (2014). Additional protection for wallet-service middlemen, such as through a cloud provider, is recommended against DDoS attacks (Scheuermann & Tschorsch, 2016).

Network attacks. The most common networking attacks are inexpensive DDoS attacks (Conti et al., 2017). Within a two-year period, 142 DDoS attacks had been reported on 40 Bitcoin services, and seven percent of all known operators were the victims (Conti et al., 2017). Distributed denial of service attacks have targeted Bitcoin currency exchanges, mining pools, gambling operators, digital wallets, and financial services of the Bitcoin market (Conti et al., 2017).

Due to the potential for a larger revenue, most DDoS attacks target currency exchange services and large mining pools (Conti et al., 2017). Larger organizations are targeted, due to bulk ransom motives and the pseudo-anonymity of Bitcoin (Conti et al., 2017; Dascalescu, 2017; Miller, 2015). Companies such as CoinWallet and BitQuick have been forced to shut down only months after launch, due to continuous DDoS attacks (Conti et al., 2017).

Malleability attacks facilitate DDoS attacks in the Bitcoin system, in that the attacker clogs the transaction queue of all pending transactions (Conti et al., 2017). The attacker instills bogus transactions, with a high priority, by depicting itself to be the highest incentive payer to the miners (Conti et al., 2017). When the miners try to verify the transactions, it is detected they

are false, but a considerable amount of time was already wasted on the effort (Conti et al., 2017). This type of attack wastes the time, and resources, of the miners and the network (Conti et al., 2017).

A specific type of malleability attack is transaction malleability, which refers to a bug in Bitcoin that enables the ability to change the transaction identifier (TXID) without invalidating the transaction (Scheuermann & Tschorsch, 2016). Each transaction can be uniquely identified by a TXID, which is a hash of the transaction data (Scheuermann & Tschorsch, 2016). Though other cryptocurrencies can have different hash functions, Bitcoin exclusively utilizes the Secure Hash Algorithm 256 (SHA 256) (Ivanecky, 2018). Changing the TXID allows an attacker to make an individual believe a transaction has failed, although it is later confirmed (Scheuermann & Tschorsch, 2016).

Currency exchanges are particularly vulnerable to such an attack. If an attacker withdraws coins from an exchange and rebroadcasts the altered version of this transaction with a different TXID, one of the two transactions will appear in the blockchain (Scheuermann & Tschorsch, 2016). Due to delays, there is a possibility of the modified transaction winning over the original withdrawal (Scheuermann & Tschorsch, 2016). If the currency exchange relies only on TXIDs (a prerequisite for this to work), it will not find the withdrawal transaction in the blockchain, will believe it failed, and the attacker can repeatedly withdraw (Scheuermann & Tschorsch, 2016). The transaction malleability flaw enabled attackers to steal about 7 percent of all Bitcoins through the Mt. Gox exchange (Merkle, 2017).

Mining attacks. To prevent other spending attacks, the Bitcoin structure needs to remain a system whereby no one entity controls over half of the computational power. To increase mining rewards, it is prevalent for individual miners to conglomerate into mining pools.

Preventing mining pools from owning more than 50 percent of Bitcoin, at any one time, prevents a 51 percent attack, a worst-case scenario (Scheuermann & Tschorsch, 2016). In the 51 percent attack, the prevalent mining pool could undermine fairness by collecting all the mining rewards, by ignoring new blocks found by others, and building their own chain (Bonneau, Clark, Felten, Kross, Miller, & Narayanan, 2015). Satoshi envisioned such majority-miner attacks would naturally be prevented because playing by the rules would lead to higher profits, for all, over time (Boehme et al., 2015).

Mining pools, such as GHash.io, have neared the 51 percent threshold, but have publicly promised to limit their size, in the future, so as not to diminish confidence in the Bitcoin system (Boehme et al., 2015; Scheuermann & Tschorsch, 2016). However, not all miners are honest and rogue miners have attacked the mining process in smaller ways to gain an unfairly high share of Bitcoins during DDoS attacks (Scheuermann & Tschorsch, 2016). Mining pools are the second-most popular target of DDoS attacks in Bitcoin (Scheuermann & Tschorsch, 2016). Malicious miners, with access to a botnet, can perform DDoS on competing miners outside of their network, overwhelming them with fake transaction requests, so they withdraw from mining (Conti et al., 2017). Big mining pools, with historical hash rates of over five percent, are more likely to be targeted for a DDoS attack than smaller pools (2014).

New threats, such as crypto mining malware attacks, have emerged (Trend Micro, 2017). Malicious miners have employed worms, malicious Android apps, and zombified home routers and used social engineering for tech support scams (Trend Micro, 2017). Recently, a trojan was updated to steal cryptocurrency wallet credentials (Trend Micro, 2017).

Plain old theft. Attacking the signature scheme enables Bitcoin-stealing. A standard transaction requires the user to provide a public key and signature, using the private key, as proof

of ownership (Conti et al., 2017). Generating a signature requires the user to choose a random value for each signature (Conti et al., 2017). To maintain security, this value should be kept secret and be different for every transaction (Conti et al., 2017). Repeating per-signature values increases the risk of a user's private key being determined (Conti et al., 2017).

Using a dictionary attack, attackers have guessed private keys and compromised accounts (Merkle, 2017). Once the private key is determined, cybercriminals employ bots to check whether cryptocurrency has been transferred, to steal the Bitcoin (Merkle, 2017). The use of highly random, and diverse, per-signature values is essential to maintaining security (Conti et al., 2017). Studies have analyzed 158 public keys which reused the signature values for more than one transaction, and enabled the ability to determine the user's private key (Conti et al., 2017).

Payment information can be spoofed (Malanov, 2017). When transferring digital money to another wallet address, malware could replace the receiver address, in the clipboard, with a different address (Malanov, 2017). Malicious hackers take advantage of digital currency's long jumble of characters (Malanov, 2017). Bitcoin has built-in address validation; however, the wallet address still needs to be verified (Malanov, 2017). Vigilance and double-checking the address, after copying it, can help prevent this problem.

Users have also been tricked into going to a phishing website, by receiving a misleading email that directs them to a fake duplicate of their online wallet provider (Malanov, 2017). Untrustworthy crypto investment ventures have also vanished, claiming to have been hacked, but in reality, vanishing with their clients' Bitcoin (Roberts, 2017). Unlike traditional banking, there is no ability to cancel or protest a transfer. "What happens in blockchain, stays in blockchain" (Malanov, 2017, para. 5).

Social engineering to access. Common to cryptocurrencies is loss or theft of the digital wallet. There is the risk of online wallet websites, or the user's computer or mobile phone, being hacked. Most users store their cryptocurrency wallets on their computer, which can be stolen, or lost if the hard disk crashes (Malanov, 2017). By January of 2016, 2,658 identity theft incidents had been filed with the Federal Trade Commission regarding Bitcoin scams which hijacked phone numbers and hacked into Bitcoin accounts (Shin, 2016). Such incidents have involved all four of the major phone carriers and involved financial loss, threats, ransom, and even physical danger (Shin, 2016). Cryptocurrency players are particularly targeted because the transactions cannot be undone and can involve large sums of money.

Theft of Bitcoin can occur if malicious hackers obtain the password to a user account at an online storage service (Roberts, 2017). By breaking into email accounts and asking the online Bitcoin storage, such as Coinbase, to reset the password, the thief easily breaks into the user's Bitcoin (Roberts, 2017). Criminal hackers use social engineering, which is employed in 66 percent of all attacks by malicious hackers, to hijack a user's telephone through a customer service representative (Shin, 2016).

The malicious hackers use a security loophole, which verifies security, via text, to a user's phone number, which the malicious hacker has already hijacked, to gain cryptocurrency keys, as well as keys to other personal accounts (Shin, 2016). Criminal hackers take advantage of the common, two-factor authentication, via text, to capture control (Shin, 2016). Although proven not to be entirely secure, cryptocurrency exchanges, such as Coinbase, still rely on two-factor authentication due to clientele in less developed countries (Shin, 2016). In addition to being susceptible to theft, system failure or human error can cause accidental loss of Bitcoins, turning Bitcoins into zombies (Barber et al., 2012).

Cybersecurity Measures in the Bitcoin World

"One doesn't invest in Bitcoin, one gambles on Bitcoin" - Dave Birch, electronic payments expert (Hickey, 2017, para. 13).

To trust Bitcoin, people need to feel the system has the properties of money, as well as a sufficient degree of security (Bulgakov, 2014). An important demand-side factor for digital currencies is the risk of loss to users (CPMI, 2015). Cybersecurity risks range from the user losing it themselves, to being attacked. Security breaches undermine users' confidence in digital currencies, especially as it involves the intermediaries who hold and store critical information (CPMI, 2015). Bitcoin users need to be able to trust intermediaries are mitigating end user risks of loss due to hacking, operation failures, or fraud (CPMI, 2015). This element of trust, in this emerging field, is vital to gaining new users, as well as maintaining current users.

In 2018, it is anticipated there will be escalating competition among providers of wallet services to earn users' trust (Rosenberg, 2017). Also, in the near future, it is anticipated cyber attacks on cryptocurrencies will continue. Cryptocurrency exchanges are under pressure to improve their security, as retail clients will expect the same level of security they are provided from traditional banks (Dunkley, 2017). Bitcoin is constantly changing and continuously under development, to face such security challenges (Scheuermann & Tschorsch, 2016).

Similar to online banking, users need to be diligent about their Bitcoin account credentials (Hickey, 2017). However, new users to cryptocurrencies are not used to the notion of being their own bank. Keeping Bitcoins secure is complicated and time-consuming. Cybersecurity is important for general information, but crucial to protecting investments in cryptocurrency. Cybersecurity hygiene needs to be scrutinized and can help in reducing

exposure to somewhat simple cryptocurrency scams that take advantage of reused passwords or lack of a second authentication, to gain control of Bitcoin accounts (Newman, 2017).

Bitcoin wallets stored on a computer are exposed, as Bitcoin wallet applications save their data in predictable locations, making them particularly vulnerable to trojan attacks (Gilson, 2013). For example, the CryptoShuffler trojan lurked on victim computers, passively monitoring the clipboard for a Bitcoin wallet address (Newman, 2017). When a suspected address appeared, the trojan swapped the wallet ID the victim copied for its malicious wallet address in the payment fields (Newman, 2017). If not detected, the transaction went directly to the thieves (Newman, 2017). If the user's malware scanner did not detect the intrusion, the user needed to be vigilant of all transactions and take steps to safeguard cryptocurrency assets (Newman, 2017). Prior to investing in Bitcoin, potential investors need to assess their financial portfolio wisely.

Invest and gamble in moderation. Financial experts in cryptocurrencies advise Bitcoin investors only to invest as much as users can afford to lose (Hickey, 2017). The traditional, sensible view with investments is that the more volatile the investment, typically the smaller proportion of personal wealth should be stored in it (Hickey, 2017). The volatility, and uncertainty, of Bitcoin prices have not led it to be considered a more stable investment, yet. Regardless, Bitcoin investors have taken out equity lines, and mortgages, to buy Bitcoin (Hickey, 2017). Investing entire life savings into Bitcoin, as some users have done, is not recommended in this industry, as Bitcoin still carries too much risk. Consumers need to be aware of the financial risk involved and that there is no guaranteed investment with Bitcoin. Rather, investments need to be diversified.

Make informed decisions. Consumers need to remember much of the virtual currency cash market operates through Internet-based trading platforms that are unregulated. Consumers

need to be careful of the Bitcoin companies with which they do business (Roberts, 2017). Investors should research the legitimacy of virtual currency platforms, as well as digital wallets, before providing financial or sensitive, personal information, so they are not victims to exit scams (Roberts, 2017). Virtual currencies are technologically-based and the cryptocurrency market can be confusing to consumers. Consumers need to educate themselves before investing and should not invest in products or strategies which they do not understand. Users should not do business with companies that do not have a good track record and proper cybersecurity measures in place.

To protect against fraud, or Ponzi schemes, in the unregulated Bitcoin market, customers should avoid purchasing virtual currency based on tips from social media or during times of sudden price spikes (CFTC, 2018). Customers should only purchase virtual currencies from online sources that have been thoroughly researched, to separate hype from facts (CFTC, 2018). Customers need to verify investments in options or futures on virtual currencies are registered with the CFTC, to avoid investment fraud (CFTC, 2017). During ICOs, malicious hackers have stolen funds by impersonating companies with fake websites, using phishing attacks (Newman, 2017; Roberts, 2017).

Use cybersecurity vigilance. Users need always to verify an Internet wallet's address and should not follow links to an Internet bank or web wallet (Malanov, 2017). Before sending, users should always double-check the recipient's address, the amount being sent, and any fees (Malanov, 2017). Scammers have found a way to make website addresses look like authentic Uniform Resource Locators (URLs) of popular cryptocurrency exchanges, such as Binance and Bittrex (Villas-Boas, 2018).

Users need to remain vigilant in looking for a green *https* tag before the website's URL, to identify if it is legitimate (Villas-Boas, 2018). The green *Secure* and *https* indicates the company obtained proper Secure Sockets Layer (SSL) certificates, which means the firm is trusted (Villas-Boas, 2018). However, small changes in the web address, hardly identifiable by looking, may mean the https address is still a fake (Villas-Boas, 2018). Double-checking URLs and manually typing in URL addresses are the best ways to avoid scam sites (Villas-Boas, 2018). In addition, Chrome has a web browser extension, Cryptonight, which helps prevent phishing scams to cryptocurrency sites (Villas-Boas, 2018). Staying with popular Bitcoin clients also helps prevent user address errors (Malanov, 2017). Less well-known alternative digital currencies are more susceptible to theft by malicious hackers, than Bitcoin.

Keep digital wallets online and offline. Users need always to maintain control of their Bitcoin private keys. Storing large amounts of Bitcoin in cryptocurrency exchanges, or digital wallet apps on smartphones or computers, is not recommended (Newman, 2017). If Bitcoins are not in a Bitcoin address directly under user control and, for example, are being held in a currency exchange or online wallet, the user is susceptible to any loss incurred by the owner of that site (Bitcoinsecurity101, 2018). Access to the Internet provides criminal hackers with many opportunities to infiltrate digital wallets, or trick users into gaining access (Newman, 2017).

Best practice is to maintain two wallets, keeping only a small amount of Bitcoins on a computer or smartphone for everyday use, with the balance in an offline wallet (Cobb, 2018). This practice protects most user Bitcoins from malware trying to intercept the wallet password or trying to find unencrypted wallet data on the random access memory (RAM) (Cobb, 2018). The key to protecting cryptocurrency is to store it in a hardware wallet that stores private keys and currency offline (Newman, 2017). Offline wallets, also called cold storage, offer the highest

level of security as such wallets are not connected to the network, so it protects against computer vulnerabilities (Bitcoin.org, 2018).

A hardware wallet ensures the user controls the storage of the cryptocurrency (Ivanecky, 2018). Secure hardware wallets allow users to choose a personal identification number (PIN) number and recovery *seed*, in case the user forgets the PIN or the wallet malfunctions (Newman, 2017). The PIN and seed also need to be highly secured, in case of needed recovery (Newman, 2017). The offline, hardware wallet needs to be kept in a physically secure location, such as a bank vault, as users have mistakenly thrown away hard drives containing millions of dollars of Bitcoins (Cobb, 2018).

The downside to hardware wallets are that transactions become less efficient (Newman, 2017). The answer to this is to maintain two wallets. Low-value transactions could be stored in a small amount, in a wallet app (Newman, 2017). The cryptocurrency wallet software should be installed on a bootable universal serial bus (USB) or live compact disc (CD) to ensure the operating system is virus-free and does not cache, log, or store wallet keys (Cobb, 2018). The key is to keep only an amount which the user is willing to part with, in an app, and never to provide the private key to anyone (Newman, 2017).

It is also recommended to only keep coins in exchanges that the user plans to sell, in the immediate future, and to maintain less than $100 in online or smartphone wallets (Bitcoinsecurity101, 2018). As security currently stands, none of the apps should be trusted with too much cryptocurrency (Newman, 2017). The user should encrypt digital wallets with a strong password the user will not forget, not relying solely on the password management application (Bitcoinsecurity101, 2018).

An added security feature would be for the user to encrypt the private keys, but the encryption password, or passphrase, must be remembered (Cobb, 2018; Gilson, 2013). As the value of cryptocurrencies rises, so does uneasiness of being the only person able to access the currency. The system's high security has resulted in numerous investors being locked out, unexpectedly (Nova, 2018). Some experts prefer not to encrypt this form of information, because descendants would not be able to access inheritance, in case of death (Cobb, 2018). Investors need to have a backup plan for the family, so the location of wallets and passwords are known, in such a circumstance (Bitcoin.org, 2018).

Paper wallets are offline, significantly decreasing the chances of Bitcoins being lost to malicious hackers or computer viruses (Cobb, 2018). Printing the contents of the wallet, the private and public keys, creates a physical record which needs to be secured in a safe deposit box or vault (Cobb, 2018). In case of death, some investors have opted to use a paper wallet as a backup to the hardware wallet.

3-2-1 backup strategy. Within the fiat banking system, the bank is responsible for the security of funds, so users do not have to be concerned with backups. The situation is different with Bitcoin, and a shift in responsibility with which the average user is not used to, so it can result in money being lost due to simple mistakes (Bitcoinsecurity101, 2018). Backups will prevent accidental loss, as well as the adversarial destruction of data (Barber et al., 2012). Regular backups of a Bitcoin wallet are necessary, to protect against computer failure, theft, or human error, but are never to be stored online, especially if the backup is not encrypted (Cobb, 2018).

Users need to make regular backups of the Bitcoin wallet, in case of hard drive failure or theft. A good strategy is a 3-2-1 strategy: three backups on two different forms of media, an

external storage device, such as a portable hard drive and USB, and one of them should be offsite (Bitcoinsecurity101, 2018). Encrypting backups that are exposed to the network is good security practice, in case the device is lost or stolen (Newman, 2017). If using a hardware wallet, the backup information needs to be placed in a safe deposit box or vault (Newman, 2017). Using a hierarchical, deterministic hardware wallet means the user only has to perform a single, one-time backup (Bitcoinsecurity101, 2018). Following such basic rules can help prevent Bitcoin loss and theft.

It is essential to consider where the user stores private keys (Newman, 2017). Users should avoid revealing the private key by having it accessible in email (Roberts, 2017). Private key information should be stored offline, in a hardware device that is not connected to the Internet (Conti et al., 2017). The most secure is offline on a piece of paper or USB stick, in a safe deposit box (Roberts, 2017). It is recommended to keep the private keys encrypted and to avoid leaving them sitting out amongst other electronics that are frequently used (Newman, 2017). Forgetting the password can result in funds being permanently lost, so keeping a paper copy in a vault is highly recommended (Bitcoin.org, 2018).

Cybersecurity hygiene. In addition to using an offline wallet, with backups and encryption, it is essential to maintain good basic cybersecurity (Bitcoin.org, 2018). It is recommended to be careful with online cryptocurrency services and computers connected to the Internet (Bitcoin.org, 2018). As with typical cybersecurity best practices, users need to make sure software is updated and has high-quality, antivirus protection to protect devices used to access digital wallets (Dascalescu, 2017; Malanov, 2017). Bitcoin software needs to be kept up to date, so security patches are fixed, as well as software updates are installed on computers and

mobile devices (Bitcoin.org, 2018). It is important always to use the latest version of available Bitcoin software and a strong password that is a minimum of 16 characters (Cobb, 2018).

Users should consider current computer security best practices and apply them to cryptocurrency, such as using a password manager and enhanced security features on email addresses (Newman, 2017). Accessing the Internet using a secure web browser, such as Tor, improves upon security, always using a virtual private network (VPN) when connecting to other networks, and keeping the most sensitive data on a separate, encrypted hard drive or encrypted flash drive, improves upon cybersecurity practices (Dascalescu, 2017). In addition, Bitcoin has a multi-signature feature which can deflect theft, as transactions can require multiple, independent approvals before being spent (Bitcoin.org, 2018). Some web wallets also are multi-signature wallets (Bitcoin.org, 2018).

One way to mitigate DDoS attacks is to continuously monitor network traffic (Conti et al., 2017). Preventing DDoS attacks can also be done by configuring the network so malicious packets, and requests from unnecessary ports, are not permitted (Conti et al., 2017). Potential transaction malleability can be detected, by ensuring all transactions in the Bitcoin network have confirmations before proceeding (Conti et al., 2017).

Good password practices. It is important to use a strong password that has letters, numbers, punctuation, is at least 16 characters long, and has no recognizable letters or words (Bitcoin.org, 2018). In addition, the user must not forget the password or passphrase to access the password (Bitcoin.org, 2018). Investors should write down a mnemonic phrase that enables recovery of a crypto wallet, if lost, or if a password is forgotten (Malanov, 2017).

Two-factor authentication. Users need to be aware of the potential of social engineering scams and proactively monitor networks for any suspicious activity. A thief can

obtain the password for an account at a storage service, by merely obtaining a user's password. Most commonly, thieves break into customers' email accounts, asking the storage service to reset the password (Roberts, 2017).

Preventive measures to social engineering attacks include locking down email accounts, and online Bitcoin storage, with two-factor authentication (Roberts, 2017). Two-factor authentication also prevents losing Bitcoins due to technical failure or user error (Bitcoinsecurity101, 2018). Since texts can be intercepted, an app-based verification option such as Google Authenticator, should be used when using an online service (Roberts, 2017). The same level of cybersecurity measures is recommended for all password-protected, online services (Roberts, 2017). More advanced cybersecurity features, such as using Gmail's Advanced Protection feature and using a PIN or password to access the user's phone number, can make it even more difficult for attackers to seize account control by transferring the user's subscriber identity module (SIM) to their device (Newman, 2017).

When setting up two-factor authentication, it is recommended to print the quick response (QR) code out on paper and keep it in a safe place, in case of smartphone loss or theft (Bitcoinsecurity101, 2018). To use such Bitcoins, the QR code would need to be scanned, or the wallet's private key entered manually, into an application (Gilson, 2013). Without two-factor authentication, Bitcoins can be stolen with just an account password (Bitcoinsecurity101, 2018).

Improve on pseudo-anonymity. Bitcoin users can improve pseudo-anonymity in the Bitcoin system by creating and using a new Bitcoin address for each incoming payment and routing all Bitcoin traffic through an anonymizer such as Tor (FBI, 2012). The best way to obscure relationships between wallets is to transfer funds between them, via a mixing service

(Gilson, 2013). Mixing services are used to improve anonymity, and unlinkability, in the Bitcoin system (Conti et al., 2017).

Due to the risk of loss or fear of fraud, transactions with several Bitcoins can be broken down into sets of smaller transactions (Conti et al., 2017). To reduce a delay in transaction approvals, it is possible to make the payments offline, called *micropayments*, made through the micropayment channel (Conti et al., 2017). Part of the Bitcoin network, the transaction is posted once both parties trust each other on the transactions (Conti et al., 2017). If either misbehaves, the transaction is broadcast to the Bitcoin network (Conti et al., 2017). Advantages are that accelerating transaction times reduces the probability of double spending attacks (Conti et al., 2017).

Summary

Currently, digital currency is not widely used, nor accepted, and faces multiple challenges for the market to have future growth. In the cryptocurrency market, Bitcoin is definitely in the lead (Gandal et al., 2018). But Bitcoin suffers from high volatility, poor pseudo-anonymity, and cyber attacks (FBI, 2012; Sabin, 2018). Bitcoin's lack of stable pricing makes it difficult to assess its real value, increasing the risk of loss to investors (Bulgakov, 2014).

It is questionable as to whether Bitcoin meets the criteria for currency, as Bitcoin does not meet the three facets required for standard currency: to be a medium of exchange, unit of account, and store of value. Since Bitcoin does not meet the status of legal tender, it has been treated as a commodity cash market (CFTC, 2017). The securities market has been pushing towards classifying Bitcoin as a security, so that it would be disposed to securities regulations (Duggan, 2017).

The larger the Bitcoin market becomes, the more impact it could have on the global, financial system (Iwamura et al., 2014a). Bitcoin spread in popularity because it is viewed as the *reserve currency* of the cryptocurrency market, similar to how the U.S. dollar compares to other currencies (Thompson, 2017). The financial community has high-profile skeptics as to whether Bitcoin holds any value and is not just driven by speculative investment. Thus far, Bitcoin has been primarily used as an investment vehicle (Boehme et al., 2015; Yermack, 2013).

The perceived value of Bitcoin is important in the market, as the value can affect price bubbles. One of the problems with Bitcoin is the instability of its market value, which is viewed as an obstacle to adopting an even wider base of users (CPMI, 2015; Iwamura et al., 2014a). While the Bitcoin system controls the rate of Bitcoin creation, the market value is determined by the supply of Bitcoins in circulation and users' rate of holding, or trading, in the currency (FBI, 2012). Scholarly, economic studies have attempted to explain reasons behind Bitcoin volatility. Before Bitcoin can mature in the market, risk in investing in the cryptocurrency has been likened to investing in a start-up company. Financial advisors caution that Bitcoin is too risky to treat seriously (Nova, 2017a).

Non-users of Bitcoin have cited concerns regarding privacy in Bitcoin's blockchain (O'Malley & Presthus, 2017). By studying patterns in the blockchain, it is possible to link user pseudonyms together. For more security, users should use a different public key for each transaction. Analyzing the transaction graph in the blockchain has also linked Bitcoin addresses to IP addresses, which completely deanonymizes users (Conti et al., 2017).

Nearly half of Bitcoin investors routinely worry about the technological security of their funds (Nova, 2017a). Bitcoin is vulnerable to fraud, theft, and criminal hackers (Yermack, 2013). Virtual currencies are a preferred target for malicious hackers because of Bitcoin value

and its relatively weak security (Dascalescu, 2017). Malicious hackers are targeting anywhere they can find a cybersecurity flaw, especially in online Bitcoin wallets and currency exchanges (Dascalescu, 2017). Main attack vectors for cybercriminals focus on key theft (Scheuermann & Tschorsch, 2016).

Bitcoin attack vectors include wallet attacks (Conti et al., 2017). Digital wallet types range from software, hardware, paper, brain, to online wallets (Scheuermann & Tschorsch, 2016). One of the most preferred ways to use Bitcoin is with a software wallet (Scheuermann & Tschorsch, 2016). However, online wallets are more vulnerable to theft than hardware wallets. The trade-off is the lack of usability with more secure wallets. Best practice is to maintain two wallets, with a maximum of $100 in an online wallet, for everyday use, with the balance in an offline, hardware wallet (Cobb, 2018). Bitcoin users need to regularly backup their wallets, to prevent accidental loss, as well as the adversarial destruction of data (Barber et al., 2012).

The most common networking attacks on Bitcoin are inexpensive DDoS attacks (Conti et al., 2017). Due to the potential for a larger revenue, most DDoS attacks target currency exchange services and large mining pools (Conti et al., 2017). Bitcoin stealing can entail payment information being spoofed (Malanov, 2017). Users have been tricked into going to phishing websites (Malanov, 2017). Thieves have also used social engineering to obtain passwords to user accounts, at online storage services, bypassing even two-factor authentication (Dascalescu, 2017).

To minimize financial risk, financial experts advise Bitcoin investors only to invest as much as users can afford to lose, due to volatility (Hickey, 2017). To minimize cybersecurity risk, investors must be knowledgeable regarding the Bitcoin companies with which they do business and should only do business with those who have instilled proper cybersecurity

measures. Investors need to practice good cybersecurity vigilance and always need to verify an Internet wallet's address (Malanov, 2017). Software needs to be updated and high-quality, antivirus protection needs to be installed, to protect devices used to access digital wallets (Dascalescu, 2017; Malanov, 2017). Enabling two-factor authentication is important, so Bitcoins are not stolen with just an account password (Bitcoinsecurity101, 2018).

Discussion of the Findings

This study examined a substantial amount of literature relating to the vulnerabilities and risk involved with the cryptocurrency market of Bitcoin. The research involved an investigation of scholarly resources to establish an academic framework of analysis. Scholarly journals provided the in-depth, technical background on the historical development of Bitcoin, as well as a microscopic glance at the complexities of the cryptocurrency market. Press releases of current events provided time-sensitive information on rapid changes within the Bitcoin market. The combined analysis formed a contemporary understanding of the complexities of the ever-evolving Bitcoin market.

Causes of Bitcoin Volatility

Bitcoin emerged as a dominant pioneer amongst a cryptocurrency market known for innovation, simplicity, transparency, and a rise in popularity (Katsiampa, 2017). Although referred to as a *currency*, Bitcoin does not meet the necessary criteria for standard currency: medium of exchange, unit of account, and store of value. Bitcoin is minimally accepted as a medium of exchange, viewed as very risky for normal transactions, not used as a unit of account, and, due to volatile price swings, not considered suitable as a store of value (Alvarez-Ramirez et al. , 2018; Bariviera et al., 2017). The CFTC considers Bitcoin to have the status of a commodity cash market, while the SEC leans towards classifying Bitcoin as a security so that regulations could ensue (CFTC, 2017; Duggan, 2017). The IRS, on the other hand, considers Bitcoin to be a property and taxes it accordingly (Williams, 2014). To most, Bitcoin is used for investment and investors' hope for huge financial gains are what drives up Bitcoin prices. Bitcoin's spread in popularity is due to the status of being viewed as the *reserve currency* to the cryptocurrency market, similar to how the U.S. dollar is viewed (Thompson, 2017).

Despite the spread of Bitcoin, one of the main problems with Bitcoin is instability of its market value (Iwamura et al., 2014b). Understanding how Bitcoin value is determined seems abstract to users who are familiar with traditional financial markets. The lack of relying on a central bank means the Bitcoin market can be affected by macroeconomic factors such as economic, social, and political news, as well as rumors (Alvarez-Ramirez et al. , 2018). Since Bitcoin is a network, the number of Bitcoin users is key to determining the value to the users (Corbet et al., 2017). The perceived value of Bitcoin is important, as the value can affect price bubbles. Studies have indicated Bitcoin is susceptible to significant bubbles, particularly prior to major events affecting the Bitcoin market or from spillover from rival cryptocurrencies (Corbet et al., 2017). Contradictory studies have indicated Bitcoin returns are driven internally, by buyers and sellers, not by external, economic factors (Corbet et al., 2017).

Lack of stable pricing creates a challenge to assessing the real value of Bitcoin and increases the risk of loss to investors, which has thwarted potential users of Bitcoin (Bulgakov, 2014). This factor renders Bitcoin, as well as other cryptocurrencies, unlikely to fully replace currencies from central banks (Iwamura et al., 2014b). The market value is determined by the supply of Bitcoins in circulation and the rate of holding, or trading, Bitcoins (FBI, 2012). There are numerous theories on Bitcoin's potential. Some economists theorize Bitcoin circulation decreasing too drastically can result in a loss of interest in the system, making it too weak to sustain itself (Barber et al., 2012). Other economists theorize the planned, finite supply of Bitcoin will hit a deflationary spiral, as Bitcoins are lost over time and supply diminishes (Bonneau & Goldfeder, 2017). The set limit of a maximum of 21 million Bitcoins prevents inflation and the system controls the rate of Bitcoin creation, so others speculate the only method of growth for Bitcoin is for the currency to appreciate (Barber et al., 2012; FBI, 2012).

Some studies ascertain Bitcoin manifests instability from the lack of flexibility in the Bitcoin supply production and the risk of price drops, which affect the sustainability of mining for new blocks (Iwamura et al., 2014b). The fixed supply of Bitcoins creates a mechanism by which the demand for Bitcoin increases as the price decreases and vice-versa, creating price volatility (Iwamura et al., 2014b). If Bitcoin prices fall too drastically low, miners could stop being incentivized to mine for new Bitcoins, placing the entire system at risk (Iwamura et al., 2014b). Other studies indicate Bitcoin price is dependent on price directionality. As prices increase, there are wild fluctuations, making it more unpredictable (Alvarez-Ramirez et al. , 2018). Some studies believe the promised potential of large returns in Bitcoin attracts speculative investors, who amplify market volatility (Alvarez-Ramirez et al. , 2018). Still, other studies point to circumstantial evidence where speculative trading did not drive the presence of excess volatility (Blau, 2017). As investment and capitalization grows, authors have argued Bitcoin is converting to market efficiency and decreasing volatility, over time (Alvarez-Ramirez et al. , 2018; Bariviera et al., 2017). Before full maturity, investing in cryptocurrency has been compared to investing in a start-up and too risky for serious investment (Nova, 2017b).

Vulnerability to the Lack of Privacy

As Bitcoin increases in popularity, the more value it generates to existing, and potential, users (O'Malley & Presthus, 2017). For non-users to join in on the Bitcoin market, elements such as stability, security, value, usefulness, ease of use, and privacy need to be addressed (O'Malley & Presthus, 2017). When a user wants to transfer Bitcoins, the transaction is broadcast into the P2P network through asymmetric cryptography (Jordan, et al., 2013; Prpic, 2017). The public nature of Bitcoin's blockchain creates a threat to privacy as user pseudonyms can be linked together by studying patterns in the blockchain. Bitcoins are linked with an

address, and it is optimal to use a new address for each transaction to enhance security and pseudo-anonymity (Miller, 2015). Each address is distinctly tied to a pair of public and private keys, which control the Bitcoins (Miller, 2015). Keeping the private key secure is crucial to theft prevention (Miller, 2015).

Satoshi's original vision was that privacy would be sustained by keeping public keys pseudo-anonymous, but Bitcoin's pseudo-anonymity has been exploited by analyzing the blockchain (Nakamoto, 2008). Analyzing the blockchain can reveal Bitcoin users and their purpose by linking multi-input transactions, which reveal other transactions belonging to the same user (Conti et al., 2017). Bitcoin addresses have even been linked to leaked IP addresses, which completely deanonymizes users, but at a low rate of possibility (Conti et al., 2017).

Methods to mitigate online exposure entail using an Internet anonymity service, such as Tor, which conceals the originating IP address and user's physical location (FBI, 2012; Scheuermann & Tschorsch, 2016). To re-establish financial privacy, a secure and anonymous mixer can be used. Mixing services mix the funds of random users before sending the mixed currency to a recipient (Miller, 2015). Mixers also pool transactions into unpredictable combinations when mixing Bitcoins (Boehme et al., 2015). The first generation of mixers had problems, in that users had to blindly trust that their funds were not stolen or their data breached (Grossmann et al., 2018). Despite improving anonymity, user's anonymity is still set to the number of users participating in the mix (Grossmann et al., 2018).

Vulnerability to Cyberattacks

The decentralized nature of Bitcoin makes it vulnerable to attack, as the lack of middlemen eliminated legal protections with cryptocurrencies. Criminal hackers find the Bitcoin

market especially appealing by exploiting third-party Bitcoin services and individual Bitcoin wallets, which have become points of failure for the system (FBI, 2012).

The only means by which Bitcoin can be stolen is for a thief to trick the user, trick a third-party the user relies on into getting access to Bitcoin, or for the third-party to be compromised (Roberts, 2017). Although Bitcoin itself has not been compromised, malicious hackers target systems that hold and store Bitcoin private keys (Kshetri, 2017). The theft or loss of private keys essentially equates to the loss of funds and is the main attack vector for cybercriminals (Barber et al., 2012; Scheuermann & Tschorsch, 2016). If a user's wallet service stores the private key, the risk of the digital wallet being compromised rises (Boehme et al., 2015). As the value of Bitcoin increases, so does the number of viruses trying to steal Bitcoins (Cobb, 2018). The ideal targets for malicious hackers are large currency exchanges.

To use Bitcoin, users need a digital wallet, which holds the pair of public and private keys. Digital wallet types can range from software, hardware, paper, brain, to online wallets, with software wallets being among the most common wallet types (Scheuermann & Tschorsch, 2016). All software and online wallets are vulnerable to security vulnerabilities because an attacker gaining access to a computer gains access to the user's wallet (Scheuermann & Tschorsch, 2016). Hardware wallets are more secure, but also less usable. Hardware wallets use a separate device that typically operates offline, which makes it much harder for an attacker to break into the wallet (Scheuermann & Tschorsch, 2016). Even more secure are paper and brain wallets. Other users prefer to store Bitcoins in an online currency exchange, making them vulnerable to the security of the exchange (Conti et al., 2017; Moore et al., 2014). Thefts of digital wallets have mainly occurred due to hacked computer systems, faulty software, and poor configuration of systems (Scheuermann & Tschorsch, 2016).

The most common networking attacks on the Bitcoin system are inexpensive DDoS attacks (Conti et al., 2017). To cause the disruption, multiple attackers launch the denial of service at the same time (Conti et al., 2017). Distributed denial of service attackers have mostly targeted Bitcoin currency exchanges and mining pools, while gambling operators, digital wallets, and Bitcoin financial services have also been targeted (Conti et al., 2017). Big mining pools, with hash rates historically over five percent, are more likely to be targeted.

Malleability attacks have facilitated DDoS attacks in Bitcoin, as the attacker clogs the transaction queue of all pending transactions (Conti et al., 2017). The attacker instills bogus transactions, with a high priority, by falsely depicting itself as the highest incentive payer to the miners (Conti et al., 2017). A specific type of malleability attack, transaction malleability, exploits a bug in Bitcoin that can change the transaction identifier (TXID) without invalidating the transaction (Scheuermann & Tschorsch, 2016). An attacker makes an individual believe a transaction has failed, although the transaction is later confirmed (Scheuermann & Tschorsch, 2016).

Bitcoin miners conglomerate into mining pools to increase mining rewards. The Bitcoin structure needs to strive for a setup where no one entity controls over half of the computational power to prevent a 51 percent attack, a worst-case scenario (Scheuermann & Tschorsch, 2016). Satoshi envisioned the system naturally prevents such majority-miner attacks. The mining pool GHash.io has neared 51 percent, but promised to limit its size, so as not to diminish confidence in Bitcoin (Boehme et al., 2015; Scheuermann & Tschorsch, 2016). Newer threats, such as crypto mining malware attacks, worms, malicious Android apps, zombified home routers, and social engineering have also been used for scams (Trend Micro, 2017).

Attacking the signature enables Bitcoin-stealing. Typical transactions require the user to have a public key and signature, using the private key, to prove ownership (Conti et al., 2017). The user is required to generate a signature by choosing a random value (Conti et al., 2017). Using a dictionary attack, attackers have guessed poorly created private keys and compromised user accounts (Merkle, 2017). It is essential to use highly random, and diverse, per-signature values, to maintain security (Conti et al., 2017).

Criminal hackers have employed various avenues of attack. Payment information has been spoofed, as well as phishing websites of actual online wallet providers (Malanov, 2017). Untrustworthy crypto investment ventures have vanished overnight, with no avenues of retribution for the investor (Roberts, 2017). Cryptocurrency wallets that are stored on the user's computer can be stolen, or lost, in case of a hard disk crash (Malanov, 2017). Theft of Bitcoin can also occur if malicious hackers obtain the password to a user account at an online storage service (Roberts, 2017). Malicious hackers have used social engineering to use a security loophole that verifies security through a user's phone number to steal user accounts and gain access to cryptocurrency keys (Shin, 2016).

Protective Cybersecurity Measures

To trust Bitcoin, people need to feel the system has the properties of money, as well as a degree of security (Bulgakov, 2014). Security breaches undermine users' confidence in cryptocurrencies (CPMI, 2015). Cybersecurity risks with Bitcoin range from users losing Bitcoins themselves, to being hacked. The challenge is that users need to be diligent about their Bitcoin account credentials, which is new for users not used to being their own bank (Hickey, 2017). Bitcoin accounts stored on a computer are exposed, since Bitcoin wallet applications save their data in predictable locations, making them susceptible to trojan attacks (Gilson, 2013).

Financial experts advise Bitcoin investors only to invest as much as users can afford to lose (Hickey, 2017). Typically, the more volatile the investment, the smaller proportion of wealth that should be divested (Hickey, 2017). Volatility and uncertainty of Bitcoin prices have led Bitcoin not to be considered a more stable investment. Investors need to be cognizant of the lack of regulation with cryptocurrencies and should research virtual currency platforms, and digital wallets, prior to investment. Bitcoin users need to exercise cybersecurity hygiene and be vigilant of all transactions, including not following links and verifying wallet addresses (Malanov, 2017). Users should double-check the recipient's address, amounts being sent, fees, and look for a green *https* tag before a website's URL (Malanov, 2017; Villas-Boas, 2018). Users should practice cybersecurity best practices, such as using updated software and high-quality, anti-virus protection, on computers and mobile devices connected to the Internet (Dascalescu, 2017; Malanov, 2017).

It is also recommended to use enhanced security features for email, make use of a secure web browser, such as Tor, to improve upon security, use a VPN when connecting to other networks, and keep the most sensitive data on a separate, encrypted hard drive (Dascalescu, 2017; Newman, 2017). Distributed denial of service attacks can be mitigated by continuously monitoring network traffic and configuring the network so malicious packets are not permitted (Conti et al., 2017). It is important to use strong passwords that are unrecognizable (Bitcoin.org, 2018). To protect against social engineering, investors can lock down email accounts and online Bitcoin storage with two-factor authentication (Roberts, 2017). Two-factor authentication protects against theft with just account passwords, technical failure, or user error (Bitcoinsecurity101, 2018). An app-based verification option, such as Google Authenticator, is recommended for online services (Roberts, 2017).

Best practice for Bitcoin users, in particular, is to maintain two wallets, a small number of Bitcoins in an online wallet, and, offline, a hardware wallet that stores the private keys and balance (Cobb, 2018; Newman, 2017). Only an amount which the user is willing to part with should be online (Newman, 2017). Offline wallets offer the highest level of security, protecting users from malware trying to intercept the wallet password, or trying to find unencrypted wallet data on the RAM (Bitcoin.org, 2018; Cobb, 2018). The offline, hardware wallet needs to be placed in a physically secure location, such as a bank vault (Cobb, 2018). Only Bitcoins the user plans to sell in the near future, should be in an online exchange (Bitcoinsecurity101, 2018). Digital wallets and private keys should be encrypted, but it is vital encryption passwords are not forgotten nor mishandled (Cobb, 2018; Gilson, 2013; Newman, 2017).

Contrary to the fiat banking system, the Bitcoin investor is responsible for backups. The investor needs to make regular backups of the Bitcoin wallet, in case of hard drive failure or theft. Recommended is the 3-2-1 strategy whereby three backups are on two different forms of media, an external storage device, and one is offline (Bitcoinsecurity101, 2018). Backups exposed to the network should be encrypted, in case of loss or theft (Newman, 2017). Pseudo-anonymity can be improved upon by using a new Bitcoin address for each incoming payment and routing all Bitcoin traffic through an anonymizer, such as Tor (FBI, 2012). Relationships between wallets can be obscured using a mixing service (Gilson, 2013).

Summary

In conclusion, this study has explored aspects of the Bitcoin cryptocurrency market which challenge a further spread of Bitcoin's popularity. The term currency is misleading for Bitcoin, as Bitcoin does not meet the basic elements to function as currency. Experts disagree on whether Bitcoin is a commodity cash market, security, or property, as the IRS classifies it. One

of Bitcoin's main, missing factors, to be considered a currency, is price predictability and the level of financial risk involved is also a hindrance. Experts cannot agree on the causes of Bitcoin volatility, but it has made Bitcoin too risky for serious investment and has fostered a start-up mentality.

Lack of privacy is one of the key factors that make potential users of Bitcoin refrain from joining in. While creating transparency, the public nature of the blockchain also threatens privacy, as linking pseudonyms can reveal transactions belonging to the same user. Mitigating online exposure requires the investor to proactively use an Internet anonymity service or a Bitcoin mixing service.

Bitcoin's decentralized nature makes it vulnerable to cyberattacks, as there is no method of repercussion available. Criminal hackers find Bitcoin appealing by targeting the points of failure, third-party Bitcoin services. Keeping private keys secure is crucial to theft prevention, which transcends to securing digital wallets. While offline wallets ensure the most security, there is also a decrease in usability which must be balanced. Optimally, users should maintain two wallets, to decrease online vulnerability. Most commonly, inexpensive DDoS attacks are used to breach account information, in addition to social engineering, and other attack methods.

Security breaches undermine user confidence in Bitcoin. As compared to traditional, financial markets, investors must be more diligent in securing cryptocurrency. Investors need to actively implement protective, cybersecurity measures, to safeguard themselves against theft or loss of Bitcoins. Lack of regulation in the cryptocurrency market creates the need for investors to research virtual currency platforms, beforehand, and to practice good cybersecurity hygiene before entering any Bitcoin account information online.

Recommendations

This study investigated the significant financial and cybersecurity concerns surrounding Bitcoin, both of which minimize Bitcoin's spread to a wider user base. Bitcoin's appeal, its simplicity, flexibility, and decentralization, also created weaknesses. The subsequent research recommendations attempt to address how Bitcoin could begin to mitigate risks, to be more incorporated into financial markets, and to gain a wider acceptance of investment.

Improve Stability: Increase User Confidence in Bitcoin

Bitcoin price stability hinges upon participant belief in its value and market value is determined by the supply of circulating Bitcoins. As speculated by economists, if the currency gained a wider acceptance, the only outlet for growth would be for Bitcoin prices to rise. Expanding the number of Bitcoins in circulation requires an increase in user confidence. Although the research presented described which security and financial risks prevent a rise in Bitcoin popularity, steps on how to directly increase popularity are still ambiguous. Advertising campaigns and the spread of Bitcoin financial services could help lead to a more widespread adoption of Bitcoin for payment.

Currently, there is no method by which financial risk involving Bitcoin can be dissolved, as it is comparable to attempting to stabilize an investment position in speculative stocks. It is speculated that if Bitcoin gained in popularity, and use, it could stabilize prices. Of all cryptocurrencies, Bitcoin has the largest cryptocurrency market share and would be the most likely to achieve such a status.

Improve Usefulness: Increase Bitcoin Adoption Among Businesses

Rather than just have Bitcoin viewed as a speculative investment, expand the view of Bitcoin as a method of payment. Bitcoin presently seems to be minimally accepted for online

transactions. If the number of merchants who accept payment in Bitcoin was to fundamentally increase, more consumers could potentially have the curiosity to try using Bitcoin. Such vendors would need to have marketing strategies that effectively educate the populace on how Bitcoin simplifies online transactions, which is one of its main benefits. To potential users, Bitcoin is still a mystery.

In general, Bitcoin tends to appeal to the technologically savvy millennials, so marketing campaigns of Bitcoin's benefits need to permeate that age group. Widespread attainment of cryptocurrency acceptance for online goods and services could also develop into a *me-too* attitude, whereby consumers want to try what others are doing, because Bitcoin seems acceptable nearly everywhere. If potential consumers could see more value in Bitcoin use, other than perhaps for its previously famed reputation for nefarious goods, more customers could lean towards acquiring Bitcoin.

Improve Security: Reduce Cybersecurity Risk with Self-Education

To reduce the risk of investors losing Bitcoins, or being hacked, investors need to, themselves, be vigilant regarding their account credentials. Every Bitcoin user is essentially their own bank. This is a new concept for many individuals. Education of the user populace is essential, as cryptocurrencies are, in large part, still a mystery. Bitcoin users need to educate themselves, on how to buy, sell, and store Bitcoins properly, and minimize security risks. Investors need to be informed on cryptocurrency volatility and the potential for monetary loss, so they diversify investments.

To maintain effective cybersecurity hygiene, users need to safeguard their assets and be vigilant of all online transactions. The reliance on third-party intermediaries creates a cybersecurity risk for Bitcoin. Bitcoin investors need to be self-informed on how to reduce

susceptibility to malicious hackers, by becoming knowledgable on security vulnerabilities of third-party Bitcoin intermediaries and cybersecurity best practices for cryptocurrency. Bitcoin users need to be informed on how to minimize privacy concerns and online exposure through Bitcoin's pseudo-anonymous network. Maintaining different public keys for each Bitcoin transaction and using secure, and anonymous, mixers maximizes online privacy.

Improve Ease of Use: Reduce Cybersecurity Risk with Cryptocurrency Advisors

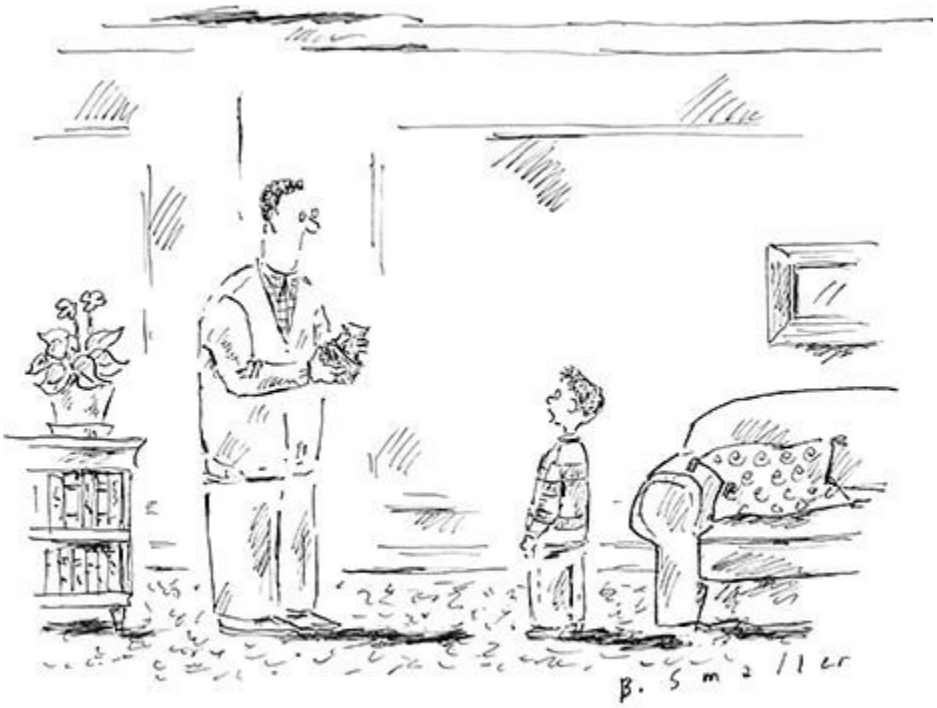
Bitcoin is not simply a new financial payment method, but also a blending of technology and finance, which compounds confusion onto its members. For investors who do not have the time, nor desire, to educate themselves on the nuances of Bitcoin security, cryptocurrency advisors should be available, for a small fee. Advisors could bridge the gap so novices to cryptocurrencies safely navigate assets in the Bitcoin system, without being overwhelmed. As Bitcoin investors first set up accounts, they are at their most vulnerable, so working with a cryptocurrency advisor, from the beginning, is essential. Cryptocurrency advisors need to be experts in fintech, or technology used to support financial services, and able to manage cybersecurity of their client's cryptocurrency assets.

Cryptocurrency advisors would work to reduce their client's vulnerability to criminal hackers by keeping Bitcoin private keys secret, and secure, and guiding investors to make wise decisions in the face of market price instability. The fintech investment office could be a one-stop shop that also offers secure, physical storage of hardware wallets, equivalent to safe deposit boxes at banks. Advisors would secure payment and digital wallet information, reduce vulnerability to malware, reduce phishing, and social engineering by improving upon user education of protection of cryptocurrency. Financial services could also provide additional protection against DDoS attacks.

Recommendations for Future Research

Bitcoin is a new technology that has great promise, and great believers in its potential, but further study will be needed, for a more informed outlook on emerging cryptocurrency markets. Causes of volatility and market price instability are still debatable and more studies on how volatility is changing over time, will need to be done. By what means Bitcoin could become less risky is still not concrete, so more data and knowledge on this topic is required. Additional areas that require research concern whether it is possible to improve upon Bitcoin, the pseudo-anonymity, and exposure within mixing services, as mixing services evolve. Methods by which to improve user confidence in Bitcoin investments, other than by addressing cybersecurity vulnerabilities, could also lead to discovering how to spread this new, financial concept.

Conclusion



"If it's all the same to you, I'd like my allowance in bitcoins."

Figure 5. The future of Bitcoin, by B. McGrath, 2013, *The New Yorker*.

Emerging as a seeming response to the central bank failures to manage the financial crisis of 2008, Bitcoin is a pioneer in a global, financial experiment. Innovative for its time, the Bitcoin market is an emerging financial system that has no similar precedents in recent history. Envisioned to be a currency, asset, payment system, and similar to gold, retain value, evidence provided during this research indicated otherwise. While Bitcoin tried to address shortcomings in traditional currency, it became clear Bitcoin has shortcomings of its own. Bitcoin proved to not be a very good form of currency, medium of exchange, nor store of value, primarily due to volatility.

As cryptocurrencies exist today, they do not threaten financial markets due to their limited connection to the actual economy and lack of wide acceptance. While there are

traditional investors who speculate on the eventual dissolution of cryptocurrencies, others speculate on the eventual integration of Bitcoin into society, as comically depicted in Figure 5. If Bitcoin became more integrated, it could become a potential source of instability if volatility did not decrease. Volatility equates to economic risk. If a time comes when Bitcoin becomes more integrated into traditional, financial markets and payment systems, regulators will more than likely want to try to pursue policies that allow more oversight of the unregulated market. The unregulated Bitcoin market is a risk to investors, but the lack of regulation is also, partially, what brings appeal to Bitcoin.

Digital currency has a long way to go, though, before the possibility of being incorporated into global, financial transactions at a popular rate and becoming long-term sustainable. Bitcoin sits on the fringes of the financial system, influencing the traditional, financial system and creating a challenge for central banking. An increase in confidence in Bitcoin, and more robust, wider acceptance, would intrinsically increase Bitcoin value and would, according to experts, potentially stabilize market prices. Lack of stable pricing increases risk of potential loss to investors, keeping them away. Lack of privacy is also a limiting factor for Bitcoin to spread to a wider user base. Bitcoin's usability, or lack of ease of use, could also be a hindrance to the spread of Bitcoin. For the low transaction volume of virtual currencies to improve, the factors addressed in this research would need to be addressed.

Bitcoin's technology can be trusted, if it is understood by the user, or the user relies on safe, third-party institutions. The element of trust is essential to acquiring new Bitcoin users, as well as maintaining current ones. Wallet service providers need to earn users' trust. As the Bitcoin system currently exists, users need to be self-vigilant of their online use and must maintain high, cybersecurity awareness levels to prevent being a victim to scams. More recent

thefts have been due to carelessness or incompetency, by Bitcoin owners, and deception by dishonest, third party Bitcoin institutions.

Cybersecurity threats to Bitcoin are a big risk, and will remain, a big risk to the Bitcoin system, due to its online environment and appeal. Most likely, there will be no technology cure-all that will solve security breaches. From users losing funds, themselves, to being attacked, security breaches undermine user confidence in cryptocurrencies and limit its spread. Cybersecurity is crucial to cryptocurrencies. Investors need to equate Bitcoin wallets to having a wallet filled with cash, which stresses its susceptibility to theft, and need to secure digital identities. Since Bitcoin users are not used to the shift in financial responsibility, fintech companies could help fill in the gap because keeping Bitcoins secure is complicated and time-consuming.

Bitcoin paved the way for a system whereby an Internet user could directly transfer currency to another Internet user. If sustained, this network could lay the groundwork for future transfers of digital property, contracts, money, and even ownership of physical assets. If the network of trust dissolves, cryptocurrencies, and Bitcoin, could also dissolve and all investments be rendered worthless. The outcome will most likely hinge upon the stabilization of market prices, a broader adoption of Bitcoin, and increase in its value.

Until Bitcoin becomes more mainstream, moving entire life investments into Bitcoin, over more balanced investment vehicles, is not recommended. It is recommended to only play with money you can afford to lose. If individuals learn to benefit from the use of some form of digital currency and alternative digital currencies grow, Bitcoin will have to think innovatively, to remain competitive and remain the *reserve currency* among rival cryptocurrencies. As Bitcoin evolves, so too will malicious hackers, in finding potential holes in the system. The future

forecast of Bitcoin is, as of yet, unclear, but cryptocurrency believers hope in its social and future financial impact.

References

Alvarez-Ramirez, J., Ibarra-Valdez, C., J, & Rodriguez, E. (2018). Long-range correlations and asymmetry in the Bitcoin market. *Physica A, 492*, 948-955. Retrieved from https://doi.org/10.1016/j.physa.2017.11.025

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better—how to make Bitcoin a better currency. *Lecture Notes in Computer Science*(7397), 399-414. Retrieved from http://dx.doi.org/10.1007/978-3-642-32946-3_29

Bariviera, A., Basgall, M., Hasperuéb, W., & Naiouf, M. (2017). Some stylized facts of the Bitcoin market. *Physica A*, 82-90. Retrieved from https://doi.org/10.1016/j.physa.2017.04.159

Bitcoin.org. (2018). *Securing your wallet*. Retrieved from Bitcoin: https://bitcoin.org/en/secure-your-wallet

Bitcoinsecurity101. (2018). *Bitcoin Security 101*. Retrieved from Bitcoin Security 101: http://bitcoinsecurity101.com/getting-started/

Blau, B. (2017, October). Price dynamics and speculative trading in Bitcoin. *Research in International Business and Finance, 41*, 493-499. Retrieved from https://doi.org/10.1016/j.ribaf.2017.05.010

Blockchain. (2018, March 12). *Bitcoins in circulation*. Retrieved from Blockchain: https://blockchain.info/charts/total-bitcoins

Blockchain. (2018, Feb 20). *Blockchain charts*. Retrieved from Blockchain: https://blockchain.info/charts

Blockchain. (2018, Feb 19). *Blockchain.info*. Retrieved from Confirmed Transactions Per Day: https://blockchain.info/charts/n-transactions

Blockchain.info. (2018, March 21). *Market Price*. Retrieved from Blockchain: https://blockchain.info/charts/market-price?timespan=180days

Boehme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213-238. doi:10.1257/jep.29.2.213

Bonneau, J., & Goldfeder, S. (2017, December 18). *5 Myths about Bitcoin you need to understand*. Retrieved from The Washington Posts: https://www.sciencealert.com/myths-about-bitcoin?perpetual=yes&limitstart=1

Bonneau, J., Clark, J., Felten, E., Kross, J., Miller, A., & Narayanan, A. (2015, May). *SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies.* IEEE Security

and Privacy. Retrieved from http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf

Bulgakov, D. (2014). Problems of using digital cryptocurrency Bitcoin. *The 9th International Forum for Students and Researchers*, *2*. Retrieved from http://ir.nmu.org.ua/handle/123456789/148297

Cheng, E. (2017, December 17). *Bitcoin debuts on the world's largest futures exchange, and prices fall slightly*. Retrieved from CNBC: https://www.cnbc.com/2017/12/17/worlds-largest-futures-exchange-set-to-launch-bitcoin-futures-sunday-night.html

Clinch, S., Davies, N., Khairuddin, I., & Sas, C. (2016, May 7-12). Exploring motivations among Bitcoin users. *CHI'16 Extended Abstracts*, 2872-2878. doi:http://dx.doi.org/10.1145/2851581.2892500

Cobb, M. (2018). *How to secure bitcoin: What are the best ways to keep it safe?* Retrieved from TechTarget: http://searchsecurity.techtarget.com/answer/Is-Bitcoin-safe-The-truth-about-Bitcoin-security-and-crypto-currency

Coin Desk Publications. (2014). Virtual currencies - Bitcoin risk. *World Bank Conference* (pp. 1-14). Washington, D.C.: Boston University.

Coindesk. (2018, Apr 26). *Coindesk*. Retrieved from Bitcoin Calculator: https://www.coindesk.com/calculator/

CoinMarketCap. (2018, Feb 21). *Cryptocurrency market capitalizations*. Retrieved from CoinMarketCap: https://coinmarketcap.com/

Committee on Payments and Market Infrastructures. (2015). *Digital currencies.* Bank for International Settlements. doi:978-92-9197-385-9

Conti, M., Kumar, S., Lal, C., & Sushmita, R. (2017). A survey on security and privacy Issues of Bitcoin. *ArXiv*, 1-36. Retrieved from https://arxiv.org/pdf/1706.00916.pdf

Corbet, S., Lucey, B., & Yarovaya, L. (2017). Datestamping the Bitcoin and Ethereum bubbles. *Finance Research Letters*, 1-8. doi:10.1016/j.frl.2017.12.006

Dascalescu, A. (2017). *Cryptocurrency security: How to safely invest in digital currency*. Retrieved from Heimdal Security: https://heimdalsecurity.com/blog/cryptocurrency-security-how-to-safely-invest-in-digital-currency/#cyberstory

Duggan, W. (2017, December 22). *Commodity, Currency, Security, Or Scam: What Type Of Asset Do You Think Bitcoin Is?* Retrieved from Benzinga: https://www.benzinga.com/analyst-ratings/analyst-color/17/12/10946463/commodity-currency-security-or-scam-what-type-of-asset-

Dunkley, E. (2017, December 20th). *Problems at two cryptocurrency exchanges raise security concerns*. Retrieved from Financial Times: https://www.ft.com/content/aa9fdd64-e536-11e7-97e2-916d4fbac0da

Dziembowski, S. (2014). Introduction to Bitcoin. *The First Greater Tel Aviv Area Symposium* (pp. 1-75). Tel Aviv, Israel: University of Warsaw. Retrieved from The first greater Tel Aviv area symposium: https://www.cs.bgu.ac.il/~crp161/wiki.files/bitcoinDec2015c.pdf

Dziembowski, S. (2015). Introduction to cryptocurrencies: A tutorial. *ACM CCS'15* (pp. 1-57). Denver, Colorado: University of Warsaw.

Eyal, I., & Sirer, E. (2013). *Majority is not enough: Bitcoin mining is vulnerable.* Ithaca, NY: Cornell University. Retrieved from https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf

FBI. (2012). *(U) Bitcoin virtual currency: unique features present distinct challenges for deterring illicit activity.* FBI Directorate of Intelligence. Retrieved from https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

Field, M., & McGoogan, C. (2017). *What is cryptocurrency, how does it work and why do we use it?* Retrieved from The Telegraph: http://www.telegraph.co.uk/technology/0/cryptocurrency/

Forbes. (2018, April 9). *Forbes/Profile/Warren Buffet*. Retrieved from Forbes: https://www.forbes.com/profile/warren-buffett/

Gandal, N., Hamrick, J., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, 1-11. Retrieved from https://doi.org/10.1016/j.jmoneco.2017.12.004

Gilson, D. (2013). *5 security tips for Bitcoin beginners*. Retrieved from Coindesk: https://www.coindesk.com/tips-keep-bitcoins-secure/

Grossmann, F., Henze, M., Klaus, W., Matzutt, R., & Ziegeldorf, J. (2018). Secure and anonymous decentralized Bitcoin mixing. *Future Generation Computer Systems*, 448-466. Retrieved from https://doi.org/10.1016/j.future.2016.05.018

Harper, C. (2018, March 2). *This Week in Cryptocurrency–March 2nd, 2018*. Retrieved from Coincentral: https://coincentral.com/this-week-in-cryptocurrency-march-2nd-2018/

Heath, T. (2017). *Bitcoin is going mainstream. Here is what you should know about it.* Retrieved from The Washington Post: https://www.washingtonpost.com/news/get-there/wp/2017/12/04/bitcoin-is-going-mainstream-here-is-what-you-should-know-about-it/?utm_term=.f05378c5d79c

Hickey, S. (2017, October 1). *Will bitcoin ever be a safe investment or always a gamble?* . Retrieved from The Guardian: https://www.theguardian.com/money/2017/oct/01/will-bitcoin-ever-be-safe-investment-gamble

Ivanecky, E. (2018, January 5). *Bitcoin cryptocurrency is not as secure as it seems*. Retrieved from Study Breaks: https://studybreaks.com/culture/bitcoin-cryptocurrency-not-secure/

Iwamura, M., Kitamura, Y., & Matsumoto, T. (2014a). Is Bitcoin the only cryptocurrency in the town? *Institute of Economic Research*(602), 1-15. Retrieved from https://ssrn.com/abstract=2405790 or http://dx.doi.org/10.2139/ssrn.2405790

Iwamura, M., Kitamura, Y., Matsumoto, T., & Saito, K. (2014b). Can we stabilize the price of a cryptocurrency?: Understanding the design of Bitcoin and Its potential to compete with central bank money. *Institute of Economic Research*(617), 1-40. Retrieved from http://dx.doi.org/10.2139/ssrn.2519367

Jordan, G., Levchenko, K., McCoy, D., Meiklejohn, S., Pomarole, M., Savage, S., & Voekler, G. (2013, Oct 23-25). A fistful of Bitcoins: Characterizing payments among men with no names. *IMC '13*. doi:http://dx.doi.org/10.1145/2504730.2504747.

Katsiampa, P. (2017). Volatility estimation for Bitcoin: A comparison of GARCH models. *Economics Letters, 158*, 3-6. Retrieved from https://doi.org/10.1016/j.econlet.2017.06.023

Kelly, J. (2017, Nov 30). *10 bitcoin facts you might not know as the bubbly cryptocurrency gets volatile*. Retrieved from Financial Review: http://www.afr.com/markets/currencies/10-bitcoin-facts-you-might-not-know-as-the-bubbly-cryptocurrency-gets-volatile-20171129-gzvkhl

Kharif, O. (2017, December 8). *The Bitcoin whales: 1,000 people who own 40 percent of the market*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market

Kharpal, A. (2018, January 18). *Blockchain cryptocurrency wallet launches bitcoin buy and sell in the US*. Retrieved from CNBC: https://www.cnbc.com/2018/01/18/blockchain-wallet-launches-bitcoin-buy-and-sell-in-the-us.html

Kim, T. (2017, Sept 7). *Bitcoin up sevenfold since Warren Buffett warned digital currency was a 'mirage'*. Retrieved from CNBC: https://www.cnbc.com/2017/09/07/bitcoin-up-sevenfold-since-warren-buffett-warned-digital-currency-was-a-mirage.html

Koshy, D., Koshy, P., & McDaniel, P. (2014). *An Analysis of Anonymity in Bitcoin Using P2P.* University Park: Pennsylvania State University. Retrieved from https://pdfs.semanticscholar.org/c277/62257f068fdbb2ad34e8f787d8af13fac7d1.pdf

Kshetri, N. (2017, November). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027-1038. Retrieved from https://doi.org/10.1016/j.telpol.2017.09.003

Liedtka, D., & Schatzker, E. (2017). *Bitcoin lost almost 20% of its value this week*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2017-12-22/bitcoin-plummets-toward-13-000-down-more-than-30-from-record

Lopp, J. (2016, November 13). *Bitcoin's security model: A deep dive*. Retrieved from Coindesk: https://www.coindesk.com/bitcoins-security-model-deep-dive/

M., C. (2017). *14 interesting facts about Bitcoin*. Retrieved from DarkWebNews: https://darkwebnews.com/bitcoin/14-interesting-facts-bitcoin/

Malanov, A. (2017, November 3). *Problems and risks of cryptocurrencies*. Retrieved from Kaspersky Lab: https://www.kaspersky.com/blog/cryptocurrencies-intended-risks/20034/

Martins, S., & Yang, Y. (2011). Introduction to Bitcoins: A pseudo-anonymous electronic currency system. *Conference of the Center for Advanced Studies on Collaborative Research*, (pp. 349-350). Toronto, Ontario, Canada. Retrieved from https://dl.acm.org/citation.cfm?id=2093944&dl=ACM&coll=DL

Merkle. (2017, December 22). *Bitcoin Is probably less secure than you thought*. Retrieved from Merkle: https://themerkle.com/poor-bitcoin-security/

Miller, P. (2015). The cryptocurrency enigma. In J. Sammons, *Digital Forensics* (pp. 1-25). Elsevier. Retrieved from https://doi.org/10.1016/B978-0-12-804526-8.00010-1

Moore, T., Thornton, M., & Vasek, M. (2014). *Empirical Analysis of Denial-of-Service Attacks.* Dallas: Southern Methodist University. Retrieved from http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_17.pdf

Moorley, J. (2015, May 1). Debate on autonomous weapons resumes. *Arms Control Today, 45*(4), p. 5.

Morris, D. (2017, December 20). *Bitcoin is not a systemic financial risk, say top economists*. Retrieved from Fortune: http://fortune.com/2017/12/20/bitcoin-systemic-financial-risk/

Morris, D. (2017). *Head of bankrupt Bitcoin exchange could make hundreds of millions from failure*. Retrieved from Fortune: http://fortune.com/2017/11/11/karpeles-mt-gox-profitable-bankruptcy/

Mulqueen, T. (2018, Feb 23). *Forbes*. Retrieved from Now accepting Bitcoin: a retailer's guide to digital currencies: https://www.forbes.com/sites/tinamulqueen/2018/02/23/now-accepting-bitcoin-a-retailers-guide-to-digital-currencies/#354643c11ed4

Nakamoto, S. (2008). Bitcoin: A Peer-to-peer electronic cash system. *Bitcoin.org*. Retrieved from https://bitcoin.org/bitcoin.pdf

Newman, L. (2017, November 5). *How to keep your Bitcoin safe and secure*. Retrieved from Wired: https://www.wired.com/story/how-to-keep-bitcoin-safe-and-secure/

Nova, A. (2017a, September 24). *Bitcoin is too risky to treat as a 'serious' investment, financial advisers say*. Retrieved from CNBC: https://www.cnbc.com/2017/09/22/why-digital-currencies-are-a-dicey-bet-for-your-retirement-savings.html

Nova, A. (2017b, November 29). *Bitcoin, once 'sketchy,' becomes more mainstream* . Retrieved from CNBC: https://www.cnbc.com/2017/11/28/bitcoin-once-sketchy-becomes-more-mainstream.html

Nova, A. (2018). *How to stop your digital fortune from going up in smoke*. Retrieved from CNBC: https://www.cnbc.com/2018/01/26/security-issues-reach-a-peak-within-cryptocurrencies-.html

O'Malley, N., & Presthus, W. (2017). Motivations and barriers for end-user adoption of Bitcoin as digital currency. *Procedia Computer Science, 121*, 89-97. Retrieved from https://doi.org/10.1016/j.procs.2017.11.013

Prpic, J. (2017). Unpacking Blockchains. *Collective Intelligence 2017*, (pp. 1-7). NYU Tandon School of Engineering.

Reuters. (2016, August 29). *Risk of Bitcoin hacks and losses is very real*. Retrieved from Fortune: http://fortune.com/2016/08/29/risk-of-bitcoin-hacking-is-real/

Roberts, J. (2017). *Fortune*. Retrieved from How Bitcoin is stolen: 5 common threats: http://fortune.com/2017/12/08/bitcoin-theft/

Rosenberg, S. (2017, December 16). *2018: The year of the cryptocurrency craze* . Retrieved from Wired: https://www.wired.com/story/future-of-bitcoin-blockchain-2018/

Sabin, D. (2018, January 3). *Everything you need to know about cryptocurrency and why it's the future of money*. Retrieved from Futurism: https://futurism.com/cryptocurrency-future-money-bitcoin/

Scheuermann, B., & Tschorsch, F. (2016, March 2). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials, 18*(3), 2084-2123. Retrieved from https://eprint.iacr.org/2015/464.pdf

Shin, L. (2016, December 20). *Hackers have stolen millions of dollars In Bitcoin -- using only phone numbers*. Retrieved from Forbes: https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#7a69a48d38ba

Singletary, M. (2018, January 23). *Bitcoin is all the rage — but is it worth the risk?* Retrieved from The Washington Post: https://www.washingtonpost.com/news/get-there/wp/2018/01/23/bitcoin-is-all-the-rage-but-is-it-worth-the-risk/?utm_term=.9076d78d3c38

Steadman, I. (2013). *There's a 60m pound Bitcoin heist going down right now, and you can watch in real-time*. Retrieved from NewStatesman: https://www.newstatesman.com/future-proof/2013/12/theres-%C2%A360m-bitcoin-heist-going-down-right-now-and-you-can-watch-real-time

Thompson, D. (2017, November 30). *Bitcoin Is a delusion that could conquer the world*. Retrieved from The Atlantic: https://www.theatlantic.com/business/archive/2017/11/bitcoin-delusion-conquer-world/547187/

Thomson Reuters. (2018). *Securities vs. commodities*. Retrieved from FindLaw: http://consumer.findlaw.com/securities-law/securities-vs-commodities.html

Tillier, M. (2018, Jan 25). *What Is A cryptocurrency?* Retrieved from Nasdaq: https://www.nasdaq.com/article/what-is-a-cryptocurrency-cm910816

Trend Micro. (2017, December 7). *NiceHash marketplace hacked, loses $64 million in Bitcoins*. Retrieved from Trend Micro: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/nicehash-marketplace-hacked-loses-64-million-in-bitcoins

U.S. Commodity Futures Trading Commission. (2017, December). Customer advisory: Understand the risks of virtual currency trading. Retrieved from http://www.cftc.gov/idc/groups/public/@customerprotection/documents/file/customeradvisory_urvct121517.pdf

U.S. Commodity Futures Trading Commission. (2018, February 15). *CFTC warns customers to avoid pump-and-dump schemes*. Retrieved from CFTC Issues First Pump-and-Dump Virtual Currency Customer Protection Advisory: http://www.cftc.gov/PressRoom/PressReleases/pr7697-18

Villas-Boas, A. (2018, February 20). *Scammers are tricking people to log into fake cryptocurrency exchange sites, and they're incredibly hard to spot*. Retrieved from Business Insider: http://www.businessinsider.com/scammers-spoofing-cryptocurrency-exchange-site-urls-incredibly-hard-to-spot-2018-2

Williams, M. (2014). Virtual currencies-Bitcoin risk. *World Bank Conference.* Washington, D.C. Retrieved from https://www.bu.edu/susilo/files/2014/10/Wlliams-World-Bank-10-21-2014.pdf

Yermack, D. (2013). Is Bitcoin a real currency? *The Handbook of Digital Currency*, 31-44. doi:10.3386/w19747