2014

Bitcoin: Is Cryptocurrency Viable?

Austin Hill
Claremont McKenna College

CLAREMONT MCKENNA COLLEGE

Bitcoin: Is Cryptocurrency Viable?

SUBMITTED TO

PROFESSOR DOUGLAS MCEACHERN

AND

DEAN NICHOLAS WARNER

BY

Austin Hill

for

SENIOR THESIS

Spring 2014

April 25, 2014

Table of Contents

Introduction

Bitcoin is a controversial new medium of monetary exchange, having been in existence only since 2009. Bitcoins are solely virtual; that is, existing only as digital information on an owner's hard drive. In the years since 2009, the public has been slow to accept bitcoins as an alternative to fiat currencies (those the government has given legal tender status), but in December 2013, the major retailer Overstock.com announced they would start accepting bitcoins as payment for goods. In addition, Virgin Galactic, the dating website OKCupid, and a Tesla dealership in California have begun accepting bitcoins as a legitimate form of payment, as well as numerous (and growing) numbers of coffee shops, yoga studios, tattoo parlors, bed and breakfasts, art galleries, bars, online vendors, and other small businesses[1].

The controversy surrounding bitcoin centers around whether it is merely a fad-driven investment or in fact a currency with the potential to rival the dollar. This thesis will examine bitcoin—its origins, its nature, its function, and its technology—and analyze whether those attributes meet the requirements necessary to function as a comparable medium of exchange to the dollar.

Chapter 1: Introduction to Cryptocurrency

The concept of a cryptocurrency—one whose creation and transaction is regulated by cryptography instead of a central authority—was first proposed by a computer programmer named Wei Dai in 1998, when he discussed the idea in chat forums on the burgeoning internet. The creator of bitcoin, known only by the pseudonym Satoshi Nakamoto, first implemented this

[1] Chowdhry, Amit. "Overstock.com Is Going To Accept Bitcoin In 2014." Forbes. http://www.forbes.com/sites/amitchowdhry/2013/12/21/overstock-com-is-going-to-accept-bitcoin-in-2014/ (accessed April 3, 2014). (Chowdhry 2013)

concept in 2009 by inventing a medium of exchange completely unregulated except by code. The code governing the bitcoin network is entirely open source[2]. In other words, anyone can access and edit the code on the internet, making the network a product of collaboration among millions of coders whose collective efforts protect the technology's integrity. This open-source nature ensures that the currency's objectivity and transparency remains intact, and anyone with the curiosity to know and coding background to understand can see first-hand exactly how the cryptography works.

Nakamoto designed the open-source code to constantly introduce a steady supply of bitcoins into the market. Coders called "miners" add new bitcoins to the market by using special software to scour the internet, looking for bitcoin transactions between peers that need verification before bitcoins can move from one account to the other. This verification process involves solving complex mathematical problems that require high levels of processing power. Once the verification process completes, the miner collects a transaction fee of 25 bitcoins. The frequency of verifications adds new coins to the market roughly every 10 minutes. By design, the verification process gets progressively more complex as more people inevitably decide to try their hands at mining and invest in more powerful processors designed specifically to solve mining problems[3]. In theory, as the number and sophistication of miners increases, the flow of bitcoins into the market can remain steady due to an increasing problem difficulty and a decreasing number of bitcoins awarded as transaction fees. A constant flow avoids exorbitant inflation that might otherwise occur with increasing demand and limited supply. However, once all 21 million bitcoins in existence are mined, the flow of coins into the market will cease, an

[2] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.com. (Nakamoto 2009)(accessed March 10, 2014).

[33] "Frequently Asked Questions." FAQ. (Bitcoin.org 2009) (Hochstein 2014)(accessed March 14, 2014).

event that is projected to occur around 2140 if the current rate of bitcoin mining continues. To provide a certain amount of elasticity in the market supply of bitcoins, each coin can be subdivided down to eight decimal places[4]. This ensures that as demand for bitcoins increases, the technology will have the means to support a large user base.

A defining aspect of the mining and transacting process of the bitcoin network is a perpetual ledger of all transactions that have taken place since bitcoin's inception, called a "blockchain." Each time a miner verifies a transaction, a record of the transaction is added to the blockchain, verifying that the bitcoins involved are not predisposed in a previous transaction. Miners essentially race to be the first to verify a block of transactions and add them to the blockchain, earning the bitcoin reward[5]. This element of competition in the verification process guarantees that countless miners look at each transaction, thus verifying beyond a doubt that the bitcoins come from an existent source and transfer to their designated destination. This peer-reviewed system means that no one can buy goods with bitcoins that are not rightfully theirs and sitting in their wallet. Further, the decentralized nature of the bitcoin system mitigates the risk of attack on the network itself because it is dispersed on each computer that participates in mining. As put by Andreas M. Antonopoulos, a technology entrepreneur in the San Francisco Bay Area and one of bitcoin's most outspoken supporters, "Bitcoin having no center means there's no target to attack, there's no concentration of power. Power is diffuse and distributed among the entire community."[6] Thousands of computers worldwide work together to update and maintain the blockchain, ensuring the accuracy and validity of each and every bitcoin transaction. Therefore, the integrity of bitcoin's operation will always remain intact.

[4] Nakamoto, "Bitcoin"
[5] "Frequently Asked Questions," Bitcoin
[6] Hochstein, Marc. "Why Bitcoin Matters to Bankers." American Banker, March 14, 2014, 1A edition.

The transactions reviewed by miners on the bitcoin network transfer directly from the consumer to the seller with no middlemen, essentially transposing a cash transaction to the internet[7]. Users are afforded complete anonymity by this mechanism and any third-party facilitators such as banks or credit companies become completely unnecessary. However, this creates risk because users must accept the responsibility of keeping their bitcoin stashes in virtual wallets on a secure hard drive. Hackers can access a user's wallet if the computer housing it has an internet connection, so users must take great care with internet security. The lack of a central authority makes users more liable for protecting their own assets.

The vulnerability inherent in a decentralized system creates difficulty for bitcoin reaching a larger user base. In order to become a lasting, respected and widely-used form of currency, bitcoin will undoubtedly need the endorsement of the United States government, in the form of legal tender status. Risk aversion will prevent most people from investing their hard-earned dollars in a currency system that works outside the bounds of the law and has no government guarantee to create inherent value. Unless the government provides a guarantee of value, such as the legal tender status that gives the dollar value, bitcoin will forever be viewed as an investment opportunity similar to a stock, whose price rises and falls daily. However, even if no virtual currency manages to become a mainstream method of payment, the technology of bitcoin and its peers provides a faster, more secure, and cheaper method of transacting, some aspects of which could prove beneficial for governments and fiat currencies. Cryptocurrency technology could prove revolutionary in the way monetary systems are operated and transactions occur, should governments decide to embrace the positive contributions the technology has to offer.

[7] Nakamoto, "Bitcoin"

Chapter 2: Propensity for Illegal Activity

Bitcoin's unregulated, virtual, and anonymous nature makes it an ideal medium of exchange for those participating in illegal activities. The identity of the user cannot, in theory, be discovered, mitigating the risk of criminals ever being caught or prosecuted for their transgressions. A relative lack of regulation means illegal bitcoin transactions can occur unfettered by any government agency. And the decentralized nature gives users freedom from banks and the exposure to suspicion and interference that accompanies any government financial institution. The virtual nature minimizes the evidence authorities could gather to incriminate participants in illegal activities; in other words, there are no briefcases of cash hanging around for police to seize. However, with all these seemingly ideal conditions for illegal activity to take place, bitcoins are inherently resistant to concealing illegal activity should anyone care to investigate, a characteristic that governments could harness to minimize the occurrence of financial crimes.

The anonymity afforded to bitcoin users both facilitates transactions and privacy protection, but by the same token makes the currency ideal for carrying out illegal transactions. A large portion of bitcoin's early adopters participated in black markets, buying and selling drugs, weapons, forged documents and other illegal commodities. One of the largest markets to use bitcoin as its mandatory currency was Silk Road, a website that guaranteed anonymity by making itself invisible to everyone except those who knew precisely where to find it in the vastness of the internet. Silk Road served as a middleman, preventing transactions from occurring directly between buyers and sellers, thereby temporarily possessing the bitcoins

exchanged in the transaction[8]. This left customers vulnerable to losing their bitcoins should Silk Road ever fall victim to hackers or be disbanded by the FBI, its ultimate fate. Based out of San Francisco and operated by a 29-year-old physics graduate named Ross Ulbricht, the illegal marketplace was shut down by federal agents in October 2013. The agents seized $3.5 million of Silk Road users' bitcoins in the process and arrested Ulbricht[9].

Since his arrest, Ulbricht has been indicted for one count of narcotics conspiracy, one count of running a criminal enterprise, one count of conspiracy to commit computer hacking and one count of money laundering. He has also been accused of attempting to buy the murders of six people who had the potential to expose the Silk Road operation, all of which the FBI orchestrated and staged. He currently awaits trial in New York State[10]. The anonymity bitcoin offers to users appeals to many like Ulbricht whose goal is to reject authority and government involvement in economics and society. The attractiveness of bitcoin to potential criminals creates a need for the government to step in and regulate the currency in order to prevent illegal activities. Even if it is not the government's place to protect people using a new technology or making financially risky decisions by investing in an untested currency, it is indisputably the government's responsibility to prevent crime and maintain an ordered society. Because bitcoin creates a new avenue for illegal activity, should the government decide to regulate the currency in some form, they are completely within their authority to do so.

Aside from the sale and purchase of illegal goods, bitcoin provides a highly effective and simple method of money laundering. Shortly after the fall of Silk Road, federal agents arrested a

[8] Zetter, Kim. "How the Feds Took Down the Silk Road Drug Wonderland | Threat Level | WIRED." Wired.com. (Zetter 2013)/ (accessed March 17, 2014).
[9] Ibid
[10] Kushner, David. "Dead End on Silk Road: Internet Crime Kingpin Ross Ulbricht's Big Fall." Rolling Stone. (Kushner 2014)(accessed March 21, 2014).

young bitcoin entrepreneur by the name of Charlie Shrem. Shrem was the CEO of BitInstant, a startup designed to exchange customers' cash for bitcoins using third-party retailers such as Walmart or Walgreens. Shrem is accused of using his startup to launder money through Silk Road. He accepted cash from a Silk Road retailer named Robert Faiella, selling him bitcoins in return and laundering the cash through his startup. Shrem was aware of the nefarious intentions of Faiella, but did not report the activity to the Treasury Department, making him a knowing participant in a money-laundering scheme. Shrem is also accused of buying drugs from the marketplace[11]. Bitcoin makes laundering money much simpler because the simple act of exchanging bitcoins for dollars is enough to clean the money of any questionable activity that had taken place in the past. Second, until recently the IRS did not have any requirements for taxing bitcoins, so users did not have to worry about keeping track of their expenditures or revenues from bitcoin transactions and the government had no idea about the number of bitcoins in circulation or their flow around the market. Therefore, it was highly difficult for the government to detect any suspicious activity based on people's tax filings.

Since the downfall of the Silk Road, however, bitcoin has proven inherently ill-suited for use in illegal activities such as money laundering and exchanging illegal goods. Two more illegal exchanges dealing in bitcoins have been shut down since, Sheep Marketplace and an unrelated revival of Silk Road, each losing $6 million and $2.7 million, respectively, of customers' bitcoins in the process[12]. Certain characteristics make bitcoin incompatible with the illegal

[11] Hurtado, Patricia. "Ex-Bitcoin Foundation's Shrem in Plea Talks, U.S. Says." Bloomberg Business Week. http://www.businessweek.com/news/2014-03-31/ (Hurtado 2014)ex-bitcoin-foundation-s-shrem-in-plea-talks-u-dot-s-dot-says-1 (accessed April 14, 2014).
[12] Zetter, "Silk Road"

activities anonymity invites: a long transaction memory, the vulnerability of wallets, and the irreversibility of transactions.

Although anonymity serves as a cornerstone of the bitcoin model, if a user were to ever convert his bitcoins into actual cash from an exchange or newly minted bitcoin ATM, the likes of which are popping up in hip cities such as Austin and Seattle, his name would instantly be linked to those bitcoins[13]. If those same bitcoins had recently been involved in illegal transactions, the person exchanging them for cash would incriminate himself by doing so. Because the bitcoins reside in their owner's wallet, he had to have had knowledge of, and therefore consent for, the illegal activity that generated the bitcoins. There would exist no way for customers of illegal exchanges to ever convert their bitcoins into cash without risking discovery and arrest. This serves as a great deterrent for owning illegally acquired bitcoins, as the limited number of establishments accepting bitcoins make the currency much less desirable than cash. Criminals using bitcoins become limited to transacting only in the bitcoin marketplace, making it a much less appealing option for conducting illegal business.

The infinite memory of the bitcoin blockchain prevents any dispute about the involvement of certain bitcoins in illegal transactions. The discovery of the identity of a person in possession of illegally acquired bitcoins leaves that person vulnerable not only to prosecution for the transaction that drew police attention, but to every single illegal transaction in which they have participated. This means that when prosecutors catch a criminal for an illegal transaction on a site like Silk Road, authorities can prosecute the perpetrator for every transgression that shows up in their bitcoin transaction history. In contrast, illegal cash transactions have no long-term

[13] Gross, Doug. "Bitcoin ATMs coming to the U.S.." CNN. http://www.cnn.com/2014/02/18/tech/innovation/bitcoin-atms/ (accessed March 18, 2014).

memory, so prosecutors can only charge criminals for the transaction that warranted their arrest instead of every single illegal transaction in which they have participated. An indisputable transaction memory makes bitcoin a much riskier currency choice for illegal activity, making its users vulnerable to their wallets' entire histories of illegal activity.

Further, bitcoin transactions are irreversible. Once the bitcoins have participated in illegal transactions, it is impossible to erase those transactions from the blockchain memory. Therefore, each and every bitcoin ever used on sites such as Silk Road carries code that can trace it back to the wallet in which the coin was housed when the illegal activity took place[14]. Additionally, should the middleman site choose to abandon operations and flee with the bitcoins currently under their ownership, there would be no preventing them from doing so. Once the bitcoins are transferred to the websites' wallets, no one, including legal authorities, can reverse the transaction and recover the money. Users of virtual black markets take a huge risk when handing their bitcoins over to the facilitators. Because of the illegality of the base operation and the unregulated nature of bitcoin, no authority exists that would help victims to recover any stolen money. The irreversibility of the transactions makes this a moot point anyway, since there is no way to return the bitcoins to the original owner unless a new transaction were to take place, a voluntary action a criminal most likely would not be willing to take.

These characteristics of bitcoins make them an ideal medium for exposing illegal transfers of cash and catching the perpetrator; a fact demonstrated by the seemingly inevitable self-destruction of every major illegal bitcoin exchange that has cropped up on the internet: Silk Road, Sheep Marketplace, and the Silk Road revival. The long, permanent memory of bitcoin

[14] Hochstein, "Why Bankers Should Care"

could be put to great use by the federal government in preventing crime and theft should they ever decide to embrace a virtual currency system in the future.

Chapter 3: Wallet Vulnerability

The existence of bitcoins solely on a user's hard drive creates a vulnerability to untraceable hacking and irrecoverable theft, as both the owner and thief are anonymous users. Once these bitcoins are gone, recovery is not an option; investors simply lose their money. The inability to recover stolen bitcoins or even to discover the identity of the thief makes bitcoin wallets easy targets for anyone with hacking skills and a desire to steal.

The wallets used to maintain an owner's bitcoins risk exposure to hackers. Theft is avoidable should the owner take proper precaution in securing his wallet on a stable hard drive that does not connect to the internet. However, when participating in illegal exchanges on the internet, a customer must expose his wallet to vulnerable internet connections in order to transfer bitcoins. Hackers will target illegal exchanges because no authority exists to recover money for a person who has bought illicit goods on the internet. Therefore, a greater risk of theft exists with the use of bitcoins on illegal exchanges as opposed to regular cash. Since the currency's inception, bitcoin business ventures have suffered a disproportionate number of devastating thefts.

In June 2011, the first known substantial hack into a bitcoin account was carried out at the expense of one "Allinvain," a username on a bitcoin forum. The loss amounted to 25,000 bitcoins, or $15.3 million in today's bitcoin market. On March 4, 2014 the bitcoin bank Flexcoin, based in Alberta, Canada had over $600,000 worth of bitcoins stolen from its servers, forcing it to close. Bitcoin exchanges provide an easy target for hackers. Numerous exchanges, Bitcoinica,

Bitfloor, Canadian Bitcoins, and Bitcurex all lost sizeable portions of their bitcoin holdings due to hacks or simple errors in coding[15]. The most infamous collapse of an exchange took place in Japan in February 2014 when the world's largest bitcoin exchange, Mt. Gox was forced to declare bankruptcy.

Due to a poorly monitored programming operation, Mt. Gox left itself vulnerable to hackers. Unlike other bitcoin exchanges, Mt. Gox failed to use a control software that would prevent programmers from accidentally deleting or writing over a colleague's work. Implementing a change as simple as new software would have ensured the reliability and effectiveness of the Mt. Gox code to protect their assets. Further, they failed to use a test environment to assess the code and instead put it into immediate use, deferring the risks of any bugs or holes in code onto the customer. As one insider put it "the source code was a mess."[16]

The exchange had already been hacked once, losing the equivalent of $8.7 million in June 2011. But, by 2014, the exchange had grown to one of the biggest in the world and hackers were able to extract over $460 million from the company. This huge loss forced the exchange into bankruptcy and robbed countless bitcoin holders of their money. Mt. Gox is currently in the midst of a "civil rehabilitation process" that may allow the Tokyo-based company to eventually rebuild and pay back some of the customers whose money hackers stole in the attack.[17]

Countless third-party bitcoin-wallet providers have been hacked over the past few years including BIPS and inputs.io, who each lost around $1 million worth of bitcoin at the time.[18]

---

[15] Hern, Alex. "A history of Bitcoin hacks." theguardian.com. http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency (accessed March 20, 2014).
[16] McMillan, Robert. "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster | Enterprise | WIRED." Wired.com. http://www.wired.com/2014/03/bitcoin-exchange/ (accessed March 25, 2014).
[17] Ibid
[18] Hern, "A history of Bitcoin hacks"

Wallet providers have proven the most vulnerable to hacker attacks. Very low barriers to entry allow almost anyone to join the burgeoning field. Programming skills, a knowledge of bitcoin, and time serve as the only prerequisites to entering the wallet-provider market. The costs are minimal and the technology is relatively straightforward. Because of the ease with which start-ups can enter the industry, an abundance of small, untested wallet providers have appeared on the internet, from which hackers can extract bitcoins without fear of consequence.

Two researchers have recently discovered the existence of over 140 types of malware programs on the internet designed specifically to infiltrate bitcoin wallets and steal the contents. The most common program searches for a wallet on users' hard drives, gathers information about their wallets, and uses it to gain the users' personalized access keys. The newness of the malware associated with bitcoin theft has taken traditional security software by surprise, with only 50% of security systems detecting and stopping the malware.[19]

After the downfall of so many exchanges and in view of the clear vulnerability of virtual wallets, proponents of bitcoin have begun to realize the need for a better wallet storage system. Bitcoin's fundamental virtual nature means online wallets are the only place bitcoins can be stored, and because of the necessity of internet connectivity for transfer, they are frequently exposed to potential hackers. This vulnerability poses a potential problem for the spread of virtual currency, as users will have to learn how to protect their assets properly, a learning curve that no longer applies to cash because of the existence of banks, the Federal Reserve, and regulatory legislation. Before bitcoin can become widely used, a more secure method of storing wallets must become available. Many startups have materialized with various solutions to this

[19] Greenberg, Andy. "Nearly 150 Breeds Of Bitcoin-Stealing Malware In The Wild, Researchers Say." Forbes. http://www.forbes.com/sites/andygreenberg/2014/02/26/nearly-150-breeds-of-bitcoin-stealing-malware-in-the-wild-researchers-say/ (accessed April 2, 2014).

vulnerability issue. Out of the Czech Republic, the Trezor wallet features a hard drive immune to malware that allows users to better "cold store" their bitcoins, the tactic of storing the wallet key on a hard drive not connected to the internet. A second startup, Xapo takes on any liability of theft by insuring customers' bitcoin against hacking, theft by an employee, or any other loss that may occur while in Xapo's possession.[20]

Efforts such as these may not only give users something like the level of security provided by federal banks, but may also eliminate the need for them to invest time learning how to store their wallets properly in order to avoid theft. Even if people store their bitcoins safely by keeping all bitcoins on a hard drive not connected to the internet, there exists the additional risk of the hard drive getting stolen or lost, taking the entire bitcoin fortune with it. The hard drive of bitcoins is akin to stuffing cash into a mattress, and when faced with that choice, the vast majority of people would rather keep their wealth safe in a bank. People's inherent laziness may prevent them from investing effort in learning how to protect their assets, but at the same time they want the peace of mind that accompanies a secure savings account. The virtual equivalent of a bank must be developed to provide users with the same security and peace of mind provided by brick and mortar banks.

Chapter 4: The Gold Standard

Bitcoin will never replace cash as a monetary unit in the United States because the government has grown too large to return to a commodity-based system like the gold standard, which bitcoin, with its limited supply, essentially replicates. Throughout the past two centuries of

[20] Perlroth, Nicole. "To Instill Love of Bitcoin, Backers Work to Make It Safe." NYTimes. http://dealbook.nytimes.com/2014/04/01/to-instill-love-of-bitcoin-backers-work-to-make-it-safe/?_php=true&_type=blogs&_r=0 (accessed April 10, 2014).

monetary history, periodic deviations from the gold standard have arisen when governments faced the need to spend more money than they possessed in gold, an issue that frequently occurred during wartime. Printing more money provided an obvious solution to this conundrum. After World War I, the gold standard largely collapsed on a worldwide scale[21]. During the war, countries around the world had stopped allowing conversion from cash into gold, and instead printed more money. This caused prices to rise. After the war ended, some countries, most notably the United Kingdom, chose to return to pre-war rates of gold convertibility. Because prices had risen, gold should have been worth more currency than it had been before the war. Yet the conversion rate between gold and national currencies had not changed. Therefore, when people went to the bank to exchange their cash for gold, they were getting much more gold than they would have prewar for the same amount of cash. This created a worldwide undervaluation of gold reserves. Changes in the flows and amount of cash were not offset by an adjustment in the exchange rate of gold[22]. Therefore, many countries were already operating on a pseudo-cash-based economy.

In the United States, the government has often strayed from the gold standard. The first metallic standard was established under the influence of Alexander Hamilton in 1792, using both gold and silver as a basis for monetary value. The problem with the dual basis was that whenever international exchange rates rose on one metal, that metal would sell internationally where it could produce a larger return. This resulted in either silver or gold becoming scarce in the United States and the other metal serving as the remaining basis. From 1792 to 1834, silver dominated. Then the value ratio of silver to gold was changed from 15 to 1 to 16 to 1 by Congress to stop

[21] Elwell, Craig. "Brief History of the Gold Standard in the United States." Congressional Reports, June 23, 2011, www.crs.gov (accessed March 6, 2014).
[22] Ibid

people from selling their gold abroad. Because silver was now worth more on the international market, a swing in the opposite direction occurred and the United States ended up back on a gold standard.[23]

The gold standard survived unfettered until the Civil War. During the war, the U.S. government needed more money to finance the war. There was not enough gold in the reserves, so the banks halted the conversion of gold to cash and the government began issuing paper currency not convertible into either gold or silver. These bills, known as "greenbacks" were the first nonconvertible currency used in the United States.[24]

In 1900, the U.S. government passed an act that declared gold the official standard of the United States monetary system. Greenbacks and all other forms of currency were redeemable in gold coin. A new form of currency was also becoming popular, the check. However, a problem arose because the use of checking accounts created periodic bank runs where masses of people would withdraw all the money from their accounts for fear of the bank not having enough cash on hand to pay off everyone. To address this problem, the U.S. government created the Federal Reserve. The Fed served to lend money to banks that could not meet their customers' demand for cash. This prevented the bank runs that could cripple a bank's operations.[25] The Federal Reserve did not affect the gold standard, but did allow banks to function more efficiently under it.

During the Great Depression, the collapse of the economy and the panic that followed led to massive bank runs by the American public and the failure of countless banks. The gold

[23] Bordo, Michael D. "The Gold Standard, Bretton Woods, and Other Monetary Regimes: A Historical Appraisal." *Review - Federal Reserve Bank of St.Louis* 75, no. 2 (Mar, 1993): 123. http://search.proquest.com/docview/227744939?accountid=10141.
[24] Elwell, "Gold Standard"
[25] Bordo, "The Gold Standard"

standard was part of the problem because the Fed would have had to print money while lowering interest rates in order to meet public demand for cash. Lowering interest rates, however, would incentivize people to sell gold abroad where the interest rates were higher, subsequently reducing the supply of gold in the United States and the value of each dollar in circulation. To stay on the standard would mean contracting the money supply to maintain the value of each dollar. This was not an option by 1933 when Franklin Roosevelt stepped into the Presidential Office. America was in a horrible state of poverty and could not afford to remain on the gold standard any longer.[26]

After taking office, Roosevelt took America off the gold standard. Banks were closed and private ownership of gold was made illegal. Under the Gold Reserve Act of 1934, all gold in circulation was removed and put into the National Treasury and the dollar was reduced to 60% of its original value. The United States monetary system was now based on a quasi-gold standard. The dollar was still defined in terms of gold, but the only remaining use for gold was in international transactions. However, the world's economies were attempting to protect themselves from the effects of the Great Depression by insulating themselves and limiting international trade.[27]

In order to counteract the insular trade policies of the 1930s, 45 countries met in Bretton Woods, New Hampshire and came to an agreement. They established the International Monetary Fund in order to oversee a new system of international valuation. The dollar would serve as the basis for exchange rates that would remain constant except to correct for a "fundamental

[26] Ibid
[27] Ibid

disequilibrium" in the rates and could only be changed with permission from the IMF. The dollar's value would continue to be based on gold, set at a price of $35 an ounce.[28]

During the late 1960s, a surplus of U.S. dollars was created by foreign investment and military spending on the Vietnam War. The dollar was now worth less than the $35 per ounce of gold exchange rate. This posed a problem with foreign trade, because no other countries wanted dollars. To address this issue, President Nixon suspended the dollar's convertibility into gold in 1971. This abandonment led to the floating exchange rate policy used today in which countries can choose to have their currency float against another countries, adopt an existing form of currency, or join a monetary union.[29]

The history of the gold standard serves to demonstrate that bitcoin will never replace the dollar as a national currency. Assuming miners continue mining bitcoins, the number of coins in the market will eventually be capped at 21 million, an event predicted to occur in 2140.[30] This means that bitcoin is a finite commodity, designed by its creator to mimic a gold supply. Therefore, widespread adoption would lead to a monetary system similar to the gold standard. The same problems that arose with the gold standard would arise in a bitcoin-based system. Sooner or later the government would need to spend more bitcoins than it possessed and would have to deviate from the bitcoin standard. Any rise or fall in international bitcoin interest rates would lead to a mass exodus or influx of bitcoins into the American market, causing the price to rise or fall accordingly, disrupting the currency as a store of value. Deflation would pose a constant risk because of the limited money supply. People might begin to hoard bitcoins to avoid inflation, as they did with gold, and stop spending, leading to a stagnant economy and deflation.

[28] Bordo, "The Gold Standard"
[29] Ibid
[30] Nakamoto, "Bitcoin"

Further, when the United States ascribed to the gold standard in the past, the government comprised only 10 percent of GDP. Today the U.S. government constitutes 40 percent of GDP.[31] The growth of the government has been financed by the indiscriminate issuance of cash. This growth could not be sustained in a commodity-based system. A return to any kind of standard would require a contraction of the government and a massive reduction in government spending. Any move by the government toward a commodity-based standard, be it bitcoin or gold, is highly unlikely. The government has become much too large and far-reaching to consider downsizing. Therefore, the bitcoin will not be adopted as a replacement for the government-controlled dollar.

The gradual international abandonment of the gold standard was the first step toward a virtual monetary system. The dollar and all other fiat currency have no inherent value except the guarantee of a government that the value of those slips of paper will be recognized by law. Gold, at least, has always held some inherent value to humans as a precious metal, and has practical purposes as jewelry or in medical devices. The Federal Reserve and similar international entities exist to protect the value of fiat currencies by issuing money to satisfy public demand for cash, keeping values as stable as possible. The inherent uselessness of fiat currencies make them equally illusory as virtual currencies, the majority of people and the government have simply agreed to ascribe value to them. Illusory currencies, such as dollars or bitcoins, exist solely to allow the government to manipulate the money supply in an attempt to prevent unpredictable economic fluctuations, an ability commodity-based systems prevent. Therefore, a virtual

[31] "Historical Tables." Office of Management and Budget. http://www.whitehouse.gov/omb/budget/historicals (accessed March 28, 2014).

currency without any government guarantees, such as bitcoin, does not serve a definite purpose other than an experimental rebellion against government financial institutions.

Chapter 5: History of Digital Currency

Bitcoin is not the first nor the only virtual currency to gain traction with a group of followers. In 1999, an oncologist named Douglas Jackson founded a new form of currency called E-gold. The gold-backed digital currency was an attempt to rival unsatisfactory fiat currencies. Eventually, the company acquired over four million accounts totaling $60 million and backed by four tons of gold. However, despite the popularity and good intentions of the E-gold model, the dominant use of the currency became illegal activities such as drug dealing and hacking. After the FBI and Internal Revenue Service raided Jackson's office in 2005, E-gold shut down. The founder spent three years on probation after pleading guilty to charges of owning an unlicensed business for transmitting money and assisting in money laundering. For the past nine years he has tirelessly tracked down former customers to return their investments.[32] Those who invested in E-gold got lucky because the price of gold has since increased and they are getting back much more than their initial investments.

Unlike contemporary virtual currencies, E-gold derived its value from actual gold. Investors at least had the comforting knowledge that their money would retain some of its value as long as the precious metal had value, no matter what difficulties the currency might undergo. Systems such as bitcoin cannot offer the same guarantee to their customers. Should bitcoin collapse, investors will likely not recover any of their money. This has recently been demonstrated by the collapse of the Mt. Gox exchange, in which $460 million was lost, never to

[32] Foley, Stephen. "Bitcoin needs to learn from past e-currency failures." The Financial Times, November 28, 2013, http://www.ft.com/cms/s/2/6d51117e-5806-11e3-a2ed-00144feabdc0.html

be seen again by the people who invested their money with Mt. Gox. The lack of a reliable return on investment for money invested in bitcoin could pose a serious problem for the currency gaining any widespread use with everyday users. The risk associated with a currency backed by nothing will not appeal to a large enough portion of the population to make bitcoin a widely used currency. Although fiat currencies do not have any inherent value or commodity backing, they do carry the guarantee of the government. The promise of the any government to recognize and protect the value of their chosen currency makes it as secure a store of value as possible. Bitcoin lacks even the slightest guarantee of value, creating too much risk to appeal to a large audience.

Aside from lacking any sort of guarantee of value for customers, today's virtual currencies lack a central controlling agency. E-gold was managed and supported by a central company.[33] A governing body comes with advantages and disadvantages. If hacking incidents or valuation issues arise, users of the currency can turn to a central authority to remedy the issue or take responsibility for losing customers' money. This fosters a feeling of trust and security that bitcoin and other peer-to-peer based currencies cannot offer. But, along with customers having the option to turn to a central authority for help, regulatory agencies and law enforcement also have an entity to target should any illegal activity take place. Bitcoin will never face punishment for the illegal activities it enables because there is no one to blame but an amorphous network of miners. A self-sustaining nature makes bitcoin invulnerable to law enforcement.

The anonymous nature of bitcoin, although a large draw to proponents of the currency, could prove a liability, much in the same way E-gold collapsed after becoming too involved in illegal activities. E-gold allowed users to sign up for their services without checking their

[33] Foley, "Bitcoin needs to learn"

identities. As Jackson observes, "[E-gold] had things backwards. Permissions would be restricted or revoked reactively in the event unusual activity was detected. It was great at finding bad guys after they did something."[34] Bitcoin, with its emphasis on anonymity, invites the same kind of illegal activities as E-gold. In addition to providing an ideal method of transacting for illegal marketplaces, such as the Silk Road, the currency creates an unregulated environment for laundering illegally acquired cash. Once launderers convert illegally acquired cash to bitcoins, their identity becomes protected by the currency's anonymity and authorities cannot continue to track their activity. The perpetrator can then simply exchange their bitcoins for clean cash. Ease of laundering with bitcoins has created a major concern for the Japanese government, as they currently debate regulation of the currency but hesitate because of the illegal activity associated with it.[35] The United States Treasury has warned companies dealing or exchanging bitcoins to take care in knowing their customers and their business dealings.[36] The exchanges must protect themselves because their customers can easily use bitcoins for illegal activities, and since bitcoin does not have a governing body, the exchanges will be the only organizations left to hold liable for any losses or illegal activity that may occur. Should the exchange go bankrupt, customers will not recover any of their investments, as in the case of Mt. Gox. Legal recourse does not exist for victims of bitcoin fraud or theft because the currency operates outside the umbrella of the U.S. government.

[34] Foley, "Bitcoin needs to learn"
[35] Yui, Monami . "Japan Says Bitcoin Not Currency Amid Calls for Regulation." Bloomberg.com. http://www.bloomberg.com/news/2014-03-07/japan-says-bitcoin-is-not-a-currency-amid-calls-for-regulation.html (accessed March 27, 2014).
[36] Casey, Michael. "Treasury's Cohen Warns Unregistered Bitcoin Exchanges ." The Wall Street Journal. http://online.wsj.com/news/articles/SB10001424052702303563304579447020246651110 (accessed March 23, 2014).

Chapter 6: Bitcoin Competitors

Several other comparable virtual currencies have established themselves since the advent of bitcoin. The main competitors are Litecoin, Ripple, QuarkCoin, and Namecoin. Each currency uses the bitcoin blockchain and mining systems but has its own unique features that potentially improve upon the bitcoin model.

Litecoin, the second largest cryptocurrency on the market, currently trades at $15.55 per coin.[37] The premise of Litecoin differs from bitcoin in that mining is much more accessible for the average computer. Unlike bitcoin mining, which has become very difficult and requires processing power only achieved with specially built computers, Litecoin can be mined by anyone who owns a computer and bothers to learn. Because of this expanded mining capacity, transaction times for Litecoin average a mere 2.5 minutes as opposed to ten for bitcoin.[38]

Although much newer than its competitors, Ripple has seen a huge rise in popularity in the past year. Because of the large number of Ripple coins in circulation, 100 billion, each coin is valued at only $0.013.[39] Unlike any other virtual currency, Ripple offers its users the ability to trade and hold any form of currency they desire. They also claim to have a transaction speed of mere seconds.[40] Ripple's ability to accommodate any currency means people can exchange dollars for yen or frequent flyer miles for bitcoins. The global, integrated nature of Ripple allows it to serve as more of a transaction facilitator than a new form of currency altogether. This may make it more sustainable and easy for governments and users to adopt in the future, as the

[37] "Markets." Bitcoin Charts. http://bitcoincharts.com/markets/ (accessed March 21, 2014).
[38] "What is Litecoin." Litecoin. https://litecoin.org/ (accessed March 22, 2014).
[39] Bitcoin Charts, "Markets"
[40] "Getting Started with Ripple." Ripple. https://ripple.com/guide/ (accessed March 22, 2014).

currencies involved in transactions are already guaranteed by government endorsement. Ripple avoids the anti-government, anti-regulation aspect of bitcoin and therefore may have a higher chance of survival while coexisting with fiat currencies.

Auroracoin, the fourth-highest valued "altcoin," as the media calls them, is an attempt by an Icelandic nonconformist to remedy the monetary issues that have plagued the island nation since the collapse of its three largest banks in 2008. Government regulations imposed at the time to protect the Icelandic economy have not been removed and auroracoin is an attempt to circumvent the restrictions on currency that still linger. As the website states "The power must be taken away from the politicians and given back to the people. Cryptocurrencies are a very important milestone in this fight for liberty. They bring the hope of a new era of free currencies, immune to the meddling of politicians and their cronies."[41] To facilitate the adoption of auroracoin, the creators held an airdrop on March 25, 2014 of 31.8 coins to each citizen of Iceland.[42] If people are given a supply of the coins and therefore made aware of their existence, the chances of eventual widespread use are increased. Bitcoin requires new users to take a large risk investing their money in an untested technology. If a free distribution of bitcoins occurred, a much larger and more diverse user base could allow it to gain more traction as a currency.

As of March 23, each auroracoin was worth $10.96, meaning each citizen received a total of $348.52 to jumpstart their auroracoin use.[43] Virtual peer-to-peer currencies provide an ideal opportunity to wrest monetary power away from government agencies. There are many who would like to see virtual currencies come into widespread use outside of any government

[41] "auroracoin." auroracoin. http://www.auroracoin.org/ (accessed March 22, 2014).
[42] Ibid
[43] Bitcoin Charts, "Markets"

regulation. This libertarian aspect of virtual currencies could present a limiting factor of their use because governments will attempt to regulate any currency that gains enough traction to pose a threat to government monetary policy.

Chapter 7: Regulatory Reactions

Since bitcoin's meteoric rise in popularity, governmental agencies have had to make choices about how to approach regulation of the new currency. Issues from taxation to money laundering have drawn the attention of governing bodies who want to keep the monetary policies of their countries stable and under their exclusive oversight.

The IRS has grappled with the issue of taxing bitcoins since the currency became a significant source of income for certain individuals and businesses. The IRS spent several months investigating virtual currencies in order to ascertain the most appropriate method of taxation. On March 25, 2014, these efforts came to fruition with an IRS notice stating virtual currencies should be treated as property and taxed accordingly.[44] The guidelines apply only to "convertible" virtual currencies, or those like bitcoin that can be readily converted into or bought for cash. To calculate gross profit from transactions involving virtual currency, taxpayers must value the currency at its fair market value in U.S. dollars at the date of transaction. If a gain or loss is incurred on the acquisition or sale of property in exchange for virtual currency, the difference in fair market value is taxable. Depending on whether the virtual currency is classified as a capital asset, the taxpayer may have to recognize capital gains and losses in their taxable income. Miners must include any virtual currency income they receive from mining activities in their taxable gross income. Further, if a miner conducts mining as an independent business, the

[44] Aqui, Keith. "Notice 2014-21." Internal Revenue Service. www.irs.gov (accessed March 28, 2014).

miner is subject to an additional self-employment tax. Any wages paid in virtual currencies are subject to federal income taxes. Taxpayers who failed to comply with these regulations before March 25, 2014 may be subject to penalties to correct any inconsistencies with the current law.[45]

These new regulations have profound implications for each and every transaction that occurs using bitcoins. If a customer pays for a shirt on Overstock.com with $20 in bitcoin previously acquired for $10, the transaction will result in a $10 taxable gain for the customer and a $20 gross profit for the website. This discourages customers from paying for everyday transactions in bitcoin in order to avoid paying the capital gains tax that would not result from a transaction using cash.

The capital gains tax rate is lower than the ordinary gains rate. This means that gains on bitcoin will be taxed at a rate lower than gains on other foreign currency investments.[46] Prior to the guidelines, holders of bitcoins could have had the option to report any gains on their investment as capital, but any losses as ordinary. This would allow them to pay lower taxes on gains while accumulating greater deferred tax liabilities on losses.

Bitcoin holders can still use ambiguity in tax regulation to avoid higher taxes. Determining the fair market value of virtual currencies is more subjective than other foreign currencies. Different exchanges report different exchange rates for bitcoin, and users have freedom to select the index that minimizes their gains or maximizes their losses.[47] For example, on March 26, 2014, the three largest virtual currency exchanges, Bitstamp, Bitfinex, and BTC

[45] Aqui, “Notice 2014-21”
[46] Fleischer, Victor. "Taxes Won't Kill Bitcoin, but Tax Reporting Might." Dealbook. http://dealbook.nytimes.com/2014/03/26/taxes-wont-kill-bitcoin-but-tax-reporting-might/?_php=true&_type=blogs&_r=0 (accessed April 6, 2014).
[47] Ibid

China, listed three different prices for bitcoins, $586, $584 and $573 respectively.[48] This discrepancy gives bitcoin investors room to manipulate their gains and losses to pay the least amount of taxes they can.

The guidelines also ensure bitcoin is subject to the same information requirements as cash transactions. This means any bitcoin transactions that serve as compensation require social security numbers and other information to comply with income tax regulations for withholding federal income and payroll taxes.[49] This is a blow to the anonymity so prized by bitcoin users. If anyone is to be legally compensated in bitcoin, the IRS needs to know the same amount of personal information to verify their identity as any other compensation contract. The federal government will now know who is receiving bitcoin as compensation. Those who choose not to comply in order to maintain anonymity make themselves vulnerable to legal action. The anonymity of the blockchain and users' wallets will still be intact, but the government will have some level of awareness as to the flow of bitcoin in the market.

These new regulations by the IRS could prove to be a huge blow to the appeal of virtual currencies. By classifying virtual currencies as property, the IRS ensures that it will be most advantageous for tax purposes for people to treat bitcoin and its peers as property. This means the very nature of the technology as a currency is in jeopardy, because people will have to pay more taxes if they want to use virtual currencies in everyday transactions. The regulation has stripped bitcoin of its fungibility. The value of gains and the amount of taxes required on them will depend entirely on the fluctuating price of bitcoin. A transaction that one day may result in a $10 gain could create a $100 gain two weeks later. This means bitcoins no longer work as a form

[48] Bitcoin Charts, "Markets"
[49] Fleischman, "Taxes Won't Kill Bitcoin"

of currency because the gains or losses will turn into real dollars through taxes whether the owner intends them to or not. All bitcoins are no longer created equal.

Further, although individuals may find ways to circumvent the regulations and maintain the currency nature of virtual-currency transactions, large retailers such as Overstock.com and Ebay will have to comply with the regulations because of their visibility. This incentivizes large corporations to return to cash-based operations. Therefore, the ability for virtual currencies to become part of mainstream transactions has been severely limited by these new regulations. The IRS has essentially guaranteed that bitcoin and its peers will forever be relegated to the dark corners of the internet, where anonymity can prevail over the legal requirements of the federal government.

On March 18, 2014, the Financial Crimes Enforcement Network, a branch of the U.S. Treasury Department, declared that bitcoin exchanges must comply with the Bank Secrecy Act.[50] Enacted in 1970, the BSA established guidelines for certain businesses in order to prevent money laundering. The guidelines apply only to those individuals or businesses FinCEN defines as a money-services business, defined as a company that provides certain financial services such as check cashing, currency exchanges, and money orders. Under this definition, all of the virtual currency exchanges currently in existence qualify as MSBs.[51] The guidelines explain the classification and how it applies to individuals and businesses involved with virtual-currency transactions. The regulations, reporting standards, and recordkeeping responsibilities required of regular MSBs also apply to virtual-currency MSBs, an attempt to protect the money of people trusting MSBs to provide the services they advertise. However, the inclusion of bitcoin

[50] "FIN-2013-G001." FinCEN. http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html (accessed March 21, 2014).
[51] Ibid

exchanges as MSBs contradicts the IRS's requirement that bitcoin does not qualify as a currency, but rather a property. By assuming bitcoin can be laundered and attempting to protect against such activity, FinCEN implies that bitcoin is a currency. These conflicting regulatory efforts by government entities will only create more paperwork and worry for businesses attempting to integrate bitcoin into their operations. A lack of consensus among regulatory agencies will damage the usability of the currency and prevent the growth in popularity necessary for the technology to obtain legal tender status.

According to Janet Yellen, the chair of the Federal Reserve, bitcoin falls outside the realm of the Fed's jurisdiction. "The Fed doesn't have authority with regard to bitcoin but it certainly would be appropriate, I think, for Congress to ask questions about what the right legal structure would be for virtual currencies that involve nontraditional players," she said in February.[52]

The SEC has made some attempts to play a role in the bitcoin marketplace by checking in on bitcoin exchanges. Recently, an entrepreneur named Mircea Popescu, who runs an exchange site, facilitated the sale of a bitcoin-based gambling website for $11.5 million. The SEC inquired about the account statements and any other contracts or documentation for the transaction. Popescu denied the SEC had any place stepping in to regulate virtual currencies. "In the spirit of candor, let me make it perfectly clear that what's being discussed here is nothing else and nothing short of the SEC's ultimate relevancy and importance in the bitcoin space, and so far I am not particularly impressed," Popescu responded to the request.[53] In the near term, Popescu

[52]"Federal Reserve's Yellen: Congress should look at bitcoin regulation." Reuters. http://www.reuters.com/article/2014/02/27/usa-fed-bitcoin-idUSL1N0LW1ZU20140227 (accessed March 27, 2014).

[53] Gail, Sullivan. "SEC gets on the Bitcoin investigation bandwagon." The Washington Post, March 20, 2014, Morning Mix section, http://www.washingtonpost.com/news/morning-mix/wp/2014/03/20/sec-gets-on-the-

may be right and the SEC may not have any jurisdiction over virtual-currency activities. But if bitcoin and its peers are to gain consistency and widespread use, the SEC may have to play a role in the future providing the kinds of valuation guarantees the peer-to-peer model cannot provide on its own.

China was one of the countries with the most loyal bitcoin following until the government took the step of banning financial institutions from dealing in any virtual currency. The central bank of China mandated in December of 2013 that financial institutions cannot trade, underwrite or offer insurance in the currency, but individuals are not prohibited from owning and using virtual currencies. The proclamation led to a 20% decrease in the price of bitcoin, as China had the greatest population of enthusiastic adopters of the new technology.[54] Further damaging the possibility of growing bitcoin popularity in China, the country's largest online retailer, Alibaba, began prohibiting the use of virtual currency on its website in January 2014.[55] Regulation by the Chinese government served to effectively halt any widespread adoption of the virtual currency that was taking place in China, removing a huge portion of the possible worldwide user base of virtual currencies.

In New York, the failure of some bitcoin exchanges and the issues pertaining to the exchanges have caused the New York State Department of Financial Services to call for all bitcoin exchanges to submit applications to become registered exchanges that have met certain state requirements to become legal monetary exchanges. These regulations attempt to ensure "robust standards for consumer protection, cyber security, and anti-money laundering

bitcoin-investigation-bandwagon/?tid=hpModule_a2e19bf4-86a3-11e2-9d71-f0feafdd1394 (accessed March 24, 2014).

[54]Riley, Charles, & Dayu, Zhang. "China cracks down on Bitcoin." CNNMoney. http://money.cnn.com/2013/12/05/investing/china-bitcoin/?iid=EL (accessed April 10, 2014).

[55] Ibid

compliance."[56] Should exchanges follow these regulations, consumers could invest in bitcoin without risking the losses that occurred with the collapse of Mt. Gox.

Chapter 8: Valuation

Bitcoin suffers from wild swings in price, making it an unreliable source of value. The fundamental characteristics of money include serving as: a store of value (it can be saved and used later at a similar value), a unit of account (goods can be measured in money) and a medium of exchange (goods can be exchanged for money).[57] Thus far, bitcoin undoubtedly fails as a store of value. The volatility that has been characteristic of bitcoin since its inception prevents it from maintaining a consistent level of value. In the past year, prices have fluctuated from a low of $70 in July 2013 to a high of $1,150 in December. The following chart depicts the frequent fluctuations in bitcoin's price.[58]

[56] "NYDFS ISSUES PUBLIC ORDER ON VIRTUAL CURRENCY EXCHANGES." NYDFS Issues Public Order On Virtual Currency Exchanges. http://www.dfs.ny.gov/about/po_vc_03112014.html (accessed April 5, 2014).
[57] Asmundson, Irena, & Oner, Ceyda. "What is money?." International Monetary Fund. http://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm (accessed April 6, 2014).
[58] "Bitcoin Charts." Charts. http://bitcoincharts.com/charts/bitstampUSD#rg60ztgSzm1g10zm2g25zv (accessed April 11, 2014).

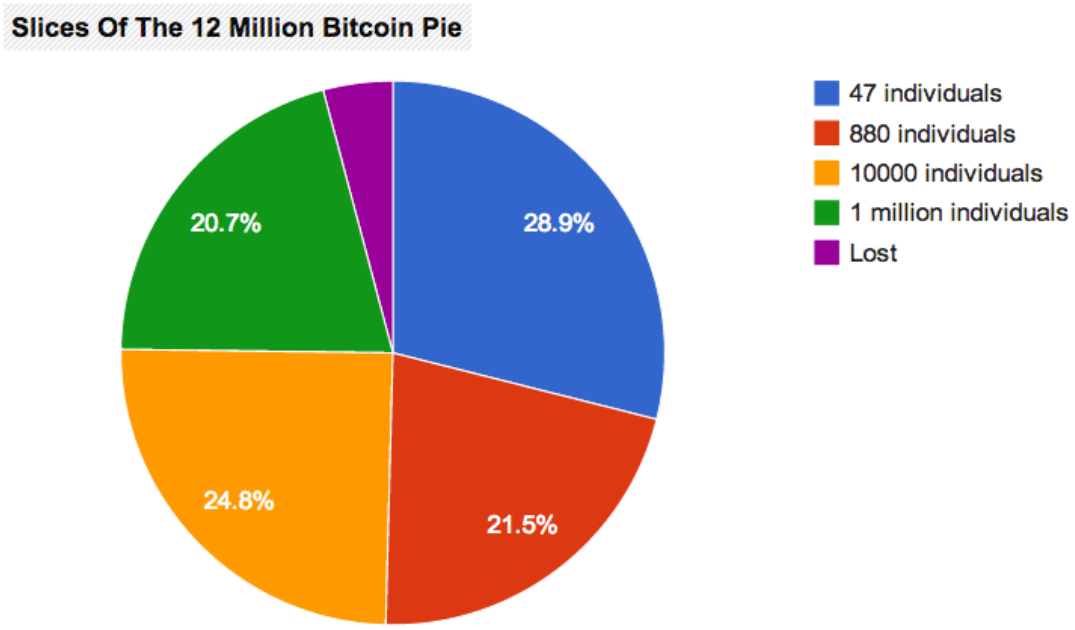
The media frenzy surrounding bitcoin and the technology it has introduced has a great effect on the market price of the currency. Each time an event concerning bitcoin makes the news, no matter how small, the price rises or falls accordingly. For example, the collapse of Mt. Gox in February 2014 caused the price of bitcoin to plummet by 25% from $550 to $418 over the course of a single day, as demonstrated by a sharp drop and immediate recovery in the chart above. Similarly, in April 2014, the Chinese government sent a notice to all bitcoin exchanges warning them of the imminent freezing of their accounts on April 15th, a national effort to crackdown on the virtual currency. The price fell from $450 to $350 immediately, also visible in the chart.[59] In contrast, when bitcoin first came to the attention of mainstream media and was touted as the wave of the future, the price soared over the course of a few months to a high of $1,100 in November 2013. These fluctuations occur because speculators drive the price up or down and the rest of the investors follow suit.

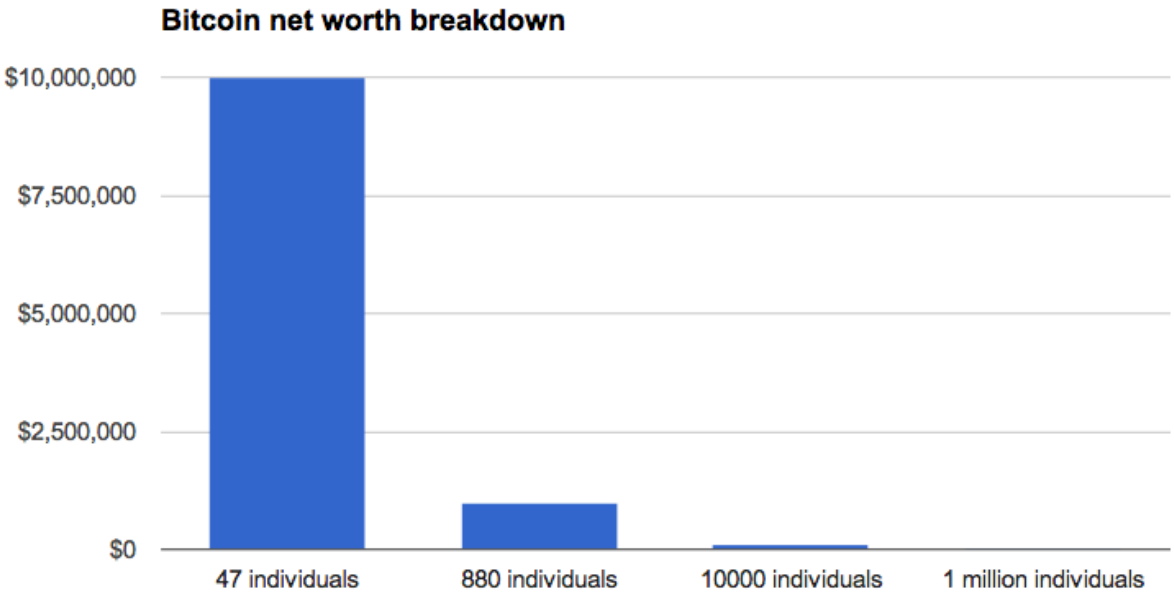
The fact that the media can have such a large impact on the value of bitcoin does not bode well for attracting new users. Exchanging reliable dollars for a currency whose price could fall by 20% in one day is extremely risky and relegates bitcoin to the status of investment opportunity. The media's effect on bitcoin's value is similar to the effect news of a revolutionary new product or revelations of fraud might have on a public company's stock. In this regard, bitcoin and other virtual currencies behave much more like investments than currency. And at this point, those who have taken the plunge and traded hard-earned dollars for a wallet of bitcoins are treating them as such.

[59] Bitcoin Charts, "Charts"

For now, bitcoin users treat their wallets as an investment rather than a usable currency. Researchers have determined that 64 percent of bitcoins are in accounts that have never been used.[60] The owners simply wait for their stashes of bitcoins to appreciate. Second, over half of all bitcoins in circulation are owned by approximately one thousand people. 47 individuals own over 28.9% of all bitcoins in circulation, each account amounting to $10 million on average, as visualized in the charts below.[61] This means the distribution of bitcoin is tiny compared to the general population. In order for bitcoin to escape its investment status and become a viable currency option, more people need to start buying and spending bitcoin on everyday transactions. The media perhaps portrays virtual currencies as more revolutionary than they are in reality. News outlets have adopted the technology as a favorite subject, causing the price of bitcoins to fluctuate wildly with each new revelation. The problem is that very few people actually *use* the currency. Without use, it doesn't matter what kind of ripple the currency is making in the media. Change will only come about if a critical mass of the population adopts the currency as a viable alternative to cash.

[60]Wile, Rob. "927 People Own Half of All Bitcoins." Business Insider. http://www.businessinsider.com/927-people-own-half-of-the-bitcoins-2013-12 (accessed March 21, 2014).
[61] Ibid





Beyond valuation issues, bitcoin must contend with the dollar as the established reserve currency in the world. After World War II, the Bretton Woods system established the United States dollar as the basis of value for 45 major countries' currencies, and therefore, the basis of

value for the vast majority of international business.[62] Even though the system collapsed in 1971, the precedent had been set and the dollar continues to have considerable impact on the value of international currencies to this day. Many international business and trade deals are done in dollars. Furthermore, over 60% of all international currency reserves are in U.S. dollars.[63] The value of the dollar holds great importance not just for the United States, but for all countries that hold it in their reserve systems. The closest competitor to the dollar for reserves is the euro, but the volatility and general decentralized nature of the euro makes it less appealing as an investment in terms of value stability.

This means that the monetary system used by the United States has great effect on the world economy. The economy of the U.S. is so large and prevalent globally that no other countries will endorse bitcoin as currency unless the United States does so first. Nations will not want to deal in bitcoin if their reserves are largely dollars. Even if other countries succeed in integrating bitcoin into their economies, as long as the United States does not provide legal tender status to bitcoin, international trade will not use the currency.

Chapter 9: Bitcoin and Government

Many bitcoin enthusiasts contend that fiat money and bitcoin can exist side by side. This can happen only as long as bitcoin does not pose any threat to government control over the monetary supply. Although the government may be averse to lending credibility to any currency

[62] "The end of the Bretton Woods System." International Monetary Fund. http://www.imf.org/external/about/histend.htm (accessed March 17, 2014).
[63] Conerly, Bill. "Future Of The Dollar As World Reserve Currency." Forbes. http://www.forbes.com/sites/billconerly/2013/10/25/future-of-the-dollar-as-world-reserve-currency/ (accessed April 7, 2014).

other than the dollar, the only way for the government to gain authority over bitcoin is to recognize it as a method of transacting.

Before the end of the gold standard, the government did not have a need to issue money or regulate the money supply. The only reason the government ever got involved in monetary issues was to serve their own purposes and fabricate the ability to finance wars for which they did not have the funds. The same incentives hold true for the regulation and endorsement of bitcoin today. The government will recognize and endorse bitcoin only if the currency 1) garners enough widespread support to pose a threat to the U.S. dollar and 2) becomes valuable enough that the government could enrich their treasury by taxing transactions involving bitcoin. These two issues would serve as enough impetus for the government to recognize bitcoin as a viable currency option whether the government supports the use of virtual currencies or not.

The latter of these two requirements has already been addressed by the IRS. By taxing bitcoin as property, the IRS can collect on any transactions involving the currency without recognizing the legitimacy of virtual currencies. Virtual currencies are not yet widespread enough that it would be more beneficial for the IRS to tax them as currency and therefore income. As of April, 2014, the highest capital gains tax rate was 28%, while the highest income tax rate was 40%.[64] For now, the government seems willing to forego the extra 12% in tax revenue to avoid recognizing virtual currencies as real currency and potentially damaging the value of the dollar, their main source of revenue. Should virtual currencies become more

[64] Internal Revenue Service. "Ten Important Facts About Capital Gains and Losses." Ten Important Facts About Capital Gains and Losses. http://www.irs.gov/uac/Ten-Important-Facts-About-Capital-Gains-and-Losses (accessed April 6, 2014).

widespread, the government will want to get as much revenue out of them as possible at a higher tax rate, even if that means recognizing them as a currency and jeopardizing the dollar's worth.

The only way for the government to maintain the value of money and goods they tax is to recognize their worth and guarantee that value to citizens, otherwise they risk people losing confidence in U.S. currency, in turn destroying government spending power. Further, if American citizens were to lose faith in the dollar, other nations would follow suit and stop accepting the dollar as viable currency, damaging international trade options. In order for the taxes collected from bitcoin to have any value once in the hands of the treasury, the government may have to recognize bitcoin as a holder of value. For now, though, bitcoin is measured in terms of dollars, eliminating the need for government recognition of bitcoin as currency. The government still collects dollars by taxing bitcoin. But, should bitcoin become widespread enough to have intrinsic value of its own, the government will be forced to accept bitcoin as tax payment and recognize it as an alternative currency to the dollar. The only way for governments to neutralize the threat virtual currencies pose to fiat currencies is to harness virtual currencies as a tool of revenue for the treasury, thereby guaranteeing them as a store of value and providing them the same legal tender status as that held by the dollar.

However, this scenario remains contingent upon widespread adoption of virtual currencies by the masses. But, as has already been discussed, this adoption will not occur unless there is assurance of bitcoin's value, as the vast majority of people will not want to invest in a risky new technology without stable value. However, as postulated above, the government will not provide this guarantee unless there is a large enough demand for bitcoins that they threaten the value of the dollar as a currency, impeding on government spending power. Therefore, in order to break this stalemate, a third entity will have to assume the role of guarantor for the

general public in order to facilitate widespread adoption of bitcoin as currency. Clearly no small task, a large treasury of bitcoins must be available in order to stabilize the bitcoins in circulation by issuing or buying up currency, regulating supply as demand changes. An exceptionally large entity highly invested in bitcoin will have to step forward and provide value stability that would convince the average American that the benefits of bitcoin outweigh the risks. Only then will bitcoin use become sufficiently widespread to provide enough value to the government through income taxes that they are willing to acknowledge it as an alternative to the dollar.

Regardless of whether bitcoin escapes the confines of its status as a volatile investment, there are many aspects of cryptocurrency technology that governments around the world could put to use now to eliminate issues with current monetary transactions.

Chapter 10: Cryptocurrency Potential

Some aspects of Bitcoin technology are revolutionary and could be adopted by government regulators to increase efficiency and security in existing monetary systems. First, the bitcoin network is written in Script, a language that allows a bitcoin transaction to be conditional upon a prior event occurring, such as the satisfaction of a contract.[65] This ability to write conditional code creates an entirely new field of law, or, as the media calls it, smart contracts.[66] Second, the virtual nature and widespread verification system makes the network a much cheaper alternative to banks for sending money around the world. Third, the "push" transaction nature of bitcoin makes it much more secure than traditional credit cards.

[65] Hochstein, "Why Bankers Should Care"
[66] Ibid

Smart contracts have conditions written into the virtual script, allowing contracts to execute themselves by only transferring money once certain conditions are met or vice versa. These contracts would be self-sufficient and eliminate the need for contract litigation. As explained by Gil Luria, an analyst at Wedbush Securities, "…were I to borrow money in order to buy a Tesla, as long as I make my payments, that would be reflected by my bank to the blockchain and I would be able to continue to operate my vehicle. But were I to stop making payments on my car, instead of lawyers and debt collectors and repo men getting involved—if the blockchain was not to receive a message from the bank that I'd made my payment that month—they could disable the Tesla and quite directly prevent me from operating it."[67] Contracts such as car payments, loans, or service agreements could all execute themselves. Banks and regulatory agencies would no longer need to serve as facilitators and enforcers. They would simply provide the capital and collect interest.

Further, the transparency of the blockchain history makes dispute resolution simple. Should any contentions arise, the involved parties can easily consult the irrefutable accuracy of the blockchain to settle the matter immediately. This technology would eliminate virtually all issues that occur with contractual agreements. It holds each party liable to execute their side of the deal, automatically halts the contract if satisfaction should not occur, and eliminates any expensive litigation that may arise during disputes. The reliability and efficiency of smart contracts and loans will create a more efficient economy in which money can flow more freely and securely.

[67] Hochstein, "Why Bankers Should Care"

The "push" nature of bitcoin transactions makes them more secure than traditional credit card transactions. In a "push" system, money will only transfer if the owner approves of the transaction.[68] Credit cards, on the other hand, are "pull" systems where the party receiving the money gains access to the payer's account information and is trusted to withdraw the proper amount. With bitcoin technology, account information is safe and inaccessible to anyone except the owner of the account. This aspect eliminates the risk of identity theft that exists with credit cards. Incidents of identity theft cannot occur, such as that which occurred at Target during the Christmas season of 2013, when over 40 million customers of the chain store had their credit-card data stolen by hackers from the store's database.[69] Target had failed to maintain appropriate security measures, such as basic encryption, for their credit-card information, thus leaving thousands of account records vulnerable to hackers. The "push" method of bitcoin would completely eliminate incidents like this by allowing transactions to occur while customer's account information remains completely private.

Bitcoin technology also minimizes transaction fees to practically zero.[70] Especially important for expensive international transactions in which the costs of exchanging currency can add significant expense to companies dealing with large volumes of international trade. Adam Shapiro of Promontory Financial Group analyzed the cost of an international transaction, putting $1,000 down on a vacation rental, using bitcoin as compared to traditional payment methods. He discovered a large discrepancy. The bitcoin transaction only cost an additional $15 whereas a credit card transaction carried $50 in fees and a bank wire cost an additional $40 to $80.[71] These

[68] Hochstein, "Why Bankers Should Care"
[69] Newman, Jared. "The Target Credit Card Breach: What You Should Know | TIME.com." Techland. http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/ (accessed April 9, 2014).
[70] Bitcoin, "FAQ"
[71] Hochstein, "Why Bitcoin Matters"

fees add up for companies making thousands of international transactions a day and bitcoin could provide valuable savings.

For everyday credit-card users, bitcoin could mean the end of any transaction fees charged by credit-card companies to the businesses accepting cards. These fees generally pass on to the consumer through raised prices, regardless of method of payment.[72] The average "interchange" fee that businesses must pay to their credit-card companies in the United States is around 2% of sales. This is two to six times more than countries in Europe, where the fees are government regulated. Mastercard, Visa, and American Express can get away with such high rates in the United States because they control 93% of the market. This oligopoly creates higher prices on practically every good in the United States. Businesses have no choice but to accept the fees or face losing a large portion of their credit-card-wielding customer base. Small business suffer most because they do not have the negotiating power of large corporations such as Walmart that bring enough revenue to the credit-card companies to demand lower rates. In March 2014, Walmart sued Visa for $5 billion, claiming the interchange fees for their credit services were unreasonably high. According to the lawsuit, Visa and its peers had profited $350 billion in excess revenue from 2004 to 2013 as a result of high transaction-fee costs, revenue that could have resulted in lower prices for consumers and higher earnings for retailers had it not been appropriated by the credit-card companies.[73]

Bitcoin and similar virtual currencies, with transaction fees hovering around an average of $0.05 per transaction, could provide a way for businesses to wrest power away from the

[72] Banjo, Shelly. "Wal-Mart Sues Visa over Swipe Fees." The Wall Street Journal, March 27, 2014, http://online.wsj.com/news/articles/SB10001424052702304688104579465690629247558 (accessed April 15, 2014).
[73] Ibid

credit-card oligopoly.[74] By implementing a virtual currency system rather than a credit-card system, small businesses could avoid credit-card fees and boost revenues. Should virtual currency one day become mainstream, cryptocurrency technology provides consumers and business owners with the means to divest large credit-card companies of their power by circumventing credit transactions and their exorbitant fees. The price of practically every single good in the United States would fall as a result, allowing consumers to purchase more and businesses to enjoy more profits.

However, despite the numerous advantages associated with cryptocurrency technology, implementation of the technology in all facets of the economy would create issues pertaining to privacy rights. Should bitcoin become legal tender, the government would require that anonymity be eliminated to avoid laundering and illegal activity. This would expose people's identities to their blockchain transactions. Anybody could, in theory, have access to every single transaction you make. This destroys one of the greatest draws of bitcoin.

The elimination of anonymity may prove essential to improving the bitcoin model. An efficient economy is dependent upon having information freely available to participants so they can make the most productive decisions for themselves and therefore for the economy as a whole.[75] By withholding the identity of bitcoin account owners, the bitcoin model prevents the dissemination of information and thereby impedes complete efficiency from occurring. If each transaction was completely transparent, and the participants knew precisely with whom they were transacting, they may not be willing to exchange goods and money. Bitcoin anonymity

[74]Bradbury, Dan. "Bitcoin Transaction Fees to be Slashed Tenfold." Coindesk. www.coindesk.com/bitcoin-transaction-fees-slashed-tenfold/ (accessed April 15, 2014).
[75] Barry, Christopher B. and Jennings, Robert H., "Sequential information dissemination and relative market efficiency" (1981).Working Papers. Paper 13.

functions differently from cash transactions because bitcoin transactions take place entirely online. Cash transactions must take place in person, exposing the identity of the participants through direct contact. Cash transactions must also occur locally, minimizing the reach of any businessperson who would wish to remain anonymous. Similarly, most online transactions are done with credit cards and require you to give your identity and address. Knowledge of the other party's identity allows people to make an informed decision about whether they want to support and further the business endeavors of the other person by transacting with them. An anonymous system allows the completion of transactions that otherwise may not have occurred had identities been readily available. This contributes to an inefficient market and the poor allocation of resources.

Conclusion

Two aspects of bitcoin are uniquely combined: 1) it is solely a monetary standard, and 2) no government in the world recognizes it as such. This is a contradictory state of being. Having no intrinsic value but carrying no government guarantees relegates bitcoin to the perpetual role of investment opportunity, deriving its value not from a practical use, but from its nominal, dollar value. This will continue to be the case until the U.S. Government sanctions bitcoin as a viable currency. Because the dollar plays such a large role in the world's economy, other countries will not adopt virtual currency technology unless the U.S. does so first. Substantial populations around the world must embrace bitcoin as a significant source of value before any monetary authority will relinquish the power associated with fiat currency. There are, however, many aspects of the virtual-currency model created by bitcoin that could be useful in improving the efficiency of money movement around the United States and the globe, by consumers, investors, and the government.

Bibliography

Aqui, Keith. *Notice 2014-21.* March 27, 2014. www.irs.gov (accessed March 28, 2014).

Asmundson, Irena, and Ceyda Oner. *What is Money?* September 2012. http://www.imf.org/external/pubs/ft/fandd/2012/09/basics.htm (accessed April 6, 2014).

auroracoin. n.d. http://www.auroracoin.org/ (accessed March 22, 2014).

Banjo, Shelly. *Wal-Mart Sues Visa over Swipe Fees.* March 27, 2014. http://online.wsj.com/news/articles/.

—. *Wal-Mart Sues Visa over Swipe Fees.* March 27, 2014. http://online.wsj.com/news/articles/SB10001424052702304688104579465690629247558 (accessed April 15, 2014).

Barry, Christopher, and Robert Jennings. "Sequential information dissemination and relative market efficiency." 1981: 13.

Bitcoin Charts. March 21, 2014. http://bitcoincharts.com/markets (accessed March 21, 2014).

Bitcoin Charts. n.d. http://bitcoincharts.com/charts/bitstampUSD#rg60ztgSzm1g10zm2g25zv (accessed April 11, 2014).

Bitcoin.org. 2009. https://bitcoin.org/en/faq (accessed March 14, 2014).

Bordo, Michael. "The Gold Standard, Bretton Woods, and Other Monetary Regimes: A Historial Appraisal." *Review-Federal Reserve Bank of St. Louis*, 1993: 123.

Bradbury, Dan. *Bitcoin Transaction Fees to be Slashed Tenfold.* n.d. www.coindesk.com/bitcoin-transaction-fees-slashed-tenfold (accessed April 15, 2014).

Casey, Michael. *Treasury's Cohen Warns Unregistered Bitcin Exchanges.* March 3, 2014. http://online.wsj.com/news/articles/SB10001424052702303563304579447020246651110 (accessed March 23, 2014).

Chowdhry, Amit. *Forbes.* December 21, 2013. http://www.forbes.com/sites/amitchowdhry/2013/12/21/overstock-com-is-going-to-accept-bitcoin-in-2014 (accessed April 3, 2014).

Conerly, Bill. *Future of the Dollar as World Reserve Currency.* October 25, 2013. http://www.forbes.com/sites/billconerly/2013/10/25/future-of-the-dollar-as-world-reserve-currency/ (accessed April 7, 2014).

Elwell, Craig. *Congressional Reports.* June 23, 2011. www.crs.gov (accessed March 6, 2014).

FinCEN. 2013. http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html (accessed March 21, 2014).

Fleischer, Victor. *Taxes Won't Kill Bitcoin, but Tax Reporting Might.* March 26, 2014. http://dealbook.nytimes.com/2014/03/26/taxes-wont-kill-bitcoin-but-tax-reporting-might/?_php=true&_type=blogs&_r=0 (accessed April 6, 2014).

Foley, Stephen. *Bitcoin needs to learn from past e-currency failures.* November 28, 2013. http://www.ft.com/cms/s/2/6d51117e-5806-11e3-a2ed-00144feabdc0.html (accessed March 27, 2014).

Fund, International Monetary. *The end of the Bretton Woods System.* n.d. http://www.imf.org/external/about/histend.htm (accessed March 17, 2014).

Getting Started with Ripple. n.d. https://ripple.com/guide (accessed March 22, 2014).

Greenberg, Andy. *Nearly 150 Breeds of Bitcoin-Stealing Malware in the Wild.* February 26, 2014. http://www.forbes.com/sites/andygreenberg/2014/02/26/nearly-150-breeds-of-bitcoin-stealing-malware-in-the-wild-researchers-say/ (accessed April 2, 2014).

Gross, Doug. *Bitcoin ATMs Coming to the U.S.* February 18, 2014. http://www.cnn.com/2014/02/18/tech/innovation/bitcoin-atms/ (accessed March 18, 2014).

Hern, Alex. *A history of Bitcoin hacks.* March 18, 2014. http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative- (accessed March 20, 2014).

Historical Tables. Budget, Washington, D.C.: Office of Management and Budget, 2013.

Hochstein, Marc. "Why Bitcion Matters to Bankers." *American Banker*, March 14, 2014: 1A.

Hurtado, Patricia. *Bloomberg Business Week.* March 31, 2014. http://www.businessweek.com/news/2014-03-31/ex-bitcoin-foundation-s-shrem-in-plea-talks-u-dot-s-dot-says-1 (accessed April 14, 2014).

Kushner, David. *Rolling Stone.* February 4, 2014. http://www.rollingstone.com/culture/news/dead-end-on-silk-road-internet-crime-kingpin-ross-ulbrichts-big-fall-20140204 (accessed March 21, 2014).

McMillan, Robert. *Wired.com.* March 3, 2014. http://www.wired.com/2014/03/bitcoin-exchange/ (accessed March 25, 2014).

Nakamoto, Satoshi. *Bitcoin.* 2009. https://bitcoin.org/en/development (accessed March 10, 2014).

Newman, Jared. *Techland.* December 19, 2013. http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know (accessed April 9, 2014).

NYDFS Issues Public Order on Virtual Currency Exchanges. March 11, 2014. http://www.dfs.ny.gov/about/po_vc_03112014.html (accessed April 5, 2014).

Perlroth, Nicole. *To Instill Love of Bitcoin, Backers Work to Make it Safe.* April 1, 2014. http://dealbook.nytimes.com/2014/04/01/to-instill-love-of-bitcoin-backers-work-to-make-it-safe/?_php=true&_type=blogs&_r=0 (accessed April 10, 2014).

Reuters. February 27, 2014. http://www.reuters.com/article/2014/02/27/usa-fed-bitcoin-idUSL1N0LW1ZU20140227 (accessed March 27, 2014).

Riley, Charles, and Zhang Dayu. *China cracks down on Bitcoin.* December 5, 2013. http://money.cnn.com/2013/12/05/investing/china-bitcoin/?iid= (accessed April 10, 2014).

Service, Internal Revenue. *Ten Important Facts About Capital Gains and Losses.* n.d. http://www.irs.gov/uac/Ten-Important-Facts-About-Capital-Gains-and-Losses (accessed April 6, 2014).

Sullivan, Gail. *SEC gets on the Bitcoin investigation bandwagon.* March 20, 2014. http://www.washingtonpost.com/news/morning-mix/wp/2014/03/20/sec-gets-on-the (accessed April 2, 2014).

What is Litecoin. n.d. https://litecoin.org/ (accessed March 22, 2014).

Wile, Rob. *927 People Own Half of All Bitcoins.* December 2013. http://www.businessinsider.com/927-people-own-half-of-the-bitcoins-2013-12 (accessed March 21, 2014).

Yui, Monami. *Japan Says Bitcoin Not Currency Amid Calls for Regulation.* March 7, 2014. http://www.bloomberg.com/news/2014-03-07/japan-says-bitcoin-is-not-a-currency-amid-calls-for-regulation.html (accessed March 27, 2014).

Zetter, Kim. *Wired.com.* November 11, 2013. http://www.wired.com/2013/11/silk-road (accessed March 17, 2014).