The Role of Alternative Currencies in the Global Market

Author:
Maxwell Christopher Renke

Supervisor:
Horváth György Ádám

November 4, 2013[1]

[1]This paper was presented on November 12, 2013 as part of the Students' Scientific Conference at the Budapest University of Technology and Economics in Budapest, Hungary and has yet to be published.

Abstract

The concept of alternative currencies is starting to grow in the global market and can prove to have lasting implications for the future of money and trade. Currencies are a means of communicating information about the value of goods and resources that when they fail to do so, cause market failures and inefficiencies. Alternative currencies provide an opportunity to correct the information problem presented by traditional currencies and could have a lasting effect on humanitys attempts at a smooth transition to a more sustainable and efficient future. Bitcoin, a cryptology based currency, is one such alternative that is currently taking hold in the global market. This paper will examine exactly how Bitcoins work, why the technology is so effective, look at Bitcoins history, provide insight into the future of transactions on a global scale, and ultimately answer the question "What gives money its value?"

Contents

1 Introduction

Currency is a means of exchanging information about the value of a good or service. In the current global market, centrally controlled government-issued currencies are the dominant means to conducting trade between parties of a single nation or that of several. These currencies, which used to be tied to items of inherent value, such as gold or other precious metals, are now reliant on the monopoly governments have on the world to regulate and create new currency (and value) in the form of paper money these governments print themselves. While the global network is dominated by established currencies there are other alternatives currencies that hope to be more useful than their regulated counterparts.

Alternative currencies provide a means to conduct trade without the use of the dominant national or multinational currencies. Such alternatives can be created by individuals, corporations, organizations or they can be created by assigning a mutually agreed upon value to an existing object or entity. Each alternative currency has a wide range of advantages and disadvantages and usually have a difficult time creating a foothold in a global economy. One such alternative that has become popular in the global market is called Bitcoin.

Bitcoin is a digital currency operating on a free and open peer to peer network. Bitcoins can be exchanged for real goods and services and the transactions are anonymous and secure. The popularity of Bitcoin is due to the fact that individuals in the Information Age believe that the power to buy and sell a good (i.e. use a currency) should not be restricted by a government and centralized authority. These individuals thrive on openness, anonymity, and most importantly technology and seek to replace centralized currencies all together. Bitcoins and other alternative currencies could also lead to a more sustainable future. Determining whether or not Bitcoin is a viable currency could have lasting implications on the currency itself, the future of other alternative currencies and currencies in general, and ultimately answer the question "What gives a currency its value?"

2 Currency

For centuries humans have exchanged goods and services through the use of direct trade and barter. A seller would offer a good or service and a buyer would offer a good or service of similar value. The value of each good or service would be negotiated and mutually agreed upon between the two parties. This was fine for markets that were small and geographically close to one another but as

humans started expanding the ability to trade goods, usually heavy and difficult to move livestock, was hindered. The world needed a means of representing value in a particular market that was easy to transport and accepted between all parties. As nations developed their governments were able to create currencies for its citizens to use and then as international trade began use between two, or more, nations. Currencies were originally representations of value stored elsewhere (such as gold or other precious materials in a bank) and could be exchanged directly back into the item of value it was representing. The global market has grown out of this need and the value of a currency was directly related to the reputation of the centralized authorities, such as a nations government or other large financial institutions, that have taken the responsibility of managing our currency.

2.1 Trust in a Currency

We all have an inherit trust in the currency we use. An exchange involving currency is merely an agreement between two parties that the transaction has a mutually accepted value. The more widely accepted a currency the greater trust two parties will have in settling their debts. Moreover, if a currency is backed by an authority that is able to enforce the value of the currency two parties will be more likely to use the currency. It is easy to demonstrate this fact with a thought experiment; if Party A owes Party B a finite amount of debt and chooses to pay for it using the US Dollar or the Euro, the two strongest currencies in the global market backed by the most powerful nations on the planet, Party B is likely to accept the payment. If Party A choses to settle his debt with a piece of paper which is has written "One Gazillion Money", with his personal promise that his payment will settle his debt, Party B will likely not accept the payment. Party A's self defined currency is not accepted elsewhere nor has sufficient reputation in the marketplace to be accepted as a representative amount of some value. It seems that the value of a currency is largely based on the trust place in the currency.

2.2 Value of a Currency

How does a currency represent a value? After all, a currency is merely a representation of the value exchanged in a transaction. But where does this value come from? Currency was originally tied to a direct exchange of an object of known value, such as gold or salt. These objects were scarce and inherently valuable (gold for its function and rarity and salt for its usefulness as a food preserve) and thus the currency representing these objects had value. The perceived value of a currency becomes more important when a currency is moved away from a direct exchange of value when the

system becomes impractical. Currency is merely the representation of a value stated by the issuing authority and perceived by those who use the currency, thus does not contain any inherent value. If the value of a currency could be inherent and provable the currency would no longer be subject to changes in valuation over time.

2.3 Alternative Currency

Most currencies in the global market are established and maintained by centralized authorities, usually large governments, that manage and regulate the currency's use. These currencies have trust and value established by these centralized authorities. There are some who believe these authorities are unnecessary and that currency can exists without regulation. Such currencies are called alternative currencies and are openly traded on the global market and often represent the same value as any other nationalized currency. Alternative currencies often provide a means of representing value in a way dissimilar to established currencies that present very interesting advantages and disadvantages as they become more and more popular. One such alternative currency that currently has a foothold in the global marketplace is called BitCoin.

3 What is Bitcoin?

Bitcoin is an open source, peer to peer, decentralized digital currency often referred to as a "cryptocurrency." Bitcoins are currently traded in the global marketplace serviced solely by its network of users. A bitcoin is a solution to a complex mathematical problem known as a hash-function that meet a certain set of requirements requiring a provable amount of work to be performed. Bitcoin Miners run free software applications to attempt to obtain a valid solution, called a block, that is then mutually verified by the network. Bitcoin is a peer to peer system where each party uses a Bitcoin Address and every transaction is secured using public and private key encryption. Transactions are transmitted throughout the network and the process of mining a new block of bitcoins secures all current transactions and adds them to chain of valid transactions that is kept up to date through network timestamps. The speed at which a new block of bitcoins can be mined and the maximum number of bitcoins in the network are fixed.

3.1 History

The original concept of Bitcoin was published in 2008 under the pseudonym Satoshi Nakamoto.

In 2009 the Bitcoin network was established and the first block of bitcoins were issued. This was the start of the Bitcoin network and the users mainly consisted of tech-savy early adopters who understood the technology and were able to implement the network that is free and open to use today.

In 2010 the first bitcoin transactions were conducted with one infamous transaction of 10,000 BTC for one pizza. A major vulnerability in the Bitcoin protocol was discovered on August 6 and was exploited on August 15. Due to a flaw in the verification of transactions throughout the network users were able to create an indefinite about of bitcoins. 184 billion bitcoins were generated from this exploit and sent to two addresses on the network. The bug was fixed within hours and the fraudulent transaction was removed from the network. This remains the only security flaw discovered and exploited in the Bitcoin protocol.

In 2011 organizations such as WikiLeaks and the Electronic Frontier Foundation, and by 2012 over 1000 other merchants began accepting bitcoins as means of payment and donation. This occurred in large part due to the growing popularity and media attention of Bitcoin at the time and create somewhat of a "snowball" effect, whereby the more influential merchants used the Bitcoin protocol the more popular it became thus prompting even more merchants to use the new payment system as well.

In 2012 Bitcoin was the main subject in the CBS legal drama *The Good Wife* in which the currency was criticized stating "Theres no central bank to regulate it; its digital and functions completely peer to peer." This was the first in many pop culture references aimed at Bitcoin as the crypto-currency became more and more mainstream and the focus of a technology world curious of the implications of a truly anonymous and digital currency. More media attention allowed Bitcoin to gain a greater foothold in the global market.

2013 has proved to be a very interesting year for Bitcoin. The digital currency has been receiving even more media attention and criticism and is also starting to become the focus of legal entities such as the US Treasury and the FBI. The use of bitcoin has been seen as a necessity by some due to the outcry for privacy and anonymity in light of the revelations brought to light about the NSA by Edward Snowden.

3.2 Exchanges

Bitcoin has appreciated rapidly in relation to other currencies such as the US Dollar, Euro, and British pound. The comparable price of Bitcoin has drastically fluctuated over the course of the currencies history dropping as low as $13 at the start of 2013 and reached an all time high of $230 on April 9, 2013. The price of a single bitcoin has changed so dramatically because of the constantly changing landscape of who uses and who will accept bitcoins. Bitcoin tends to vary in price, either positively or negatively, following some announcement in the media or some other event related to the validity of the technology as a viable currency in the marketplace. Two notable events had a large impact on the exchange rate both involving the legal aspects of Bitcoin in the Untied States of America, the first involving a price increase after Financial Crimes and Enforcement Network (an agency of the US Department of Treasury) released a statement regarding Bitcoin's legal status, and the second involving the seizure of The Silk Road (an online black market known for its use of Bitcoin) by the Federal Bureau of Investigation causing the price to drop in response. The current bitcoin exchange rate, as of the date of this paper, is 1 BTC to $194.4 (€139.9).

3.3 Functionality

Bitcoin relies on the SHA-256 cryptographic hash function. A hash function is a mathematical function that is difficult to perform, omni directional, and guarantees a fixed length output regardless of input size. An input of any size can be hashed and will produce a unique fixed length output. The processes is irreversible thus knowledge of an output does not grant knowledge of an input. This means there is a finite and controllable amount of work associated with the creation of a block of bitcoins. Each block of bitcoins is defined by a sequence of targeted solutions to the SHA-256 hash function such that the indexed number of leading digits of the output are all 0. This is accomplished simply by trial and error; a block of bitcoin transactions is chosen and an integer value is added called a nonce. This nonce is incremented until the resulting hash of the block contains the targeted run of zeros. The Bitcoin network can vary the difficulty in such a way that correct solutions are reached at a relatively constant rate. The resulting solution is referred to as a Proof of Work.

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

This is a Proof of Work example. The base string "Hello World!" is concatenated with a nonce starting at 0. The target is a SHA-256 hash with the first 4 leading digits being zero. Finding a match for the base string takes 4251 tries.

3.4 Creation

Bitcoin has no central or regulating authority, so anyone can create, use, and trade bitcoins. A person who attempts to create a block of bitcoins is called a Bitcoin Miner. A single PC or mobile device can attempt to mine a bitcoin but most Bitcoin Miners use highly specialized hardware to generate the tremendous amount of computing power necessary to quickly and efficiently find correct solutions. The market of mining bitcoins is very competitive as finding a correct solution is a race against all others in the network. However, the speed at which bitcoins can be mined is halved every 2016 blocks until the value will eventually be rounded to zero. At such time no new bitcoins will be added into circulation and the total number of bitcoins will reach the maximum number of bitcoins at 21 million units. To accommodate for this, each bitcoin can be subdivided to eight decimal places creating 100 million sub-units called satoshis creating 2.1×10^{15} tradable units.

3.5 Proofs of Work

Proofs of work are used in Bitcoin block generation. In order for a block to be generated and verified it must provide the results tied to a quantifiable amount of work. The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to about one every 10 minutes. Due to the complexity of generating a successful proof of work determining which node in the Bitcoin network will generate the next block is unpredictable. Proofs are work are important to Bitcoin because it is the sole reason the currency has value and that value is time. The amount of time it takes to create a Bitcoin is provable and directly related to the worth of the bitcoins it creates; while also providing means of validating a bitcoin block or transaction chain and preventing the issue of double spending (i.e. keeping the master chain of transactions and current number of bitcoins consistent across the entire network).

3.6 Distribution

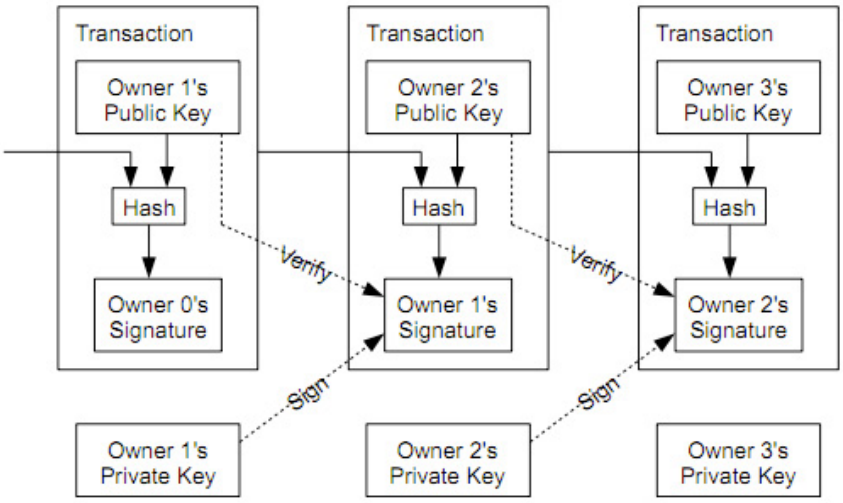
The distribution of all currently available and future bitcoins is fixed. This property is unique to Bitcoin as a currency and is a direct result of the technology behind bitcoin mining. The network increases the money supply to a fixed maximum amount of 21 million BTC as a geometric series. As

previously stated in 3.3 Creation bitcoins can be subdivided to ensure that the network has enough units of bitcoin in circulation. While the total number of bitcoins available, and therefore capable of being awarded for each block generation, decreases the average amount of time required to create a new block will remain consistent at about one new block every 10 minutes (this is achieved by the network periodically adjusting the difficulty of finding the next block). To compensate for this the number of bitcoins awarded for successfully mined block is halved roughly every 4 years until no new bitcoins can be generated. Currently, 25 bitcoins are awarded for each block which is one step away from the original distribution of 50 bitcoins per block and roughly half (10.5 million) of all bitcoins have already been mined. This means that not only was mining bitcoins easier when the network was first established, miners were awarded more bitcoins. As of 2012 the network required over one million times more work to successfully confirm a block than when the first blocks were confirmed. This served to encourage early adopters to put computational and electrical resources towards mining early on to create a large enough initial distribution to serve the market and to prevent the currency of grinding to halt with miners seeing little incentive to create bitcoins. The notion that Bitcoin has a fixed distribution allows the currency to maintain its value which is provable based on the technology that describes Bitcoin.

3.7 Transactions

Bitcoins are stored in a digital wallet with a unique bitcoin address. Each user may have more than one wallet and each wallet may contain at least one bitcoin address. Bitcoin addresses are cryptographic public keys, a unique alphanumeric string of characters, and are tied to the private key of the owner, usually secured by a strong password or other means of authentication within the digital wallet. Each transaction is signed by the private key of the user initiating the transaction and a bitcoin is defined as a chain of these transactions (described in Figure 2 below). These transactions are broadcast to the network which signs a time stamp to each transaction adding it to what is known as a block chain when a new block of bitcoins has been mined. The transactions are part of the most recent block chain are also the longest chains on the network which not only provides a chronological order of events but also shows the sequence is verified by the the majority of the network. Previous ownership of a chain can be easily verified by checking the most recent transaction because Verifying the correctness of a chain is trivial. A transaction cannot be modified without redoing the work done to sign blocks since the modified block was added to the chain. Such modification is impractical; if successful “rouge chains” would propagate the network but timestamps would allow the correct

chain to be mutually accepted by the network. The network maintains current by broadcasting the longest known chain to every node, thereby allowing individual nodes to leave or rejoin the network at will. It is important to note that all bitcoin transactions are broadcast public to the network but there is no way of discerning which user belongs to which bitcoin address other than recognizing a pattern of transactions, however a user wishing to remain completely anonymous would potentially use a different bitcoin address for each transaction.



A diagram of a bitcoin transfer. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

3.8 Advantages

Bitcoin has several advantages as an alternative currency, mostly coming from the Bitcoin protocol itself rather than the currency's actual implementation. These advantages may be unique to Bitcoin, at parity with other alternative currencies, or advantages shared by normalized currencies that exist in the global market today.

Bitcoin is a decentralized currency meaning it has no regulating, centralizing, or governing body to create, maintain, or promote the currency. This allows bitcoin users to operate independently of their home nation and conduct trade between two parties, domestically or internationally, without the involvement of fees, third parties, or any form of regulating legislation. The creation and distribution of bitcoins is completely controlled and fixed by the protocol standard which is open source. Bitcoin as an open platform is perhaps the most important advantage to note; it means that the implementation of the Bitcoin network is completely transparent and run by the users of

the currency. No one user has any right or ability to change the landscape for personal gain. The currency is truly deregulated.

Bitcoin and other similar digital and virtual currencies are popular due to the fact that they provide the user with anonymity. Bitcoin addresses are human readable strings consisting of pseudo-random alphanumeric characters that are no way tied to your identity - only the private key in which you use to encrypt your digital wallet. While all transactions are broadcast publicly across the entire network there is no way to discern someone's identify from their bitcoin address. The promise of anonymity is further compounded by the fact that users can create as many or as few bitcoins as they wish, meaning a user wishing to keep all of his transactions separately anonymous from one another can do so.

The bitcoin protocol is based off of very strong cryptographic technology such as the principles of public and private key encryption as well as the SHA-245 hash function. Not only are the transactions of bitcoins completely secure but the storage of owned bitcoins is strongly encrypted as well (usually through the use of a strong master password). That being said, it is possible to steal a user's digital wallet but that is usually the result of poor security practices of the victim user and not fault of the protocol itself.

Bitcoin operates on a peer to peer network system. This advantage is two fold, allowing any two parties who wish to conduct a transaction to do so without the involvement of a third party and the transaction can be completed in almost real time. Absence of a third party means that transactions are not subject to fees or taxes and is independent of the rest of the network. Due to the speed at which data can be sent (roughly the speed of light) and the vastness of the Bitcoin network two parties anywhere in the world can conduct a transaction securely, anonymously, independently and virtually instantaneously.

Proof of Work is an important part of Bitcoin and other like digital currencies. The amount of work required to generate a single bitcoin is tied to directly to the currency's value and provides a safeguard about its use in the network. In a sense, Bitcoin is more provably valuable than a centralized or heavily regulated currency (such as the US Dollar) because the inherent value is clearly defined, provable, and repeatable only by performing all previous work done by the network, rather than a trust between the user of a currency and its regulators. It is arguable that currencies that incorporate proofs of work are superior to other currencies that do not because the value of said provable currency is represented not only in the perceived worth of the currency but in the technology behind it as well.

3.9 Disadvantages

Bitcoin has several disadvantages stemming from the fact that it is both an alternative and digital currency. These disadvantages are an integral part to the currency that may or may not have effective solutions. However, defenders of Bitcoin say that the advantages far outweight the disadvantages.

One such disadvantage is the idea of public transactions defined by the bitcoin protocol. Bitcoin transactions are secure, anonymous, and encrypted but due to the way the technology works each and every bitcoin transaction is broadcast to every user in the network. The technical reasons of this are to keep the network up to date (since there is no centralized authority to monitor the state of each bitcoin) but lead to a possible insecurity in the system. As stated previously a user is able to increase his anonymity by using multiple bitcoin addresses for separate transactions, allowing the user to mask his usage from those who could use the publicly available transactions records from the network to determine a pattern of transactions that could then be linked to a bitcoin address. However, it is impossible to discern the identity of a user merely from a bitcoin address alone.

The lack of a central authority to regulate the use of bitcoins is the reason public transactions are needed for the technology to function and is perhaps Bitcoin's most controversial property. Opinions on whether or not a central authority is an advantage or disadvantage for a digital currency are widely mixed, some stating that all regulated currencies must be replaced with deregulated ones and others believing the only currencies that can and will work in the global market are those that are centralized. With no central authority there is no single entity to trust, maintain, or manage the currency and thus those that believe this is a disadvantage will say that the currency cannot succeed in the future when and if more and more individuals, organizations, or even nations start using Bitcoin. On the other hand all these functions and more are accomplished by the entire Bitcoin network as a whole allowing all parties to mutually agree on the direction the protocol is taken as well as keep the system in check through the process of peer review. At this time it is unclear whether or not Bitcoin can overcome this disadvantage (if it is even a disadvantage at all) in the near future.

Bitcoin was born in the digital age and therefore comes with some requirements possibly taken for granted by its creators and user. Bitcoin, while completely free and open, has two major requirements before a user is able to conduct transactions - understanding and infrastructure. The use of Bitcoin requires a certain level of knowledge, not only about how to obtain a bitcoin address, bitcoin wallet, and conduct a bitcoin transaction but it is arguable that there is a minimal threshold

of understanding the technology behind the currency itself in order for a user to be able to see and therefore trust in the value of using bitcoin. Many who are hesitant of using the bitcoin protocol are so because they simply do not understand why bitcoins have value and why they are not simply fabricated pieces of information with no value. Infrastructure is vital to the use of Bitcoin; the Bitcoin network would simple not operate without an infrastructure of nodes. This infrastructure has been mainly developed by early adopters and third party services lessening the user's barrier to entry to simple access to the network. The Bitcoin network is built on the internet therefore access to the internet is required to use the currency. This statement is obvious but brings to light the fact that without access to the internet the currency becomes useless. This is a major disadvantage to the currency because while the Bitcoin protocol may be open, it is proven time and time again that corporations and governments have the capability and the desire to restrict a person's right to access and use the internet freely, thus allowing any such entity to restrict the use of bitcoin by simply denying access to the network itself.

A topic that goes along with the notion of a required infrastructure and lack of a central authority is the storage of one's digital wallet. Wallets store addresses and these addresses store the ownership of a finite amount of bitcoins. These wallets use strong encryption in conjunction with a master password to keep them secure when they are stored. Stored wallets exist on the storage device (either on a personal computer or a smartphone) and are the sole record of ownership of the contained bitcoins. If the wallet is lost, stolen, deleted, or corrupted the information no longer exists. The network is a peer to peer system and there is no centralized authority or third parties involved therefore there is no way to retrieve the information stored in a lost wallet and the responsibility of maintaining ownership of the stored currency falls on the user, rather than in the case of a centralized currency a banking institution. Several anecdotal as well as documented cases have arisen throughout Bitcoin's history involving wallets being stolen or simply lost due to device failure or disaster. The solution to this problem of course is the adoption of a proactive backup strategy of a user's wallet, but this a timely and difficult process to maintain.

Bitcoin, and all other digital currencies, have no physical attributes whatsoever. This means that while the currency has a set and provable value critics will argue that it should not be used in exchanges of other physical properties. Yet all of the value of a bitcoin is essentially only information stored in a digital medium. There is some debate of whether or not value can exist in the digital space the same way it does in the analog world. All other currencies are stored in both an analog and digital form and the conversion between does not change the value of the currency in either

form. Bitcoins do in fact exist as physical tokens but these are merely representations of the digital information in the analog world.

3.10 Credibility

Critics of Bitcoin will almost always start with targeting the currencies credibility in the marketplace. There is no doubt that Bitcoin has become a successful and widely used currency among those who are interested in a market-based decentralized digital currency. Critics will argue that that demographic is simply too small to matter and that the currency itself will never have a permanent foothold in the global marketplace. However, there is substantial evidence that the crypto-currency has been recognized with legal precedent, reached a critical mass in popularity that it current is and will remain a popular and widely used currency, and that the digital currency can react to events in the global economy much in the same way nationalized currencies can be affected by political events.

3.10.1 FinCEN

The Financial Crimes and Enforcement Network (FinCEN) is a bureau of the US Department of Treasury who's main goal is to fight money laundering in the United States of America. FinCEN establishes guidelines for what they term "decentralized virtual currencies" such that sellers of said currencies may be subject to registration and other legal obligations under the classification of Money Service Businesses (or MSBs). Bitcoin and Bitcoin Miners fall under such categorization and on March 18, 2013 FinCEN issued a report citing Bitcoin as a virtual currency falling under MSB regulations stating digital payment systems such as Bitcoin are not legal tender under any sovereign jurisdiction and therefore are classified as "virtual currencies." FinCEN went on to say in that report that, "A user of virtual currency is not an MSB under FinCENs regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations." Moreover, the bureau went on to say "...a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter." This means Bitcoin Miners who create and sell bitcoins fall under the same rules and regulations as MSBs. FinCEN went on to say "In addition, a person is an exchanger and a money transmitter if the person accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency." Clearly FinCEN and the US Treasury

recognize the Bitcoin currency as something at the very least is of interest of them to monitor as it is viable enough to require regulation and legislation. Proponents of the Bitcoin currency will say that this regulation is unnecessary and may end up being detrimental to the currency as a whole which wishes to remain completely deregulated and decentralized.

3.10.2 Merchants

A currency is useless if no one uses accepts it. As such the viability and usability of Bitcoin is directly related to the number of users trading with bitcoins and combined faith of the users in the currency (i.e. its value). Bitcoin is a peer to peer system which means the simplest and most popular use is trading value between two individuals but there are entities that serve as third party solutions for those wishing to conduct transactions using bitcoins. The two most notable organizations are Coinbase, an online digital wallet and payment system solution, and BitPay, the world leader in bitcoin business solutions. Both solutions offer no transactions fees, no cashbacks, no waiting on third parties and a host of benefits associated with the bitcoin protocol. Since October 2012 BitPay has reported over 1000 merchants using their service including Wordpress.com and hundreds of ecommerce solutions. Organizations such as WikiLeaks, an international non-profit organization which publishes secret and classified information online, and the Electronic Frontier Foundation (EFF), a non-profit digital rights advocate charity, also accept bitcoins as means of donations. However in June of 2011 the EFF temporarily suspended their ability to accept bitcoin after raised concerns of a lack of legal precedent of the, at the time, new digital currency system. This decision was reverted on May 17, 2013.

3.10.3 The Silk Road

The Silk Road was an online black market, launched in February 2011, operating as a hidden service users could access anonymously and securely without being monitored. Often referred to as the "Amazon.com of illegal drugs" and was in fact used to trade drugs, illicit materials, and even purchase a hit (murder for hire) and was most certainly the underground of the internet. The FBI arrested Ross William Ulbricht in a sting operation on October 2, 2013 and identified him as the founder of Silk Road. He was charged with purchasing murder for hire and narcotics trafficking in a sting operation and the FBI seized and shut down Silk Road. What does this have to do with Bitcoin? Due to the fact that bitcoins are completely anonymous and decentralized the currency was the required means of payment for all transactions. Ulbricht, who had 26000 bit coins seized

from his personal wallet, is thought to be in possession of nearly 600000 bitcoins, nearly 5% of all bitcoins in existence and worth approximately $80 million, that the FBI also attempted to seize. The lack of legal precedent for the seizure of digital currency the FBI is treating the seized bitcoins as a valued good and at such a time when the investigation is completed the seized property will be released back into the market to the highest bidder. The seizure caused the price of a bitcoin to drop heavily before it bounced back slightly by the end of the day due to raised concerns that Bitcoins were so closely tied to criminal activities. Defenders of Bitcoin will say that any currency can be used in a black market and that the use of bitcoins in an illegal transaction is no different than using cash (which usually is anonymous when it changes hands) of any other currency. Due to the market and media response to this even it is clear that Bitcoin has a use in all markets, especially those in which buyers and sellers wish to preserve their anonymity.

4 Bitcoin Comparisons

Bitcoin is often compared to established digital currency systems as well as the centralized currencies in the global marketplace. These comparisons not only help define Bitcoin but also allow the usefulness and validity of the currency to be approached from various perspectives. In its current state Bitcoin cannot replace any well established currency system, however these insights may show how Bitcoin needs to improve or what the goal of other digital currency systems wishing to be more successful than Bitcoin need to do in the future.

4.1 Video Game Currencies

Early video games used a simple point system to track a players progress. These points were awarded by the game creator for performing various actions or completing certain tasks within the video game. As these points were largely arbitrary and relative only to another instance of the same game they served no purpose, or value, outside of the game itself.

As video games became more complex, involving characters and a plot based story, progress was often tracked through the use of a fictitious currency within the game. The first and best example would be gold coins, the most iconic example being the 1985 platformer *Super Mario Bros.* Gold coins are scattered throughout the level and more the more coins you as a player collect the more points you receive at the end of the level. This straightforward approach treats the coins as collectibles rather than an actual currency (the coins cannot be exchanged or used in any way, only

to translate into points relative to a players progress), the only parallel being that gold coins in our market place have real value.

More advanced single player video games use currency in one of two ways, either as an item to be collected that will translate into either points or progress, or an actual form of currency that can be used in the game world in exchange for goods or services. These games usually have a means of purchasing upgrades or required items for the game but they do not have a true economy, the currency in game is merely converted into an item and upgrade without the notion of a transaction. Currency gained in these games are only available to the current instance of the game and thus cannot be traded, giving them no value.

Massively multiplayer online games (MMOs) involve large numbers of players all participating in a single global instance of a game. The players work together to accomplish tasks and achieve goals and in nearly every case there is some form of economy within the game. In these games progress is often conveyed through the means of displaying the amount of time a person has played the game or the amount of wealth a person has obtained within the game. Items in the game have value within the game based on their usefulness in the game or their cosmetic appeal. MMOs usually have an economy based on items that are able to be bought and sold between players in game and the prices are driven in a similar way to a market based economy, including supply, demand, and scarcity. These economies are often most prevelant through the use of in game action houses.

Auction houses in MMOs reflect traditional auction houses where players can buy and sell items based on their in game value and prices the players set for themselves. *World of Warcraft* is the most popular MMO today and uses an auction house based on their in game currency, 'gold'. Blizzard, the company who develops *World of Warcraft*, states that the only way to obtain 'gold' is through in game means. This does not prevent secondary markets from forming that consists of players acquiring in game currency that they will real currency, called gold farming. Blizzard bans gold farming in their terms of service and there are some taxation and legal issues regarding those who participate in gold farming.

While Blizzard attempts keep its *World of Warcraft* auction house strictly in game, *Diablo III*, another title developed by Blizzard, uses an auction house that is tied to real world currency. Interestingly *Diablo III* is a single player game but the players can obtain items of varying usefulness and rarity and trade amongst one another using real money. This marriage between in game items and real world currency proved to be detrimental to the game and Blizzard has since decided to remove the auction house from its game permanently in March 2014.

A game to successfully operate a market based economy within the game that is tied to real world currency is *EVE Online*, developed by CCP Games. The game is in fact largely economy driven by the players, creating supply and demand and even manipulating the market on a grand scale. The game itself is a fascinating look at an isolated economy where true market risks, including scamming, are present. The economy is so complex that in 2007 CCP games hired an economist to help the studio, the first for a games company. While players can pay CCP games to renew their subscription or directly obtaining in game currency, the reverse (turning in game currency into real world curreny) is forbidden.

In every instance of these game economies the game developers unanimously state that there is no monetary value in any in game currency and that the companies maintain the rights to any in game assets. This essentially means that a game developer has no obligation to return any monetary value to a player if he or she loses access to their character, the character is accidentally deleted, or even if the game is shut down preventing any future access to any assets obtained while playing the game. When a developer takes monetary value in exchange for an in game item or service they are not performing a monetary exchange but rather they are granting you temporary rights to an in game commodity.

The main differentiator between Bitcoin and fictional currencies is that while bitcoins are virtual much in the same way video game currencies are they still represent true monetary value. An exchange between an established global currency and bitcoins can be reversed, therefore bitcoins must be treated as a digital currency separate from virtual currencies present in video games.

4.2 Gold Standard

Throughout the early history of economies gold was a widely accepted form of currency. Gold was preferred because of its rarity, durability, divisibility and its ability to be widely recognized, all hallmarks of a strong currency. Governments created a *de facto* gold standard establishing a fixed means of exchange where the true value of a currency is directly tied to a fixed value (or amount) of gold that is independent from the inherent value of the currency itself. This means that paper money could be used for the first time in exchanges allowing two parties to conduct a transaction based on the value of gold but using another currency guaranteed by the government to be equal in value to a fixed amount of gold. In the early days of these standards these notes could be directly exchanged for their equivalent value in gold by the government.

A currency that uses a gold standard has no intrinsic value, rather the value is represented by

the promise of a centralized authority (in most cases the government) to redeem the currency at any item for the equivalent amount of gold. This is accepted by the two parties conducting a transaction and allowed economies to grow; paper money was much easier to use. The use of a gold standard introduces the first player of trust parties who wish to conduct transactions must accept in a paper based economy, the trust in a centralized authority. A true gold standard is trivial to understand and traders can clearly comprehend and agree that their transaction has value because they only have a single degree of separation between the currency in the transaction and the actual store of wealth.

Ignoring the fact that bitcoin transactions are digital and not paper based, bitcoins are not separated from the actual store of wealth nor require trust in a central authority to maintain their value. This seems to suggest that the use of bitcoins is in fact stronger than the gold standard, as in fact the gold standard is no longer used in the global marketplace.

4.3 US Dollar

The US dollar was originally based on a silver standard, defined in the Mint Act of 1792. The US dollar continued to be backed by silver with the exception of the period of the Civil War and the War of 1812. Gold coins were not used as a standard until 1834 and gold did not become a standard until the Gold Standard Act was passed in 1900. On August 15, 1971 the US dollar was suddenly removed from the gold standard and slowly transistioned into the role as the global reserve currency.

The US dollar is perhaps the strongest currency in the global market due to the fact that the US is one of the worlds largest superpowers. This means the trust in the US dollar is rather high due to the ability the United States government has to enforce the currency as means of legal tender. However, through most of its history, the US dollar has been backed by some form of external value, be it silver or gold. The break from these standards several decades ago created a global market in which a nation's currency was valued against the value of other nation's currencies. While the US dollar may be the strongest there is no one currency that defines the value of the market. Therefore without the use of a gold standard, or any standard of value whatsoever, the value of the US dollar is only its inherent value, which is negligent, and its ability to be accepted across the entire global market.

The argument can be made that the US dollar lacks any true value outside of the enforcement and acceptance brought about by the US government. That is to say that the currency's value is directly tied to the central and issuing authority responsible for the currency. Bitcoin does not rely

on a central authority to retain its value rather bitcoins are inherently valuable due to their proof of work (in this sense bitcoins may be superior to the US dollar). The issuing authority for the US dollar is the Federal Reserve, while bitcoins have no issuing authority.

4.4 Federal Reserve

The Federal Reserve System, established December 23, 1913, is the central banking and issuing authority of the United States. It was created upon the enactment of the Federal Reserve Act in response to several financial panics in the US. The main objectives of the Federal Reserve are to ensure maximum employment, stable prices, and moderate long-term interest rates. The United States economy works by using a number of private banks that can keep their reserves at their local Federal Reserve Bank, allowing private banks to lend funds to one another. Federal reserves also contain federal reserve credit which can be converted into federal reserve notes. The system of lending between banks and keeping stores in the Federal Reserve controls how currency is distributed throughout the economy and how said currency is controlled through the use of central banking. This provides further stability to the US Dollar as the economy is heavily controlled. In contrast, Bitcoin has no banks or central authority, and the distribution of all current and future bitcoins is controlled through the use of the protocol itself, eliminating the need for a regulator.

4.5 New York Stock Exchange

The New York Stock Exchange (NYSE) is the world's largest stock exchange with a market value of its participating companies at over $16 trillion as of May 2013. The NYSE is a delicate balance of digital systems monitored by brokers to conduct business transactions. In the Information Age these transactions occur thousands of times a second and provide an enormous amount of data for investors. This data is then used to create algorithms to conduct trades based on several market factors in real-time (meaning trades can be analyzed and new decisions can be made at the same rate the transactions are being processed). These algorithms are much more efficient than human traders and become increasingly more powerful and accurate each year. However, this leads to the conclusion that a large portion of the market (at least for the NYSE) is dominated by computer controlled, digital transactions. All money flowing in and out of the NYSE is in digital form but the numbers being processed do not have any value whatsoever and are merely representations of other forms of currency. One small mistake in an algorithm could not only exchange money in non-desired and even disastrous ways, but it could prove to be catastrophic as the numbers representing wealth

could be permanently altered or lost for good. Bitcoins retain their value no matter how they are represented as their representation is tied to their value, or proof of work.

5 Bitcoin as a Currency

Bitcoin has been well defined an circulated alternative currency. There is still debate, however, over whether or not Bitcoin currently is or can possibly become a currency. As previously stated a currency is hallmarked by four major attributes: means of exchange, means of accounting, means of a store of wealth, and means of legal tender. Any alternative currency meeting these requirements could be considered a true currency in the global marketplace. These four aspects will now be discussed in detail. Note that this discussion will not attempt to decide whether or not Bitcoin can be considered a true currency rather a discussion of the requirements when applied to the currency.

5.1 Means of Exchange

Bitcoin examined as a means of exchange will determine the ability and effectiveness of a bitcoin transaction communicating an exchange of a good or service.

A bitcoin transaction must be able to evaluate any good or service in a given marketplace. Currently bitcoins are used to settle debt between two parties, purchase digital and physical goods, donate to organizations and charities, and much more. The ability of a finite amount of bitcoins to define a good or service is only limited by the willingness of two parties to use the currency as a means of defining the exchange required, thereby fulfilling the definition.

A bitcoin must remain useful over time to be considered a true currency. Due to the required amount of work to generate and use a finite amount of bitcoins the resultant proof of work remains useful as it is part of a chain of all previous and future transactions. The limit of usefulness is therefore only restricted to the amount of time information transmitted in digital form will be useful (which for all intensive purposes includes all of the foreseeable future).

There must be a low cost of storage associated with storing a finite number of bitcoins, not only for a single user but the entire network. The bitcoin network exists on the internet where each node is capable of storing the entire networks history and then transmit the same amount of information every time a new node wishes to update the network. The cost of storing bitcoins on a single node is negligible in todays market as digital storage devices are prevalent across the entire network.

A true currency would not be usable if it only existed in a single denomination or unit as prices

in the market could not adjust to change as easily. As such, currency needs to be easily divisible. Due to the fact that Bitcoin is a digital technology and that dividing a single bitcoin is built into the protocol, subdividing a bitcoin is trivial.

In order for a currency to be effective it must have a large market value. Previously gold and precious metals or scarce materials were used as a means of currency because these objects were able to convey meaning based on their weight and volume. Quite simply larger objects had more worth than smaller ones, but could be divided. Bitcoins are a unique series of transactions appended to one another to form a chain, though the length of this chain does nothing to differentiate bitcoins from one another and does not have any relation to its value. The value, or weight, of a bitcoin is inherited by the proof of work function which has a provable value within the context of the bitcoin system, but not necessarily in the context of the global market.

A true currency is also recognizable. This topic is somewhat of a gray area for Bitcoin, because the bitcoin addresses themselves are technically human readable but you need specific software to be able to parse and understand that information. There are physical representations of bitcoins that are not quite as popular that take the form of a coin with a recognizable Bitcoin logo. Many bitcoin addresses are presented in the form of QR codes (scannable codes used to display text based information) that is often marked with Bitcoin branding, explaining the purpose of the code and its intended function. Despite the ability to be recognized there is nothing about a bitcoin or bitcoin address that is inherently recognizable on its own.

A currency must not be difficult to forge or counterfeit. While it is theoretically capable to craft fraudulent transactions and attempt to circulate them across the network the attempt would require a repetition of all the work done previously in the network and then would require to be propagated throughout the entire network with a time stamp greater than that of the most recent . Practically speaking this is impossible and bitcoins it seems cannot be forged without an amount of effort considerably larger than the entire network is exerting at any given time.

5.2 Means of Accounting

Bitcon examined as a means of accounting will determine the ability of the bitcoin network to perform accounting functions. All currencies rely on a system of accounting to track an amount of currency and provide records of transactions. Individuals, organizations, corporations, banks, and the government all use similar methods to allow numbers using in accounting methods to reflect a value. In the case of most nationalized currencies, a number in an accounting document represents

value by the understanding that the currency exists in a different state and the account record can be verified to be accurate. This is usually accomplished, as with all centralized currencies, by means of a third party authority. Bitcoin, as a peer to peer network, remains up to date by broadcasting the accounting information of the entire network to every node. That is to say, every node is aware of every current and previous transaction in the network, thereby eliminating the need for a third party authority to manage the records of the currency.

5.3 Means of a Store of Wealth

Bitcoin examined as a means of a store of wealth will determine the ability of the currency to convey its value over a long period of time.

A bitcoin, and therefore a bitcoin transaction, will remain valuable because it is a a set off all previous transactions each of which is required to keep the finite number of bitcoins in said transaction usable. All previous work performed in a transaction chain is stored in the current transaction and is necessary to conduct a future transaction. This proof of work system allows the currency to be valuable as well as serve as a representative of the value already held in the currency. This value is stored in chronological order allowing a bitcoin transaction to convey its meaning over an extended amount of time.

Scarcity is a vital factor in any currency and is required to allow a unit of currency to display some value. While bitcoins are being generated their distribution is fixed and their scarcity increases over time as less and less bitcoins are mined the longer the network is in place. This gives bitcoins scarcity until the time at which all bitcoins are generated. The market need for more bitcoins and the exhausted supply will mean bitcoins will become a completely scarce resource. At such time each individual bitcoin can be divided into smaller units to fill market needs.

Inflation is also a key factor in any currency; as the general price level rises each unit of currency is capable of purchasing less and less goods and services. Inflation is normally regulated by a centralized authority but this is not the case with Bitcoin. A centralized authority can increase the money supply to meet market demand causing large amounts of inflation. With Bitcoin, the money supply is fixed and prices are negotiated between members of the network and can be adjusted for by subdividing the existing bitcoins into smaller units. It would be possible to inflate bitcoins to the point in which there is a need to divide the currency further than the protocol allows but such a scenario is not necessarily relevant given the size and usage of the currency at this time.

5.4 Means of Legal Tender

At this time no sovereign nation recognizes Bitcoin as a means of legal tender. accepted between two parties.The key feature of a currency and the reason it can be used to represent value and allow for trade between two parties is that the currency is mutually accepted. A nation's centralized currency is backed by its respective government and is the authority on whether or not debts can be settled using said currency. This classifies the currency as legal tender and allows the government to act as an intermediary if payment is rejected by one party or another. A peer to peer system such as Bitcoin has no such authority to determine whether or not the currency has any legal standing in the context of settling debts. Due to the fact that a bitcoin, at this time, cannot be attributed as a means of legal tender it is hard to say if the Bitcoin system can be defined as a true currency.

6 Bitcoin in a Sustainable Culture

A sustainable culture is increasingly becoming the goal of our society. As we face more and more economic and environmental problems in the global market new solutions have to arise. These solutions must offer benefits for the current generation and more importantly provide lasting positive effects for our future generations. A look at sustainability in the global market will offer insight into how an alternative currency such as Bitcoin can benefit a sustainable cultures and also what potential shortcomings the cryptocurrency has.

6.1 Digital Currency

Digital currencies, such as Bitcoin, provide an advantage to current monetary systems as they do not require any physical resources to be consumed. Paper money and coinage, predominant in the global marketplace, require time, energy, and resources to produce through the process of minting. Minting paper money and coinage is rarely cost effective as it is often the case that the cost to produce a single denomination of currency is greater than the value the resulting denomination is worth. For instance, as of 2012 it cost the US government $0.0199 to produce and distribute a penny, worth $0.01. Digital currencies eliminate the need for paper money or coinage and are transmitted and stored as information, an unlimited renewable resource. The process in which these digital currencies are generated, however, can be heavily resource intensive. Such is the case with Bitcoin mining operations.

6.2 Mining Operations

Bitcoin mining operations are essential to the success of the cryptocurrency and require a tremendous amount of effort. The race to generate the next bitcoin block is highly competitive. Miners use not only a single computer but a network of computers that work together to perform the bitcoin mining task known as a supercomputer. Others use a network of GPUs, a component within a computer that displays graphics, specially designed for the sole purpose of mining bitcoins. In essence the more computing power a miner can put towards the mining task the more that miner is to generate the next block (normalized across the network to keep mining fair). Miners either work independently, receiving all the alloted bitcoins, or work in groups in a process known as Pooled Mining. Miners pool their resources together to give the group a better chance at generating the next bitcoin and the rewarding number of bitcoins are split among the participants. Large mining operations are not necessary however, as early miners who ran the mining software on their personal computers sometimes got lucky and were able to be the first to successfully generate the next block of bitcoins. These large mining operations require large amounts of electricity and produce a large amount of heat as waste. Some of this effort is attributed to the worth of a single bitcoin, however much is lost due to the fact that the resulting bitcoin from a mining operation can only prove that the successful operation was performed, which does not include all other guesses.

6.3 Resource Management

Mining operations become obsolete once the total number of bitcoins reaches the fixed maximum number of bitcoins. Operations require a large amount of energy and produce amount of heat as waste product, both of which are not accounted for in the valuation of a bitcoin. Resources will be used during the set amount of time it takes for all mining operations to complete. This value is predictable based on the fixed distribution of Bitcoin and can allow these resources to be managed while they are currently in use. Once resources are no longer required to generate bitcoins the total amount of effort will be reflected in the value of bitcoins in the marketplace. Resource management for the lifetime of the Bitcoin network is not necessary; it is only necessary for the lifetime of Bitcoin mining operations.

6.4 Open Platform

Bitcoin is an open source protocol. Source code, implementation, and all other technologies describing exactly how the cryptocurrency functions are all publicly available. Transparency is key when dealing with a service as secure as bitcoin because it allows users to verify that the service is doing exactly and only what it is stated to be doing. Consequently this means that there are no trade secrets associated with Bitcoin and the entire system can be copied an implemented by anyone else wishing to create their own deregulated digital currency. Competition between Bitcoin and other similar services means that the global market will continue to work to improve upon the service to potentially meet the needs defined by a market pushing for sustainability.

6.5 Networked Infrastructure

The Bitcoin network consists of thousands of nodes all across the world. Each node is an individual user (or group of users) that can conduct peer to peer transactions and received the most recently updated block chain from any or all other nodes. Such a network requires a large infrastructure that can efficiently connect all nodes regardless of their location. Fortunately one such network does exist and the bitcoin network is simply a subset of nodes already connected to one another by the internet. There is no overhead required to create the Bitcoin or any other network and adding a node to the network is trivial. Bitcoin infrastructure maintenance is virtually guaranteed due to the fact that all financial institutions (as well as nearly every other national and international company or service) use the internet to conduct trades and do business. The trade off with Bitcoin relying on the internet is while the network will predictably never go down as a whole, parts are capable of being shut down by those who control access, as well as restrict the use of the infrastructure to disallow Bitcoin. In addition while Bitcoin is free and open for anyone to use it cannot be used if one does not have access to the infrastructure.

6.6 Exclusivity

It is true that Bitcoins are free and open to anyone in theory. In practice there are several minimal requirements those promoting Bitcoin as the world's first universal currency may take for granted. These minimal requirements include being able to understand the protocol enough to use it and a sufficient internet connection to be able to use the service. Bitcoin was created by those who lived and breathed technology and therefore the barrier of entry to them was very low. In contrast an

average person who needs to go to the bank or hire a professional to help with their finances will see the barrier to entry to Bitcoin as insurmountable (if they even understand why they would be interested in the service in the first place). This has led some to believe that Bitcoins are meant for the elite and the tech-savy. Some people are afraid of Bitcoin becoming an exclusive commodity as the existing members raise the barrier of entry higher and higher until they eventually have a control on the currency.

Access to the internet is the absolute minimal requirement to conduct Bitcoin transactions. Internet access used to be a priveldge but it is now considered to be a basic human right. Even still governments and corporations are constantly limiting, restricting, monitoring, and censoring their citizens and customers internet usage. It is common knowledge that oppressive governments can shutdown internet access to its citizens for political or wartime reasons. Internet infrastructure is also subject to physical and cyber attack. Without access to the internet bitcoins become useless.

For Bitcoin to operate truly operate freely and openly, as the protocol sets out to do, these minimal requirements must be addresses. Future alternative currencies relying on technical complexity and internet access will also have to bear these concerns in mind.

6.7 The Third World

Using bitcoins in the third world, or places in the world where internet is nonexistent, is impossible. Companies such as Google are creating initiatives to bring connectivity to those in third world countries that cannot afford the infrastructure required. However, electricity is often missing in these places as well. Bitcoin addresses can theoretically be stored on paper (as they are human readable alphanumeric strings) but trading by means of paper is impractical and the absence of an internet connection makes transactions impossible. If Bitcoin can be considered exclusive in the first and second world and nonexistent in the third world it seems it cannot be considered to be a true global currency.

7 Other Alternative Currencies

Bitcoin is certainly not the only alternative currency that exists in the global market and is certainly not the last. Alternative currencies have proven to be useful and effective in the current market and in the future they prove to have an even larger impact. It has been the focus of this paper due to its popularity, functionality, and potential impact on alternative currencies as a whole. Bitcoin

is an open source platform allowing several alternative digital currencies to exist that all share the same (or very similar) technology. Cryptographic and digital currencies are not the only alternative currencies being considered in the current global market and developing or future technologies may lead to an even more beneficial and efficient means of communication wealth and value in the future. The two most interesting of these proposed alternative currencies are the notions of energy and information based currencies.

7.1 Bitcoin Alternatives

Bitcoin has many competitors and companion currencies that exist in the market today, albeit less popular. The three most notable of these examples are LiteCoin, FeatherCoin, and PrimeCoin. It is interesting to note that while the technology behind crypto-currencies remain nearly identical to one another the foothold each option is able to create in the marketplace is largely tied to factors external to the benefits of the currency itself. These factors include the time at which a currency was released compared to each other, a currency's popularity in the marketplace, the media and legal attention a currency has received, and an overall preference of users in the global market. It is important to note Bitcoin remains to be by far the most widely use, recognized, and accepted cryptocurrency available on the market today.

Litecoin is perhaps the most well known alternative to Bitcoin, derived from the same open protocol but several differences the developers hope users will see as benefits over the original cryptocurrency. The time to generate a block of litecoins is 2.5 minutes, 4 times slower than that of Bitcoins, allowing for faster transaction confirmation. Litecoin uses a different proof of work algorithm known as scrypt originally intended to avoid giving the advantage to GPU miners over CPU miners (an advantage present in Bitcoin) but it has since been realized that GPU mining is nearly an order of magnitude more efficient than CPU mining in Litecoin's implementation. The total number of litecoins available to the network is capped at 84 million litecoins, four times the total number of bitcoins available. Both litecoins and bitcoins can be subdivided into 100 million sub-units.

Feathercoin, a cryptocurrency based heavily on Litecoin, shares the same hash function and a time to generate each target block of 2.5 minutes as its parent. The network difficulty of Feathercoin is adjusted every 504 blocks as opposed to Litecoin and Bitcoin's slower 2016 block to allow for the increased speed in which blocks (and thereby transactions) are generated (processed).

While Litecoin and Feathercoin are cryptocurrencies based off of the open protocol behind

Bitcoin, Primecoin is based on cryptography but does not use a strong hash function. Instead, Primecoin relies on finding long Cunningham chains, a sequence of prime numbers, for proof of work. Cunningham chains are used in other cryptology applications thereby providing more value outside of the use of primecoins themselves, unlike Bitcoin's SHA-based proof of work system which has no value outside of its own network. Primecoin blocks are generated at a rate 10 times faster than that of Bitcoin blocks meaning transactions are also confirmed approximately 10 times as fast.

7.2 Energy Based Currencies

The need for a global unified currency is a need shared by environmentalists who feel that the current system of commercial economics has many shortcomings when dealing with monetary units as opposed to real physical units. Monetary accounting systems do not account for environmental processes, non-renewable resource assets, or the lasting effect of a good or service on the environment. Environmentalists believe that this prevents policy changes due to the resistance of the commercial economics sector to act on factors that are not present in their monetary system. As it is not in the interest of the financial sector to change, environmentalists believe, it is up to the scientific community to develop a monetary system that represents both human and natural processes. Fortunately the global market is in need of unified currency to facilitate the need for simple and efficient international trade. One commodity that is universally produced and consumed by every nation on the planet is also measured in meticulous detail and vital to every economic process - energy. Energy based currencies represent the work already performed in a process as well as the work potential of a process or resulting processes and is already produced by every nation in a wide variety of sources. Commercial, political, or environmental activity would not subject the currency to any evaluation changes as the energy consumed is the true value of a good and the energy produced is the true value of a service. The use of an energy based currency is inhibited by the lack of a standard measurement and the lack of technology to provide a means of implementation. Scientists could help economics in determining which is the best unit to base an energy currency on, perhaps kilowatt hours as it is the best known and most widely used measurement. The benefit of using a kilowatt hour as a basis of a currency is that a kilowatt hour (or any other energy measurement) is the same in every nation thereby eliminating the need for speculation or conversion between nations and the amount of energy a kilowatt hour represents does not change over time. Energy based currencies offer a unique approach to a truly global and unified currency solution.

8 The Future of Money

Our current monetary systems have allowed for massive economic growth. This growth has created economic benefits but has done virtually nothing to solve the problems of sustainability in our culture. Currency relies on regulate by governments and thus any economic reform is treated as a political policy change. Domestic and international policies and the desire of politicians to stay in power prevent the sort of changes needed in our monetary system to be able to solve the long term problems our society has. Humans have a difficult time placing long term benefits over short term gains.

We must look for sustainable solutions in the global marketplace in order to combat the ecological and environmental problems of the present and more importantly in the future. Our current monetary systems to not take these problems into account therefore these issues are externalities that are far too costly to attempt fix. Environmental problems must be internalized into our monetary system in order to find the most efficient and cost effective solutions.

Any regulated currency is going to be limited by the wants and needs of the regulating body and can only adjust in accordance to the policies of the regulator. The value of a regulated currency, in a market place that no longer uses a gold standard (or any other standard of value for that matter), is directly linked to the power and authority of the regulating government behind the currency. This means that while the value of currency may be strong in the short term, political and economic changes in one nation can have a rippling effect on the value of all other currencies in the market. This instability in value is damaging to a marketplace that wishes to focus on sustainability as the value of economic problems remains constant while the solutions can become more costly.

Alternative currencies may hold the answer to these problems. Deregulated currencies, such as Bitcoin (and its alternatives) and the proposed energy based currencies, have the opportunity to root their value in something that will remain constant regardless of political or economic changes. In the case of energy based currencies the environmental changes and problems are in fact internalized in the value of the currency itself. This means that finding cost effective solutions for energy based currencies in turn create environmentally friendly solutions, thus creating a more sustainable culture. The global market is dominated by information and digital transactions so it makes sense to find a solution that is created on the backbone of the share of information. After all, currency is simply the means in which we exchange information on the value of a good or service. When the value of a currency includes no only the perceived value, but the inherent value, and the value of

the social, political, economic, and environmental problems all at once, then we may have found a solution that achieves the goal of sustainability.

What does this mean for the future of money, or monetary systems in general? At the moment regulated and centralized currencies have far too much momentum to be done away with overnight, if they even need to be completely removed at all. Bitcoin being the example, alternative currencies have shown that they can present some great advantages over regulated currencies and are capable of gaining a strong foothold in the global market. It is clear that these alternatives have disadvantages but as more and more alternatives come into existence and are tried the strong these alternatives will become. Some believe Bitcoin will be the answer to all of our problems, others believe alternative currencies will never be fully accepted. It is clear, however, that alternative currencies and solutions may be necessary for the global market to start turning its attention towards sustainability.

9 Conclusion

The role of alternative currencies in the global marketplace has been defined as a means to escape the limitations of established regulated currencies and offer benefits for not only economic problems, but political and environmental problems as the global market itself works towards a goal of greater sustainability. Alternative currencies allow a way for the global market to examine the value of its currencies and determine how value is given to a currency in the first place. As it stands, the global market may never rid itself of regulated currencies, but the need for deregulated currencies is growing, especially in the digital era.

Bitcoin is by far the most popular and successful alternative digital currency in the marketplace today. The crypto-currency gets its strength by being an anonymous, peer to peer, deregulated currency that is transferred purely digitally with its value rooted in proofs of work. In the information age, as digital solutions become more and more prevalent, the power and value and value of digital currency solutions will increase. However, it is important to note that while the world is rapidly moving towards a complete digital infrastructure, the global market as a whole is very far away from being capable of adopting a complete digital solution. Bitcoin, while it may never replace cash or the gold standard, has found a niche in the global market and will continue to grow.

Sustainability as a goal for the global marketplace is one that will require a change in our monetary systems, or at least in the way economic policies are made. At the moment it is nearly impossible to create policy changes with environmental aspects solely in mind as the cost of envi-

ronmental problems are not reflected in our currencies. In order for these problems to be solved the must be internalized and the costs must show up in the way we represent the value of our currency. Ultimately, the solution will come down to how we place value in our money.

What gives money its value? Before currency was used value was represented by tangible assets, the value of which was negotiated between two parties. As trade grew and became international, standards were formed on mutually accepted commodities of value, such as gold and silver. Paper money was then created as a more convenient means of exchange and was directly tied to the precious commodities, thus retaining the equal value, but requiring trust in a central authority. Once these commodity standards were removed from currencies their value was tied only to the trust in the central authority and therefore only the perceived value of the currency. Our current monetary systems are not linked to anything of value other than their mutual acceptance and their comparability. But these are regulated currencies, deregulated currencies hold their value in something either tangible or provable. In the case of Bitcoin, the digital crypto-currency, the currency holds its value through a provable amount of time and effort such that the representation of the currency is also the direct representation of the value. Energy based currencies take the concept of inherent versus perceived value one step further in that the actual use of the currency is the exchange of the true value of any good, the sum of the energy required to create it as well as the potential energy of the good. In this case, value is clearly defined by all parties. Ultimately money is valuable, whether it be inherent or perceived, by the quantifiable ability for it to be used in the exchange of goods and services.

References

[1] Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System* 2008 http://bitcoin.org/bitcoin.pdf

[2] Percival, Colin. *Stronger Key Derivation Via Sequential Memory-Hard Functions*. Retrieved 13 October 2013. http://www.tarsnap.com/scrypt/scrypt.pdf

[3] Gibson, Steve. Merritt, Tom. *BitCoin Cryptocurrency* (10 February, 2011) https://www.grc.com/sn/sn-287.txt

[4] Bordo, Michael D.; Dittmar, Robert D.; Gavin, William T. (June 2003). *Gold, Fiat Money and Price Stability* (PDF). Working Paper Series. Research Division Federal Reserve Bank of St. Louis.

[5] Litecoin.org" *Litecoin.org, April 2013* http://www.litecoin.org Retrieved 13 October 2013

[6] King, S. (2013, July 7). *Primecoin: cryptocurrency with prime number proof-of-work*. Retrieved from http://ppcoin.org/static/primecoin-paper.pdf

[7] Ars Technica, *How the feds took down the Dread Pirate Roberts* (October 3, 2013). Retrieved 16 October 2013. http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/

[8] Orsini, Lauren. *I Bought Bitcoin In Person And Here's What Happened* (October 23, 2013). Retrieved 23 October 2013. http://readwrite.com/2013/10/23/i-bought-bitcoin-in-person-and-heres-what-happened

[9] Lee Hutchinson (Sept 17 2013) *Diablo 3 to permanently remove its auction houses in March 2014* Retrieved 1 November 2013. http://arstechnica.com/gaming/2013/09/diablo-3-to-permanently-remove-its-auction-houses-in-march-2014/

[10] Grady, DB (July 2, 2012) *The Toadstool Exchange: An Examination of 5 Video Game Currencies*. Retrieved 1 November 2013. http://mentalfloss.com/article/31083/toadstool-exchange-examination-5-video-game-currencies

[11] FinCEN, USA.gov (May 2013) *Money Services Businesses Home*. Retrieved 15 October, 2013. http://www.fincen.gov/financial_institutions/msb/