Cryptocurrencies and the Anonymous Nature of Transactions on the Internet

By
Elizabeth Anne Casale

A PROJECT

submitted to

Oregon State University

University Honors College

in partial fulfillment of
the requirements for the
degree of

Honors Baccalaureate of Science in Business Administration
(Honors Scholar)

Presented June 1, 2015
Commencement June 2015

AN ABSTRACT OF THE THESIS OF

Elizabeth Casale for the degree of Honors Baccalaureate of Science in Business Administration presented on June 1, 2015. Title: Cryptocurrencies and the Anonymous Nature of Transactions on the Internet

Abstract Approved:

_____

Victor Tremblay

Bitcoin is a digital cryptocurrency, meaning that it is a currency that is not backed by any government, uses cryptography for security and is difficult to counterfeit. Bitcoin's popularity stems from the fact that it has little regulation and affords some degree of anonymity in transactions. Bitcoin currently has little governmental regulation but greater regulation is expected, as Bitcoin has come under scrutiny from federal regulators because of its role as a medium of exchange for illicit activities and the high degree of anonymity it gives users. Some proponents of Bitcoin welcome regulation, but others feel that it inherently goes against the liberatarian aim of a cryptocurrency.

Key Words: Bitcoin, Cryptocurrency, Regulation, Libertarian, Digital, Anonymity, Economic theory

Corresponding e-mail address: casalee@onid.oregonstate.edu

Cryptocurrencies and the Anonymous Nature of Transactions on the Internet

By
Elizabeth Anne Casale

A PROJECT

submitted to

Oregon State University

University Honors College

in partial fulfillment of
the requirements for the
degree of

Honors Baccalaureate of Science in Business Administration
(Honors Scholar)

Presented June 1, 2015
Commencement June 2015

Honors Baccalaureate of Science in Business Administration project of Elizabeth Anne Casale presented on June 1, 2015**.**

APPROVED:

Victor Tremblay, Mentor, representing Economics

Elizabeth Schroeder, Committee Member, representing Economics

Jon Chesbro, Committee Member, representing Economics

Toni Doolen, Dean, University Honors College

I understand that my project will become part of the permanent collection of Oregon State University, University Honors College. My signature below authorizes release of my project to any reader upon request.

Elizabeth Casale, Author

Table of Contents

Cryptocurrencies and the Anonymous Nature of Transactions on the Internet

Introduction

Bitcoin is a digital cryptocurrency that was created by Satoshi Nakamoto in 2009. There is much debate as to whether Satoshi Nakamoto is a real person, or a pseudonym, as the person identifying as Satoshi Nakamoto has never been revealed offline. Cryptocurrencies have been growing in popularity since that time, due to the ability to use them as a medium of exchange for anonymous transactions on the Internet as well as their use for trade internationally. Bitcoin is very volatile, fueled by speculative activity and changes in consumer confidence. It is unregulated and unbacked by any central government. The growth of the currency is managed by a series of complex algorithms that determine the rate of creation of bitcoins.

Bitcoin has a diverse group of core users and is used for many different types of transactions. In order to understand how core users use Bitcoin, it is important to discuss why Bitcoin was created, how Bitcoin works, and how it measures against traditional currencies. It is also necessary to discuss the social benefits and costs of Bitcoin as a currency in order to discuss the arguments for and against regulation.

The purpose of this study is to analyze how the regulation of Bitcoin would affect its core user base. The research question is: would an increase in regulation solidify Bitcoin as a legitimate currency or drive away its core users? This is important

because Bitcoin can be used for a variety of different purposes and attracts a diverse user base. By analyzing the outcomes of regulation, one can discuss the effect regulation would have on its core user base.

Background

What is Bitcoin?

Bitcoin is a digital cryptocurrency that is not backed by any central government or regulatory agency. Since the creation of Bitcoin by Satoshi Nakamoto, five other developers from four different countries have access to the source code and have taken up the role of developing and maintaining the Bitcoin platform. The source code is the software as it was originally written, and is what tells the program how to function. Each of these developers has access to the Bitcoin source code, and changes to the source code must have a 51% majority of the network download the system for a new version to take effect. (Turpin 337) This means that any changes made to the Bitcoin network must have a majority vote in order to have that change be made. This is meant to make it difficult to make changes that would only benefit one party. However, the overall code is also available online for anyone to download and review.

A Bitcoin is a chain of digital signatures saved in a ledger.[1] This chain of signatures verifies the authenticity of the Bitcoin and records the history of the transfer of ownership. A user of Bitcoin has a wallet in which the bitcoins are digitally stored. Each wallet has a public key, and an address where another party can send you bitcoins. It also has a private key, which is what enables the wallet's owner to send bitcoins to someone else (Turpin 338).

[1] A ledger is a wallet file in the world of Bitcoin

The Need for Bitcoin

Bitcoin is a peer-to-peer electronic cash system, first proposed by Satoshi Nakamoto in his manifesto *Bitcoin: A Peer-to-Peer Electronic Cash System* published on October 31, 2008. In his proposal, Nakamoto argues that an important benefit of Bitcoin is that it allows payments to be made without having to use a financial institution as an intermediary. The need for a peer-to-peer version of electronic cash is necessary, in his opinion, because of the "…inherent weaknesses of a trust based model." (Nakamoto, 1) By creating a cryptographic proof, rather than relying on trust, Nakamoto believes that this system is more reliable. According to Nakamoto's *Bitcoin: A Peer-to-Peer Electronic Cash System*, the system is advantageous because it makes transactions impractical to reverse, which protects sellers and buyers from fraud, and is monitored by a timestamp and chronological order of transactions to further prevent fraud. The timestamp records the time at which the transaction was made and the block chain records the transactions in the order they happen.

How Does Bitcoin Work?

Bitcoin is an electronic currency that can be used as payment for a good or service. The previous transaction, and the public key,[2] of the owner are then added to the end of the "coin", allowing the payee to verify a coin's chain of ownership (Nakamoto).

There are various steps taken to prevent the double spending of a coin. The first step is a timestamp server. A timestamp server takes a hash of a block of items and then publishes this in a public record. The timestamp verifies that the data existed at a certain

[2] A public key is used to send and receive transactions made using Bitcoin.

point in time. Each timestamp includes the previous timestamps, which forms a chain to reinforce the history of the hash (Nakamoto).

The next step is a proof-of-work. The proof of work verifies that the transaction took place (Turpin 339). Every time a transaction is made, CPU power is exerted to complete the transaction. From here, the block value cannot be undone without redoing the work. Later blocks are chained to the previous blocks, creating a chain of work that acts as a public ledger of transactions.

To prevent fraud, or incorrect blocks being added to the block chain, the proof-of-work system is governed by one-CPU-one-vote (Nakamoto). This means that the majority decision is represented by the longest chain of blocks, and that it has the greatest amount of work invested in it and is also the block chain that grows at the fastest rate. This prevents fraud because it means that one would have to posses enough computing power to operate faster than the rest of the Bitcoin network and would also have to be able replicate past work, which is very difficult or impossible to do. As the number of Bitcoin miners (mining is discussed below) and hardware speeds increase, the proof-of-work difficulty is determined by an average targeting for number of blocks per hour, and if they are generating too fast, the difficulty increases. (Nakamoto)

As an incentive to use the proof-of-work system, the first transaction in the block starts a new coin that is owned by the creator of the block. This distributes coins into circulation, since there is no central authority, and creates the incentive to use CPU power and electricity to create the block chain and add more coins into circulation. There are a predetermined number of bicoins, and after these are all released into circulation, the

incentive to exert CPU power to complete transactions will be transaction fees (Nakamoto). This process is known as “mining”, with those taking part in the process known as “miners.” The proof-or-work system is meant to make it difficult for a dishonest miner to try and process transactions in a fraudulent way so as to double-spend coins (Nakamoto).

Why Do People Use Bitcoin?

Bitcoin is used to complete transactions on the Internet. Bitcoin has many aspects that drive users to use it to complete their transactions. Bitcoin is differentiated from existing methods of payment on the Internet because it is unregulated and operates outside the traditional banking system. The motivations to use Bitcoin are that it has the ability to complete transactions anonymously, it can be used world wide, it is easier to carry than cash, it is non-counterfeitable, it has a fixed supply, and has relatively low transaction costs. Understanding the motivations for using Bitcoin is an important aspect of understanding Bitcoin’s core users. Below is a discussion of some of the benefits that lead people to choose to use Bitcoin.

Anonymity

One advantage of Bitcoin is its use for anonymous transactions. When making a transaction with Bitcoin, users do not have to give identifying information other than their key chain identifier. Their Bitcoin identities are also pseudo-anonymous, meaning that the transactions are mostly anonymous, but that it could be possible to identify the spender. (Meiklejohn) While the online identities are not specifically tied to a certain person, all transactions are completely transparent, because they are posted to the block ledger.

When making a purchase with Bitcoin, a person is only identified by their specific key address, not by their name or other identifying information such as in traditional transactions made using mediums such as credit cards. This makes Bitcoin popular with those seeking to make purchases on the deep web. The deep web is popular among those seeking to purchase illicit substances on the Internet.[3] Bitcoin is the primary medium of exchange for those making these transactions, because users do not have to worry about the transaction being tracked back to their name.

This anonymity is also favorable for people in crisis countries. (Woo) It would be advantageous to use Bitcoin for those who worry about having their property unfairly confiscated, or fear high taxes and regulations. The lack of governmental control of Bitcoin protects against that fear as people would not have to worry about having their bitcoins unduly taken.

The anonymity is also favorable for those who are potentially looking to avoid taxes or other regulations. By operating outside the traditional banking system, it also leads to the possibility of avoiding records being made of someone's purchase history. This is advantageous for those who don't want their purchase history recorded.

Ability to Use World Wide

Another strength of Bitcoin is its ability to be used worldwide. While each country has individual regulations regarding Bitcoin, it can technically be used from anywhere worldwide. Bitcoin also reduces or eliminates the need for currency exchange when traveling abroad, because users can make their payments in Bitcoin, without worrying about acquiring the local currency.

[3] See Appendix for definition of Deep Web

Easier and Safer to Use than Cash

Bitcoin is also much easier and safer to carry than cash. It is primarily available in a virtual format, so it is not cumbersome for users to carry around. As Bitcoins are a digital currency, they are also relatively difficult for thieves to steal. In a traditional sense, someone would be unable to stop you on the street and attempt to steal your coins. The coins are stored in an encrypted format on an owner's computer, thus making them relatively difficult to take. Since they are stored on one's computer, they are also easier to keep track of than cash. It is also possible to store Bitcoins online, in a mobile wallet, in a paper wallet, or in a USB wallet as backups. Bitcoin transactions are also completely transparent, so the transaction history of a bitcoin can be completely viewed since its inception, so there are no questions about its ownership.

Non-Counterfeitable

Bitcoin is also a promising alternative to traditional currencies because it is almost impossible to counterfeit. (Woo) Because Bitcoins are created through the mining process governed by a predetermined series of algorithms, and have very specific identifying features, they are very difficult to counterfeit. The timestamp server, proof-of-work, and block chain all prevent the double spending of Bitcoin, and thus make sure that the transactions that are being made are authentic. Counterfeit money led to a direct domestic cost of $61 million in the United States in 2007. (Quercioli) Thus, Bitcoin has lower costs to its users than users of traditional currencies, such as the dollar because of its relative inability to be counterfeited.

Pre-Determined Supply

There is also a finite number of bitcoins that will ever be circulated. Bitcoins are created at a preset rate that is proportionate to the number of the blocks being added to

the block chain. As miners use their CPU power to process the transactions being made with Bitcoin, they are rewarded with bitcoins as well as a small fee charged from the transaction. (Arias) The rate at which the supply of coins is increased is also correlated with the difficulty of the algorithmic proof-of-work problems. These respond to the increase in the number of miners and the computing power of the network. As such, the growth rate is cut in half every four years and will stop approximately around the year 2140 when the supply of Bitcoins is capped at 21 million. (Arias) Among some users of Bitcoin there is uncertainty regarding the effect of the finite supply. Proponents of Bitcoin counter these concerns by presenting the idea that each bitcoin can be split into 100 million satoshis, so it would not be difficult to continue using Bitcoin. (Buterin) This finite supply of bitcoin can reduce the fear of inflation and of governmental interference in the creation of money.

Low Transaction Costs

Bitcoin is advantageous for users because it has relatively low transaction costs as compared to using cash. The peer-to-peer nature of Bitcoin means that a central clearinghouse is not needed for transactions. Miners, who as previously discussed, have an incentive to play by the rules when posting transactions to the ledger, process the transactions. They have an incentive to play a role in processing the transactions because they receive bitcoin as a reward for helping to process the transaction.

Bitcoin also has low transaction costs because it provides an alternate payment method to those who do not have or wish to use credit or debit cards or other electronic forms of payment. (Woo) The use of bitcoins to complete transactions also appeals to those who do not wish to place trust in a central banking system. Because a

predetermined algorithm for the creation of bitcoin governs Bitcoin, the supply is not affected by monetary policy or human decisions.

The Weaknesses of Bitcoin

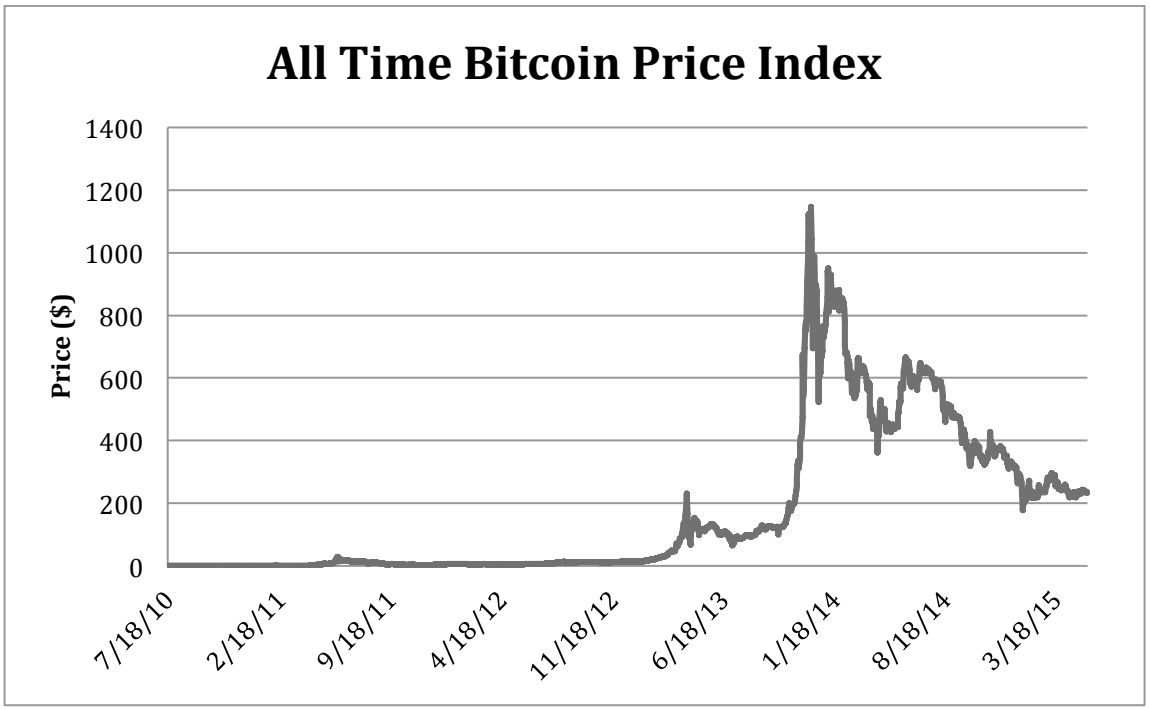
While Bitcoin has many positive attributes that attract users, it also has some weaknesses. These include its volatility, wait time, and lack of strong exchanges. These weaknesses inhibit many people from using Bitcoin, and inhibit Bitcoin's use as a global currency. Some of these weaknesses are what lead different agencies to issue guidelines on, and attempt to regulate Bitcoin.

Volatility

One of Bitcoin's inherent weaknesses is its volatility. This stems from Bitcoin's decentralized nature, and lack of a central regulatory agency. Bitcoin is often affected by speculation. The dollar conversion price has been very volatile over its history, often affected by governmental policy decisions regarding Bitcoin and by the crashes of major Bitcoin exchanges.

Its volatility is three to four times higher than a typical stock, and its exchange rate with the dollar is about ten times more volatile than that of the Dollar with the Euro and Yen. (Yermack) Please see Figure 1 below for the all time price index for Bitcoin. While other currencies, such as the Argentine Real and Mexican Peso, have had large fluctuations in value over time, they typically tend to stabilize after a period of time. Thus, as a store of value, Bitcoin is not a very stable choice for those looking to safely store their money.

Figure 1 All Time Bitcoin Price Index



Data Available From:

http://www.coindesk.com/price/#2010-07-17,2015-04-04,close,bpi,USD

Prices in USD$

Close data from 7/18/10 to 5/18/15

Standard Deviation= $240.34

Lack of Recognition

Bitcoin is also limited in that it is not yet widely accepted for transactions. While the overall adoption rate of Bitcoin has grown, it is not readily accepted as tender by most vendors. The average consumer would have to make vast changes to their lifestyle in order to try and use Bitcoin for all of their transactions. A typical consumer would be unable to go to their local grocer and pay for their groceries using Bitcoin.

Companies such as Overstock.com, Expedia, Dell, and Microsoft say that they accept Bitcoin as payment for goods and services. (Davidson) However, in practice these companies do not technically accept Bitcoin. They typically partner with an intermediary to make Bitcoin transactions happen. When a customer pays in Bitcoin, the company they are purchasing the good or service from uses an intermediary to convert the Bitcoin in cash. (Davidson) Thus, these companies indirectly accept Bitcoin in practice.

This process can be tedious for companies to organize. As long as companies want to convert the transaction payments from bitcoins into dollars, they will be reliant on third party currency converter sites. This can also present a security issue for companies, as any bank or government does not guarantee the Bitcoin exchanges. This also increases the cost of doing business using Bitcoin. It requires companies to expend the energy working to convert Bitcoin into another currency.

Not Totally Anonymous

While many choose to use Bitcoin because of its relative anonymity, it does not create a wholly anonymous transaction. A user's public key serves as their identifier. When a transaction takes place the receiver (new owner) of the Bitcoin adds their public key (public identifier) to the list of previous transactions. (Nakamoto) Thus, the Bitcoin block chain creates a transparent ledger allowing the new owner to identify the ownership history of the bitcoin they now possess.

It is becoming increasingly more difficult for people to keep their offline identity separate from their online identity. However there are steps users can take to keep their offline identity from being tied to their Bitcoin usage. When accessing the deep web

using TOR[4], a user is linked through multiple channels so that the risk of traffic analysis is reduced. However, when browsing the "clear" web, a user's IP address can fairly easily be identified, thus a transaction could be linked back to an individual.

Use for Illicit Activities

Some of Bitcoin's early adopters were drawn to it because of its ability to be used to purchase illicit goods on the Internet. Most of these transactions take place on the deep web that is only accessible using the Onion Router. [5] Bitcoin is the chosen medium of exchange because it is not directly correlated with someone's offline name, and it is not governed by any specific government agency. Bitcoin is known to many as the means to make these illicit transactions happen and this negative publicity directly affects the credibility of the currency. Many people thus are wary of using Bitcoin because of its negative press due to its association with illegal activities.

Wait Time

Another shortcoming of Bitcoin as a currency is that there is a lag associated with its use for transactions. To prevent double spending, the payment must be verified. It takes about 50 minutes for enough additional blocks to be added to the block chain to prevent double spending from happening. (Woo) For two parties that know each other, this is less of an issue because they trust each other and do not have to wait to verify the payment receipt. The person receiving the payment can quickly see if the network has accepted the transaction, but they cannot verify the payment. (Nakamoto) For anonymous transactions, there is the need to wait for the transaction to verify, thus slowing down the time it takes to complete a transaction. As there is no central clearinghouse for

[4] See Appendix for definition of TOR
[5] See Appendix for definitions of deep web

transactions, Bitcoin is likely to remain less than perfectly liquid, thus hindering it's ability for large-scale adoption. (Woo)

Weaknesses of Exchanges

Bitcoin also suffers from the weak security of its major exchanges. As Bitcoin is not backed by a central bank, users of Bitcoin must trust using third party exchanges. Firstly, a user must accept the large fluctuations in exchange rates that take place on these currency exchanges. Secondly, the existing Bitcoin exchanges have been subject to a number of thefts that have resulted in large losses of currency.

In February of 2014, Mt. Gox, then one of the prominent Bitcoin exchanges, was hacked. In the hack, $470 million worth of bitcoins were stolen. At the time, this represented about 7% of the total bitcoins in circulation. (Sidel) The hack of Mt. Gox showcases the inherent risk in using Bitcoin exchanges. As no government or regulatory agency backs Bitcoin, those who had their bitcoins stolen do not have many options for legal recourse.

Competitors

Another threat to Bitcoin is its competitors.. Because Bitcoin is an open source project, it is relatively feasible to create similar projects, and thus has inspired many copycats. (Lee) Some of these other digital currencies include Dogecoin, Litecoin, and Dash (formerly known as Darkcoin). Cryptocurrenices other than Bitcoin are often known as "altcoins." (Lee) This influx of competitors could dilute Bitcoin's value, as users could choose to switch to other digital cryptocurrencies.

While Bitcoin remains the largest and most valuable digital currently, this could change depending on the regulatory horizon for Bitcoin. As Bitcoin is the first and largest digital cryptocurrency, it receives the most press, both positive and negative, leading to

more scrutiny than the other currencies. However, it is possible that if Bitcoin were to become more regulated than the other currencies, that users could choose to switch. It is also possible that a currency could be created that has more favorable characteristics than Bitcoin, or that a flaw in Bitcoin could be discovered leading users to stop using Bitcoin.

Not Legal Tender

The greatest hindrance to Bitcoin's ability to become an international currency is that it is not legal tender. Businesses are not required to accept Bitcoins as payment because it is not a recognized currency. This means that Bitcoin is really only worth the value perceived by its users. (Woo) Bitcoin is also fiat money because it does because it is not immediately convertible into coins or precious metals, like gold or silver. (Mishkin, 56) Thus, the value of Bitcoin could fluctuate widely over time as reflected by what its users think its worth at a particular time. This affects Bitcoin's ability to serve as a store of value, thus undermining its ability to serve as global currency.

Traditional Measures of Currency and Bitcoin

In order to evaluate Bitcoin's feasibility as a currency and the effect regulation would have, it is important to evaluate Bitcoin against some of the traditional metrics of currency. In economic terms, the measures of currency are medium of exchange, store of value, and unit of account.

Bitcoin As a Medium of Exchange

One of the traditional functions of currency is as a medium of exchange. This medium of exchange function is typically associated with the acceptance of a currency as payment for goods and services. The U.S. dollar serves this purpose because it is widely accepted in the payment for goods and services. The role of medium of exchange also

serves to promote economic efficiency and reduce the cost that goes into conducting a transaction.

Bitcoin can be used as medium of exchange because it is accepted for transactions. However, Bitcoin's acceptance as a medium of exchange is primarily limited to transactions on the Internet. Many vendors that accept Bitcoin as a method of payment immediately convert it to another currency.

In some regards, Bitcoin reduces the costs going into a transaction because it is a peer-to-peer network. Transactions made using Bitcoin also do not have to go through a financial intermediary in order to be completed. However, there is a lag time associated with using Bitcoin because of the peer-to-peer nature, and this does not necessarily promote economic efficiency.

Overall, Bitcoin moderately acts as a medium of exchange because it is accepted as payment for goods and services. However, it does not necessarily promote economic efficiency because many vendors immediately convert Bitcoin into a hard currency. Also, various countries have differing levels or regulation regarding what Bitcoin can be used for, thus Bitcoin's acceptability as a medium of exchange varies from country to country. However, Bitcoin can decrease transaction costs because it is decentralized. Thus, Bitcoin moderately meets the traditional measure of currency, medium of exchange.

Store of Value

Another traditional metric of a currency is its use as a store of value. Store of value refers to the level of a medium of exchange's ability to act as a store of wealth. (Fisher, 11) The function of a store of value is to save purchasing power from the time income is acquired until the time that income is spent. (Mishkin, 55) Store of value also relates to

the liquidity of an asset. People often choose how they want to store their assets based on the liquidity they are looking for. As a medium of exchange, money is the most liquid asset because it does not have to be converted into anything else in order to be used. The measure of a store of value also depends on its ability to hold its wealth dependent on the price level.

Bitcoin does moderately have the ability to act as a store of value. Bitcoin can be saved to a person's wallet and does not have to immediately be used for another transaction when received. However, Bitcoin can be extremely volatile in terms of worth, and in this regard is a weak store of value. In the period between December 31, 2012 and December 31, 2013, Bitcoin began around $13 US dollars, fluctuated to over $1,000 US dollars, and eventually fell to around $700 at the close of the year. These large fluctuations do not create consumer confidence in Bitcoin's ability to store and hold value over a long period of time.

Bitcoin's use as a store of value can compromise its viability as a medium of exchange because of the high volatility of the currency, largely due to speculative activities. (Woo) Users of Bitcoin have to be willing to tolerate significant fluctuations in the value of their investment. There is also speculation that those primarily seeking to use the currency for black market activities, as Bitcoin may help the user to avoid certain federal regulations, could use Bitcoin as a store of value, but it is still risky given Bitcoin's volatility.

Unit of Account

Unit of account is used to measure the value of money in an economy. (Fisher 11) Unit of account also reflects the worth of the unit as a medium of exchange. Bitcoin does

have the ability to serve as a unit of account. It reflects the value of an item, and can be used to purchase items. However, part of the definition unit of account includes the ability for two parties to both be able to understand how much the currency is worth. Bitcoin does not really meet this because its value is solely reflected by the value consumers place on it.

Overall, Bitcoin moderately meets the measure of unit of account. However, users do still have to covert to another currency in many cases to complete the majority of their transactions.

The Regulation of Bitcoin

Money is typically regulated by a centralized federal agency. The U.S. Dollar is regulated by the Federal Reserve, which controls the supply of money and the rate of inflation. The United States Federal Reserve also creates confidence in the banking system for the general public because of its regulatory constraint, and serves as a lender of last resort for banks. Confidence in the banking system is also created through the Federal Deposit Insurance Corporation (FDIC). The FDIC insures depositors in a commercial bank or mutual savings fund up to $250,000. (Mishkin, 47) If a financial institution were to fail, the FDIC will pay off depositors up to the value of $250,000.

Bitcoin is unregulated, as it was created outside of the traditional confines of the banking system. This lack of regulation can lead to lack of confidence in Bitcoin as a viable currency. An increase in regulation could increase the confidence in Bitcoin, decrease volatility, and strengthen the major Bitcoin exchanges.

Arguments for the Regulation of Bitcoin

Decrease Volatility

A positive outcome of the regulation of Bitcoin is that it would decrease the volatility of the currency. If Bitcoin were backed by a central bank or government, it would help to reduce the amount of fluctuation of Bitcoin's value relative to real currencies. By reducing the volatility of the currency, Bitcoin would better serve as a store of value. As a stable store of value, Bitcoin could come to be more widely accepted as a legitimate currency. Serving as a stable store of value would also allow users of Bitcoin to have faith in the currency, and not worry that the value of their investment could disappear overnight.

Increased Recognition

Increased regulation of Bitcoin would be a positive thing for users because it would increase the recognition of the currency. This would lead to more businesses accepting Bitcoin as means of payment for goods and services. Businesses would also feel more comfortable accepting Bitcoin as payment, knowing that it has central backing from a major regulatory agency. Regulations regarding how to handle Bitcoin also help individuals and businesses know that they are acting properly in the eyes of the government. However, this could potentially harm black market users because it would make it more difficult to complete their transactions.

Strengthen Exchanges

Increased regulation would also strengthen the security of Bitcoin exchanges. Many users of Bitcoin get their Bitcoins from using currency exchangers as opposed to

mining the currency themselves. Over the history of Bitcoin, the exchanges have been plagued with a series of hacks that have stolen sums that number in the millions. Increased regulation would strengthen these exchanges because it would allow users of the exchanges to know that their coins are backed by a central regulatory agency.

Increased regulation would also take the step of decreasing the likelihood of a bank run. A bank panic or bank run occurs when people fear that multiple banks will fail simultaneously, so they withdraw their investments leading to the point where banks fail. This situation occurs in the absence of, or with, limited deposit insurance and is caused by asymmetric information. (Mishkin, 188) When Mt. Gox, one of the prominent Bitcoin exchanges, halted withdrawals on February 8, 2014, a digital bank run occurred. Users went to withdraw their money, and were unable to do so. Later it was revealed that Mt. Gox had suffered from an elaborate heist with over $470 million worth of Bitcoin taken. Mt. Gox users were without legal recourse to try and get their money back. Regulated Bitcoin exchanges would reduce the likelihood of a bank run, and would increase confidence in using a Bitcoin exchange.

There has already been some movement in regulation and recognition regarding Bitcoin exchanges. In January of 2015, Coinbase launched Lunar, a Bitcoin exchange. Lunar is the first licensed U.S. based exchange. Coinbase is also unique in that it claims to have insurance, thus providing some sort of comfort to potential users of the exchange. (Bensinger) The announcement of an exchange with insurance clearly had a positive effect on the currency as the day of the announcement the price of Bitcoin spiked 16% relative to the U.S. dollar. (Clinch) Coinbase is licensed for use in 24 states, and only users in those states that are licensed can access Lunar. This Bitcoin currency exchange is

a strong step towards increasing the acceptance of the currency, and creating the perception that it is a legitimate currency.

Arguments Against Regulation

While the regulation of Bitcoin could help to cement it as a legitimate currency, some feel that it goes against the inherently libertarian aim of Bitcoin. Bitcoin was founded on the grounds of being a peer-to-peer medium of exchange, governed by the collaborative mining system. If Bitcoin were to be regulated, avid users feel that it would decrease the freedom of its use, a core reason bitcoin was created. Regulation by the United States would also require the government to associate with something that has been widely associated with illicit transactions.

Decrease Freedom

If Bitcoin were to be completely regulated by a government or agency, it would decrease the freedom Bitcoin allows its users. Many of Bitcoin's original adopters chose the currency because it was separate from a specific government or regulatory agency, and was seen as being free from human intervention. As the number of Bitcoins in circulation depends on a pre-determined algorithm, the amount cannot be altered to adjust for depreciation or inflation.

Bitcoin came into being in 2009 during a time of recession. Some early adopters may have seen Bitcoin as a way to operate outside of the central banking system that could be manipulated by policy makers. While the supply of Bitcoin would not be affected by Bitcoin regulation, there would be interference by a central bank or government agency.

Satoshi Nakamoto created Bitcoin to serve as a purely peer-to-peer electronic cash system. (Nakamoto) Bitcoin was meant to cut financial institutions out of the

transaction process because of the inherent trust the financial system requires. When online transactions using traditional mediums of exchange, such as cash, are mediated by a financial institution, non-reversible transactions are not possible, and trust of the financial system is required. (Nakamoto) By introducing financial institutions or governments into the Bitcoin transaction processes, an element of trust in a financial institution is again required for the transaction. Regulation thus goes against the original reason for the creation of Bitcoin.

Use in Illicit Transactions

U.S. regulation of Bitcoin would also involve the United States to directly deal with a currency that has been widely associated with illicit transactions. Bitcoin played a large role in facilitating the transactions that took place on the Silk Road.[6] The top three largest categories of items sold on the Silk Road were "Weed" (marijuana), "Drugs" (encompasses narcotics or prescriptions the seller did not categorize), and "Prescriptions." Of the top twenty categories on the website, the four most popular categories were related to drugs, and sixteen of the top twenty were drug-related. (Christin 8) The website generated more than $213 million in illicit revenues during its existence. (Luther) By regulating Bitcoin, the U.S. government would be acknowledging or would need to at least legally deal with a currency that is used to facilitate illegal transactions.

Regulation by the United States would also be seen as detrimental by those hoping to use Bitcoin to purchase illicit substances. Regulation would make it harder to complete these transactions on the clear web, however these transactions could still potentially be possible on the deep web.

[6] See Appendix for definition of the Silk Road

10. Bitcoin's Core Users

It is difficult to find concrete data on whom exactly Bitcoin's core users are. One user base is Libertarians, who appreciate Bitcoin because it is unregulated by any central bank or organization. Another core group of users are computer programmers, who appreciate Bitcoin because it is completely digital, and managed by a series of complex algorithms. And finally, another core user group are those who use Bitcoin primarily for illegal activities on the Internet. (Wilson) Overall, it is difficult to track Bitcoin's users because many of them use Bitcoin on the Deep Web.

11. Affect of Regulation on Core Users

The issue of regulation of Bitcoin seems to divide users. Those who regard Bitcoin as the future of currency, and use it for primarily legal transactions, will benefit the most from Bitcoin regulation. Regulation could change how Bitcoin is taxed, which would be beneficial for those that hold large amounts of the currency, and currently have it taxed as property. Regulation would decrease the volatility of the currency, making it a safer investment and less risky to hold. It would also potentially increase the security of Bitcoin exchanges, which would make more people feel comfortable changing hard currency into virtual currency.

Those that use Bitcoin primarily for illicit activities will probably deride regulation, as it would decrease its usefulness as a medium of exchange for those activities. However, it would still be possible to use Bitcoin for illicit transactions, as regulated currencies are routinely used for illicit transactions every day.

12. Recommendations For Regulation

The ideal route for regulation of Bitcoin seems to be the regulation of Bitcoin exchanges. As Bitcoin is based off of a computer algorithm, it would be impossible to regulate the creation and distribution of Bitcoin. It would also be impossible to regulate or tax every transaction that takes place because transactions are made possible through the peer-to-peer system. The regulation of exchanges is ideal because it increases consumer confidence in using the exchange, and helps decrease the volatility of Bitcoin. Decreased volatility then stabilizes Bitcoin as a medium of exchange. A regulated Bitcoin exchange would also decrease the instance of theft, thus making it a safer medium of exchange for users.

13. The United States' Position on Bitcoin

It is legal to use Bitcoin in the United States, however it is not regulated by the United States government. A number of reports have been released by the United States Department of the Treasury regarding the treatment of Bitcoin for tax and other purposes.

On March 18, 2013, the Department of the Treasury Financial Crimes Enforcement Network (FinCEN) released a notice providing guidance on digital currencies. (FIN-2013-G001) The notice relates how to apply the Banking Secrecy Act to virtual currencies. Regarding virtual currencies, FinCEN states:

> In contrast [to real currency] 'virtual' currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. This type of real currency either has an equivalent value in real currency, or acts as a substitute for real currency. (FIN-2013-G001)

Thus, the Department of the Treasury recognizes that virtual currencies can serve as a medium of exchange, but are not legal tender and thus do not have to be accepted for

payment for goods and services. The report also defines user, exchanger, and administrator for tax purposes. (FIN-2013-G001) Using the virtual currency to purchase real or virtual goods does not make one a money service business, but being an administrator or exchange of a virtual currency does make one a money transmitter. For purposes of a de-centralized virtual currency, a person who "creates" (mines) the currency is not a money transmitter, but those who create units of the virtual currency and then sell those units to another person in exchange for real currency are money transmitters. (FIN-2013-G001)

On March 25, 2014, the IRS released a report regarding the treatment of virtual currencies for tax purposes. The report states that virtual currencies must be treated as taxable property. The report acknowledges that people use virtual currency to pay for goods and services, and that it could also be used for investment purposes. This helped to further clarify the United States' view of virtual currencies and acknowledges that Bitcoin is considered to be a convertible virtual currency. (Notice 2014-21) The most important aspect of this report is that it acknowledges that miners of virtual currencies must report the virtual currency as gross income. United States taxpayers also have to acknowledge capital gains or losses when exchanging virtual currency for other property. (Notice 2014-21)

14. Conclusions

Overall, the issue of regulation divides users because regulation inherently goes against the original aim of the currency. Bitcoin was created as a peer-to-peer network, managed by those individuals that take part in the mining and block chain creation process. While complete regulation would be beneficial for some of Bitcoin's core users,

it is unlikely to happen. While it is possible to regulate certain aspects, it is unlikely that full regulation would be possible as Bitcoin is not controlled by any central government or regulatory agency. Bitcoin seems likely to continue to grow in popularity, but is unlikely to become a predominant global currency due to its lack of regulation and association with illicit activities on the Internet.

Appendix

Definition of Key Terms:

Bitcoin-Refers to the concept of Bitcoin as a whole, or used when discussing the network. Example: The scope of Bitcoin is global.

bitcoin (lowercase)- Refers to bitcoin as a unit of measurement, similar to the concept of $1 bill. Example: I spent one bitcoin yesterday.

Blocks- Record that contains and confirms transactions

Block Chain- Public record of Bitcoin transactions in chronological order

Clear Web or Visible Web- Everything you can find on the in Internet using conventional search engines that use web crawlers

Coin- Chain of digital signatures

Cryptocurrency- Digital currency that uses cryptography for security, digital to counterfeit and not regulated by a central authority

Cryptography- Area of mathematics that allows people to create proofs that provide high levels of security. In Bitcoin, it is used to prevent the theft of someone else's coins, and also can be used to encrypt a user's wallet.

Deep Web or Invisible Web -Term for some of the more disreputable corners of the Internet, typically only accessible through an encryption method such as TOR

Hash Rate-The measuring unit of the processing power of the network

Mining- The process of using computer hardware to do mathematical calculations to confirm transactions

Peer-to-peer (P2P)- Systems that work like an organized collective group by allowing individuals to directly interact with each other

Satoshi-Unit of measurement, 100 million satoshis=1 bitcoin

Silk Road- Website accessible only through The Onion Router. Allowed users to purchase illegal goods such as drugs, fake documents, and stolen credit card numbers. Was begun in February of 2011 and was closed by the Federal Bureau of Investigation in October of 2013. The site has re-emerged in many forms such as Silk Road 2.0 and Silk Road 3.0.

The Onion Router (TOR)-Originally developed with the United States Navy in mind. Works by routing transactions through various paths so that no single route can link back

to the destination. Creates a private pathway, and allows users to browse the Internet anonymously.

Wallet- Similar to a wallet in the physical world, allows you to see your balance of bitcoins, as well as send them to others

Works Cited

Arias, M., & Shin, Y. (2013, October 1). There Are Two Sides to Every Coin-Even to the Bitcoin, a Virtual Currency. *The Regional Economist*

Bensinger, G. (2015, January 25). First U.S. Bitcoin Exchange Set to Open. Retrieved April 12, 2015, from http://www.wsj.com/articles/first-u-s-bitcoin-exchange-set-to-open-1422221641

Bitcoin Price Index. (n.d.). Retrieved April 4, 2015, from http://www.coindesk.com/price/#2012-12-30,2013-12-30,close,bpi,USD

Bitcoin Price Index. (n.d.). Retrieved April 4, 2015, from http://www.coindesk.com/price/#2012-12-30,2013-12-30,close,bpi,USD

Buterin, V. (2013, October 28). Satoshi's Genius: Unexpected Ways in which Bitcoin Dodged Some Cryptographic Bullets. Retrieved May 1, 2015, from https://bitcoinmagazine.com/7781/satoshis-genius-unexpected-ways-in-which-bitcoin-dodged-some-cryptographic-bullet/

Christin, N. (2013, May). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213-224). International World Wide Web Conferences Steering Committee.

Christopher, C. M. (2014). Why on Earth Do People Use Bitcoin?. *Business & Bankruptcy LJ, Forthcoming*.

Clinch, M. (2015, January 26). Bitcoin Gets First Regulated US Exchange. Retrieved April 12, 2015, from http://www.cnbc.com/id/102367943

Cryptocurrency Definition. (2013, July 29). Retrieved May 15, 2015, from http://www.investopedia.com/terms/c/cryptocurrency.asp

Davidson, J. (2015, January 9). No, Big Companies Aren't Really Accepting Bitcoin. Retrieved April 12, 2015, from http://time.com/money/3658361/dell-microsoft-expedia-bitcoin/.

Fin-2013-G001. (2013, February 18). Retrived October 17, 2014, from http://www.fincen.gov/statutes_reg/guidance/html/Fin-2013-G001.html

First U.S. Bitcoin Exchange Set to Open. (n.d.). Retrieved May 13, 2015, from http://www.wsj.com/articles/first-u-s-bitcoin-exchange-set-to-open-1422221641

Fisher, D. (1980). Money, Banking, and Monetary Policy. Homewood, Ill.: R.D. Irwin.

Greenburg, A. (2013, October 12) End of the Silk Road. Retrived May 1, 2015, from http://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/

How to Store Your Bitcoins. (2014, December 22). Retrieved June 1, 2015, from http://www.coindesk.com/information/how-to-store-your-bitcoins/

Invisible Web (n.d.) Retrived February 13, 2015, from http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html

Kotenko, J. (2014, August 14). A Beginner's Guide to Tor. Retrived February 13, 2015, from http://www.digitaltrends.com/computing/a-beginngers-guide-to-tor-how-to-navigate-through-the-underground-internet/

Lee, T. (2015, May 14). What's up with Bitcoin competitors such as Litecoin and Dogecoin? Retrieved May 20, 2015, from http://www.vox.com/cards/bitcoin/whats-up-with-bitcoin-competitors-such-as-litecoin-and-dogecoin

Luther, W. (2015, February 23). Dark Dollar Dealings. Retrived April 12, 2015, from http://www.usnews.com/opinion/economic-intelligence/2015/02/23/us-has-no-business-regulating-bitcoin-because-of-illegal-dealings

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013, October). A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference* (pp. 127-140). ACM.

Mishkin, F. (2013). The Economics of Money, Banking, and Financial Markets (10th ed.). New Jersey: Pearson.

Nakamoto, S. (2008, October 31). Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto. Retrieved December 23, 2014, from http://nakamotoinstitute.org/bitcoin/

Notice 2014-21. (2014, April 14). Retrieved April 12, 2015, from http://www.irs.gov/pub/irs-drop-n-14-21.pdf

Quercioli, E., & Smith, L. (2009, January 10). The Economics of Counterfeiting. Retrieved May 1, 2015, from https://research.stlouisfed.org/conferences/moconf/2009/Quercioli.pdf

Sidel, R., Warnock, E., & Mochizuki, T. (2014, February 28). Almost Half a Billion Worth of Bitcoins Vanish. Retrieved May 1, 2015, from http://www.wsj.com/articles/SB10001424052702303801304579410010379087576

Some Bitcoin words you might hear. (n.d.). Retrieved May 18, 2015, from https://bitcoin.org/en/vocabulary

Tor: Overview. (n.d.) Retrieved February 13, 2015, from https://www.torproject.org/about/overview

Wetjen, M. (2014, November 3). Bringing Commodities Regulation to Bitcoin. Retrieved December 2, 2014, from http:wsj.com/articles/mark-wetjen-bringing-commodities-regulation-to-bitcoin-1415060058

Wilson, Matthew Graham and Yelowitz, Aaron, Characteristics of Bitcoin Users: An Analysis of Google Search Data (November 3, 2014)

Woo, D., Gordon, I., & Iaralov, V. (2013). Bitcoin: a first assessment. *FX and Rates*.

Yermack, D. (2014, February 18). Bitcoin Lacks the Properties of a Real Currency. Retrieved May 20, 2015, from http://www.technologyreview.com/view/524666/bitcoin-lacks-the-properties-of-a-real-currency/