MS thesis

Financial Economics

Is Bitcoin money?

An analysis from the Austrian school of economic thought

Ísak Andri Ólafsson

Birgir Þór Runólfsson, Ph.D.

Department of Economics

HÁSKÓLI ÍSLANDS

June 2014

Is Bitcoin money?

An analysis from the Austrian school of economic thought

Ísak Andri Ólafsson

M.Sc degree thesis in Financial Economics

Advisor: Birgir Þór Runólfsson, P.hD.

Department of Economics

School of Social Sciences at the University of Iceland

June 2014

Is Bitcoin money?

This is a 30 ECTS credit thesis for a M.Sc. degree in Financial Economics, School of Social Sciences at the University of Iceland.

Printing: Prentmet

Reykjavík, 2014

Preface

This thesis is a 30 ECTS credit final project for a M.Sc. degree in Financial Economics. The advisor of this project was Birgir Þór Runólfsson, Ph.D. I sincerely thank him for his advice and suggestions. I thank my friend Candice Michelle Goddard for invaluable proofreading (again). Finally, I thank Kristbjörg Gunnarsdóttir for feeding me while I was writing, and for her unconditional support and understanding.

Abstract

This thesis aims to explore whether digital crypto-currencies such as Bitcoin can be considered money from the perspective of the Austrian school of economics. It begins by describing the functions and design of the Bitcoin system in detail. Other innovations that either build on or improve Bitcoin will be explained as well. The functions of money are then defined from the origins of money, providing a categorical approach toward a comparison between Bitcoin and incumbent money. The risks and complications of Bitcoin will be discussed in this thesis with an emphasis on the role of policymakers. One of the main reasons why Bitcoin has yet to be regarded as money in a traditional narrow sense is the barrier generated by network effects, in particular, the presence of excess inertia. Other risks and complications that are present within the context of this thesis will also be discussed.

A significant part of the criticism of Bitcoin as a medium of exchange that comes from the Austrian school arises because Bitcoin does not seem to follow the regression theorem Mises put forth to explain the emergence of money. An attempt will be made to reform the regression theorem so it accounts for digital innovations such as Bitcoin, if proven unsuccessful, another perspective is offered in which Bitcoin does not violate the theorem. When the complication of the regression theorem is solved, it is possible to address whether Bitcoin is money or just a secondary medium of exchange.

From an Austrian perspective, Bitcoin is not money, however, an argument will be made that Bitcoin is an imperfect form of memory, one which fits somewhere in between commodity money and fiat money, a synthetic commodity money. The possibility of Bitcoin substitutes to incite an expansion of the money supply will also be analysed from an Austrian perspective.

Table of contents

1 Introduction

Krüger and Godschalk (1998) wrote that technological progress and innovation in payment systems result in decreased transaction and information costs and that this could lead to the viability of alternative currencies[1] (Krüger & Godschalk, 1998).

Bitcoin was developed by Satoshi Nakamoto, a pseudonym for an individual or a group of people. The peer-to-peer network described in the paper was a breakthrough, because it did not rely on trust between agents but rather mathematics, making it the first decentralized digital medium of exchange to solve the problem of double spending. This has understandably generated a lot of controversy and public exposure. To top it off, the deflationary nature of Bitcoin goes against the grain of mainstream economics to some extent. This thesis is meant to examine the underlying structure and functions of Bitcoin, find a way to decide whether it is money from an Austrian economic perspective, and finally to provide a comprehensive overview of the complications and regulations surrounding Bitcoin. To answer the research question, it is first necessary to understand how Bitcoin works, both to acquire insight into how the double-spending problem is solved and to understand how Bitcoin can offer many of the things it can as a medium of exchange. One of the qualities of Bitcoin is the anonymity the system provides, which will be discussed further along with introducing the concept of Zerocoins, an innovative addition to increase the anonymity of Bitcoin users.

Another improvement that is based on the Bitcoin system, called Peercoin, will be introduced as well. This is done in order to minimize the risk of this thesis becoming obsolete in the near future, as most of this thesis applies just as well to other crypto-currencies, such as Peercoin. To elaborate further, Peercoin could be a successor to Bitcoin, but only time can tell which of the dozens of crypto-currencies available presently will prevail, if any. Bitcoin is deflationary by nature as well as using a proof-of-work system that has been criticized for wasting electricity. Peercoin has a built in,

[1] Translated by Peter Surda from the original text: „Der technologische Fortschritt und Erneuerungen im Zahlungsverkehr führen zu einer erheblichen Senkung der Transaktions- und Informationskosten. Bedingt durch diese Senkung kann die Alternative der Nutzung unterschiedlicher Währungseinheiten wieder aus wirtschaftlichen Gründen eine Renaissance erleben“ (Surda, 2012, p. 32).

steady inflation rate of 1% and utilizes a resource efficient verification method called proof-of-stake.

Next, the origins of money are traced to find the three defining functions of money, as a store of value, liquidity, and transaction costs. An Austrian perspective is also examined, where money is the most universally liquid commodity and other functions of it are provided from that premise. From there, Mises' regression theorem can be introduced. Some have argued that Bitcoin violates the theorem but a reformation that allows for Bitcoin and other technological advances will be shown in this thesis. Another perspective will also be established, which builds upon the reformed theorem by utilizing the premise of the original regression theorem. More specifically, although non-monetary demand is necessary for the emergence of money, it is not necessary to sustain it.

After the theorem has been redefined, so the seemingly spontaneous value of crypto-currencies does not violate it, it is possible to investigate further whether Bitcoin is money or just a medium of exchange. A concept of money as memory is introduced, as Bitcoin, and other crypto-currencies are the closest thing to being a perfect memory to date, as defined in the chapter five. From that notion it can be established that Bitcoin as imperfect memory cannot be placed as either commodity money or fiat money. Instead, a proposition of Bitcoin as synthetic commodity money is supported, making Bitcoin a unique hybrid of an artificially scarce medium of exchange that does not possess any monetary value. Inelastic money supply in a fractional reserve system will then be discussed from an Austrian economic viewpoint, using a Keynesian approach to provide balance, or at least a constant, to the discussion.

The problems associated with Bitcoin will be analysed and their significance assessed. The most prominent of those problems being the complications regarding network effects and excess inertia. Finally, a brief overview of the regulatory history of crypto-currencies within The Financial Crimes Enforcement Network (FinCEN) along with a guidance of the correct way to approach the regulation of crypto-currencies will be put forth.

It must also be noted that the term crypto-currency is a misnomer, as crypto-currencies are not universally agreed to fit within the strict definition of currency. In a

similar vein, the term synthetic commodity money, although not necessarily a misnomer, does not fall into the category of money in the narrow sense. Finally, when Bitcoin is written with a capital letter, it stands for the design, system, protocol, or network of Bitcoin while bitcoin with a lower-case letter stands for medium of exchange units of bitcoins.

2 What is Bitcoin?

Satoshi Nakamoto published the original Bitcoin paper in November 2008 (Nakamoto, 2008). In the paper, a method to use peer-to-peer (p2p) networking to create a cryptographic transaction system was explained in detail. In January of 2009, the original Bitcoin network was created from the first open-source Bitcoin client. Bitcoin utilizes a decentralized authorization of payments that leads to a pseudo-anonymous transaction process. These transactions are protected against double spending by a verification method called proof-of-work, a central characteristic of Bitcoin. When users of the network complete the verification process (known as proof-of-work) using computational power, they obtain bitcoins (BTC) as a reward. This process is known as *mining*.

2.1 The double-spending problem

The double-spending problem had proven a hindrance in the implementation of a decentralized digital medium of exchange that would not require the aid of an intermediary, until Bitcoin was created. Before Bitcoin existed, a third-party intermediary was always required to oversee the transaction of two people over the internet. This inconvenience was a necessary step because of the way computer programs function.

If Alice wanted to send Bob an arbitrary amount of money before the invention of Bitcoin, she would need to use an intermediary such as Paypal. Paypal and other third-party intermediaries, like MasterCard, keep a ledger of all their clients' accounts. This was necessary (and still is when not trading with bitcoins) to ensure that double spending cannot occur. Without those third-party intermediaries, and without the Bitcoin system, the only realistic way of spending digital money is by using a system that keeps money as files on a computer, or in a personal balance sheet confined within a computer for example. The file system could work like this; a file is sent that, when opened, automatically transfers money from the buyer's account into an account the file opener chooses.

If Alice wanted to send Bob money through the system, she could simply send the money file. The problem is that computer files can be duplicated with ease, leading to

the core issue; Alice could just as easily send Charlie the very same money file she sent Bob earlier. The result would be that Alice would end up with twice the amount of goods she can actually afford while either Bob or Charlie gets a used file. Who gets the worthless file depends on who tries to use the file first, if Bob uses the file immediately and gets all of Alice's money transferred into his account; there is no more money in her account for Charlie (Brito & Castillo, 2013, pp. 3-4). This is the essence of the double-spending problem. Bitcoin's design prevents it by making the ledger, or the opening of money files, public. By doing so, in addition to the proof-of-work verification system, it is almost impossible to double-spend bitcoins.

To double-spend bitcoins, it is first necessary to create a fork (or a split) in the block chain, the public record-keeping device maintained by the network (it will be explained later in detail how the block chain operates). The reason this is nearly impossible is that when two blocks are published nearly simultaneously (so a fork is created), the nodes are programmed to follow the block chain with the greater proof-of-work difficulty and discard the others. This ensures that the record keeping is provided by a single block chain that is accepted by all users. The forked block chains integrate into the main block chain within a few blocks' time (Barber, Boyen, Shi, & Uzun, 2012, p. 403). To double-spend bitcoins would thus require a 51% attack (more generally known as a Sybil attack[2]) on the proof system, which is extremely hard and, in fact, has been shown to have less expected value than simply using the resources necessary in legal operations (Bitcoin Wiki, 2013) (Andresen, 2012). The more valuable a bitcoin becomes, the higher the incentive for illicit users to make a 51% attack. However, the more valuable a bitcoin becomes the incentive to mine grows as well, which increases the number of miners and making a 51% attack harder. This means that the demand for security increases the incentive to mine.

An important externality resulting from the solution to the double-spending problem is that Bitcoin becomes not only a decentralized payment network, but also a full-fledged medium of exchange, since the network unit of accounts are denoted in bitcoins

[2] An attack where some kind of a reputation system is subverted by forged identities in peer-to-peer systems (Miers, Garman, Green, & Rubin, 2013, pp. 8-9).

rather than dollars like Paypal and other similar intermediaries (Brito & Castillo, 2013, p. 4). Bitcoin as a medium of exchange has many alluring qualities that are worth mentioning. For example, there are lower transaction costs within the Bitcoin system than there are with other types of electronic payment methods. This can be attributed to the lack of a third-party intermediary. With cheaper transactions and a theoretical ability of quicker transactions as well, the possibility of micro transactions becomes feasible (Brito & Castillo, 2013, p. 10).

2.2 Transaction costs and credit cards

There are no inherent transactions costs when utilizing bitcoins. The costs mostly come from optional fees for verifying transactions. There are however three conditions that must be met in order for a transaction to be sent without fees. It must be smaller than 1,000 bytes (1 kilobyte is 1,024 bytes) which is not a problem at present, since transactions average 0.5 kilobytes. This might however become one of the biggest setbacks of Bitcoin in the future, as every transaction, no matter how small, is replicated among many nodes and needs to be stored in the block chain (record keeping device) forever. This is not free and some are inclined to say that micro transactions pollute the block chain, encouraging users to bypass the Bitcoin system when micro transactions need to be conducted. The second condition is that all outputs of the transaction are larger than one hundredth of a bitcoin. This should not be a problem, since there is no real reason for a user to pay with multiple wallets, each payment being less than 0.01 bitcoins (Bitcoin Wiki, 2014). The third condition is that the transaction must have a certain level of a predefined priority. This priority is calculated by taking a value-weighted sum of input age and then dividing that sum with the byte size of the transaction. In another format, this can be shown as:

$$Priority = \frac{Input\ value\ in\ base\ units * Age\ of\ input}{Size\ of\ transaction, measured\ in\ bytes}$$

Transactions need to have a priority above 57,600,000 to avoid the enforced limit. This seemingly arbitrary number is found by using a day old bitcoin in an environment where there are 144 blocks solved per day and an average transaction size of 250 bytes (Bitcoin Wiki, 2014).

If those conditions are not met, a standard fee of 0.0001 bitcoin is set for all low priority transactions, transactions that are smaller than 1,000 bytes and transactions that have outputs lower than 0.01 bitcoins. The 0.0001 bitcoin fee is a standard one (and therefore a minimum one as well) set by the Bitcoin program, it can be changed however if a quicker verification is needed to increase the incentive to mine. Another 0.0001 bitcoins are added for every 1,000 bytes. In the future, it is likely that the standard size of transactions will rise because of a longer block chain, thereby increasing transaction fees. This could be problematic for the future of Bitcoin, especially when the transactions become closer and closer to the limit of one megabyte (1,024 kilobytes), effectively raising the transaction fees tenfold. A simple solution would be to eliminate the artificial minimum bar of 0.0001 bitcoins fee and let the free market designate a new price that would, in all likelihood, be lower (Bitcoin Wiki, 2014).

There are a number of other differences between Bitcoin and other types of electronic payment systems. Among other payment systems, electronic credit card payments are both very prominent and a clear contrast to bitcoins. The credit card system charges businesses the transaction cost while Bitcoin charges the users (albeit a much lower fee). One of the first things a newly established business needs to do is create a unique merchant account with every credit card firm. Through the merchant account, businesses pay customer-service fees, interchange fees, transaction fees and a variety of authorization fees. The cumulative sum of these fees succinctly creates a barrier-to-entry for entrepreneurs. This is still preferable to the alternative of boycotting the credit card firms by not making a merchant account, since a lot of business will be lost given how widespread the use of credit cards is (Brito & Castillo, 2013, p. 11).

Bitcoin is different from the infrastructure described before, as the users themselves pay the (possible) transaction fees. By doing so, Bitcoin effectively eliminates the costly charges that inevitably follow third parties. It does so without failing to facilitate the previous service managed by credit card firms because of a lack of central authority. A venture capital named the Founders Fund led by Peter Thiel (the cofounder of Paypal), invested US$3 million in a payment-processing company called BitPay (Simonite, 2013). BitPay was invented in 2011 and is currently trusted by over 30,000 businesses and

organizations (BitPay, 2014). In January of 2014, that number was just above 20,000, and growing at the rate of about 1,000 new merchants per week (Southurst, 2014). One of the co-founders of BitPay, Anthony Gallippi, has stated that one of the reasons BitPay has been doing so well is because credit cards were never designed to be used on the internet and it shows, Visa spends billion dollars a year funding their fraud prevention facility, Bitcoin makes these measures obsolete (Olanoff, 2013).

Bitcoin has thus had an immediate effect on the market where many business owners, especially those in small businesses, have turned at least partly to Bitcoin when processing transactions (Brito & Castillo, 2013, p. 11). Although the main concern of these business owners is to lower transaction costs, others are adopting Bitcoin for the increased efficiency and speed of transactions (Reutzel, 2013). Still others, who have difficulty finding a payment processor willing to work with them because of their high-risk status or otherwise undesirable track record with the credit card companies, are turning to Bitcoin merchant service providers like BitPay as an affordable and convenient alternative (Reutzel, 2013).

2.3 Verifying transactions using proof-of-work by mining

Proof-of-work (some crypto-currencies prefer to use other systems, which will be discussed later) allows the clearing authority to be completely decentralized and not dependent on trust or the premise that humans act without error. The transactions are grouped together for processing (authentication). For authentication to take place, a computation of a complicated cryptographic problem must be completed. Users on the network who decide to engage in the brute force guesswork that is needed for the solution, are mining.

An algorithm revises the rate of block creation whenever 2,016 blocks have been solved. It does so by altering the length of a digit chain composed of zeroes in the proof-of-work (Nakamoto, 2008, p. 3). The result is that a new block is mined approximately every ten minutes. If the average solving time diverts from ten minutes after a set of 2,016 blocks, the algorithm swiftly adjusts the difficulty so that the solving time becomes approximately 10 minutes again (Nakamoto, 2008, p. 3).

The reason behind the ten-minute intervals is to solve the Byzantine generals' problem[3]. The problem has to do with synchronization and is a subject that could fill a thesis on its own. In short, the delay is necessary to make sure that everyone within the system is working with the same information (Gibson, 2013).

The reason for using terms such as *miners* and *mining* is that when a *block* (a group of transactions) is authenticated, the first user to have successfully done so (the *winner*) receives bitcoins after sharing the solution with everyone else on the network. He does so by adding the authenticated transactions to the block chain (the public record of every single transaction since the creation of Bitcoin) which all users have access to through the client. The winner of each block can be an individual or a shared computer network that then shares the mined bitcoins. The bitcoin reward is currently 25 BTC and will be halved every 210,000 blocks or approximately every 4 years (Bitcoin Clock, 2014). The double-spending problem is then elegantly solved; every user can observe the block chain, making it simple to affirm the ownership of bitcoins and impossible to spend the same balance twice (Luther & Olson, 2013, p. 5). When the last Satoshi (a 0.00000001 fragment, the smallest amount a bitcoin can be divided into, named after its creator) will have been mined in approximately the year 2140, the total amount if bitcoins will amount to 21 million. After the year 2140, according to the adjusting algorithm, there will be no more bitcoins to mine. Instead, the incentive for miners to keep mining, thus upholding the verification system, comes solely from transaction fees. These fees have been introduced to the Bitcoin network but have not become a standard so far, although some people will pay additional fees for quicker verification times (than the usual maximum of around 10 minutes) (Brito & Castillo, 2013, p. 7). As of now, 12,747,825 bitcoins are in circulation and that number is growing in a linear predictable manner, thanks to the algorithms used in the Bitcoin system (Blockchain, 2014).

[3] Bitcoin only solves the Byzantine generals' problem under the assumption that possible attackers are computationally limited, in other words, that they do not possess over 51% of the total hashpower. Because the problem is solved in a probabilistic way it is not a valid solution to the two generals' problem.

2.4 What does Bitcoin mean for business owners?

Andreas Antonopoulos, a Bitcoin analyst, points out that the merchant service providers managing bitcoins, like BitPay, are most likely only a temporary economic structure. Since merchant providers must abide by laws and regulations, they are forbidden to handle transactions relating to illicit activities. Because of this, individuals who want to attach their business to industries that are connected to illegal substances or other legally reprehensible money markets are forced to search for yet another way to conduct their transactions. The most straightforward way to do so is by cutting the intermediary altogether, accepting payments directly to a Bitcoin wallet that the merchants have set up themselves. Bitcoin offers that function without cost. It might be said that these service providers have the purpose of introducing bitcoins as a viable alternative medium of exchange, rather than representing some sort of an additional service (Reutzel, 2013). When speculating the long-term viability of these services, they might prove to be a sustainable practice. After all, by accepting credit card payments, businesses are taking a risk that might prove to be unnecessary in the future. That risk stems from charge-back frauds (also known as friendly frauds), which are becoming increasingly common as the user base of the internet becomes larger. These payment reversals are initiated by customers of the payment service on the false claim that a product or a service has not been delivered or applied. They can be thought of as reverse credit card transactions. The inherent problem with this kind of fraud, as with so many others, is that it is easy to request a charge-back but very hard for businesses to prove that it has done work or delivered a product (Maltby, 2011). Merchants that utilize these services, such as paypal, are therefore at risk of losing payments for items and the items themselves. To add insult to injury, they are required to pay a charge-back fee in most cases (Brito & Castillo, 2013, p. 12).

The Bitcoin system is structured in a way that makes charge-back frauds impossible. When a transaction is made, it is made for good. Whether this is good or bad is up for debate. When the possibility of charge-backs is gone, in addition to the deregulatory environment that defines Bitcoin, and the need for exchanges that work outside of laws and property rights (since bitcoins are not strictly defined as property), it is a prime target for other types of scams. With this knowledge, it is easy to estimate that even though business owners prefer bitcoins or any type of payment system that rids them

off the perils of charge-back frauds, although not charge-backs in general as the feature is desirable when establishing consumer trust, consumers in general will prefer credit cards. The reason is two-fold. First off, the credit card companies charge the business owners transaction fees while Bitcoin charges the customers themselves. Secondly, credit card companies provide a safety net with the same features some consumers are abusing, such as the charge-back system. The charge-back system is a necessity because it protects the customer against errors made by merchants and against corrupted businesses (Brito & Castillo, 2013, p. 12). Even though these benefits of credit card usage will still attract customers, Bitcoin is an alternative that customers will utilize for different reasons, ranging from concern of anonymity to liberal idealism to charge-back fraud prevention, especially in unofficial transactions such as online sales (Brito & Castillo, 2013, p. 13).

There are positive externalities that serve as an added incentive for consumers to embrace Bitcoin. When a business accepts bitcoins and trades with consumers who accept bitcoins in return, its overall profit margins rise, since the fees become trivial (Paul, 2013). This in turns creates an opportunity for the business to lower its prices and thereby sharpen its competitive edge, so to speak (Brito & Castillo, 2013, p. 13).

On a similar note, if bitcoins were to be accepted globally as an alternative currency the positive effects could prove to be colossal, as Bitcoin enhances certain aspects of traditional currencies that open up opportunities because of increased efficiency. One of those improvements would be a great decline in service fees when transferring remittances and at an increased speed (Silver-Greenberg, 2012).

The average fee the *bricks and mortar* wire transfer services, such as Western Union, charge for the transfer of funds between countries is 8.36%, as of March 2014 (The World Bank, 2014, p. 1). Bitcoin charges between 0.0001 to 0.0005 BTC for transactions, which is far less than traditional wire transfer services can offer, especially since most of them have standard fees as well that are not percentage based (Silver-Greenberg, 2012). This has attracted investors that are interested in improving the money transfer system currently employed (Simonite, 2013). Investors are not the only ones Bitcoin has attracted, as the corporations Bitcoin is out-performing, such as Western Union and MoneyGram International, have started contemplating whether they should offer

transaction solutions in the future that contain possibilities related to Bitcoin. There are however no immediate plans to do so (Johnson, 2013).

2.5 Data transfer using the Bitcoin network

One of the many innovative applications that are possible with the use of the Bitcoin system is the ability to transfer other things than just bitcoins. Because the Bitcoin system is in its essence an open source peer-to-peer data transfer system, it is easy for programmers to apply the digitally available schematics to create useful legal and financial services that utilize the Bitcoin system. Bitcoins are, like many other products of the digital age, just packets of data. The Bitcoin network sends these packets back and forth. The system is open source, which means that the packets can easily be converted into something other than bitcoins such as classified information, stocks, bonds, and even bets (Brito, 2013). A few of the things built in the Bitcoin protocol is ways to manage disputes by means of mediations, assurance contracts and micro-payments (Brito & Castillo, 2013, p. 18). The conversion of packets has generated a lot of technological innovation. It could enhance Bitcoin's stability and security by adding another layer of protocol over the base protocol (Willett, 2014). Another way to utilize the option of transferring packages is a very secure way of sending encrypted messages back and forth without relying on any centralized authority (Warren, 2012).

Colored Coins is a concept that uses an additional protocol layer that creates a new set of information about coins (Bradbury, 2013). Depending on what attributes have been assigned to a coin, he becomes a certain color and by doing so changes the coin into a token for other financial instruments and goods, such as bonds, shares and IOU's[4] (Bradbury, 2013). Color Coins is just one example of many innovate systems designed from the Bitcoin source code, some of which will no doubt become an increasingly larger part of our daily lives.

[4] The abbreviation comes from the phrase *I owe you* and usually represents an informal document acknowledging debt.

2.6 Anonymity of crypto-currency users

The transactions within the Bitcoin network are only pseudo-anonymous (or quasi-anonymous) because of a mechanism called public-private key technology.

The public-private key system functions by making Alice use her private key to verify that she is the rightful owner of her *Bitcoin wallet*, a term for user accounts, when she wants to buy something (Nakamoto, 2008, p. 2). Alice then identifies Bob by his public key when making a transaction. Once he is identified, the Bitcoin client sends out an authorization request that the transaction is valid. When it has been authenticated by other users, who do so by mining, all users of the network are notified by an update in the block chain that functions as a record keeping device. The update contains the information that Bob is now the new owner of Alice's bitcoins that were used in the transaction. Everyone has a verified and an updated record that has a complete list of transactions in the Bitcoin system (Brito & Castillo, 2013, p. 5)

The act of owning bitcoins is completely anonymous and they can be transferred anonymously, given that the transaction is not dependent on physical delivery or communication. When bitcoins are bought, either through an exchange or with cash, some information must be revealed, whether that information contains the person's physical identity, an address, or a bank account number. This applies as well to the act of using bitcoins to buy goods or services (Luther & Olson, 2013, p. 5).

On one hand, there are cash transactions that are completely anonymous in theory and on the other are credit transactions through means such as banks or Paypal, in which both users are identified. Bitcoin falls somewhere between these extremes, when Alice pays Bob in bitcoins, there is no third-party intermediary that acquires information about their exchange. Their anonymous transaction itself, however, is fully transparent and in plain sight of all Bitcoin users. There are some ways for users to mask their identity but around 40% of Bitcoin users can be identified from simply observing the public block chain and analysing it with behaviour-based clustering techniques (Androulaki, Karame, Roeschlin, Scherer, & Capkun, 2013, p. 35).

The physical location of Bitcoin users can be linked to them directly through their IP address (internet protocol address), since the IP address of all connected users is broadcasted by the network every 24 hours (Bitcoin Wiki, 2013). A research conducted

by the University College of Dublin in Ireland showed that there was an inherent limit to the amount of anonymity when using bitcoins (Reid & Harrigan, 2011, p. 3). The research also stated that when agents that had access to information not usually regarded as public, such as bank account information or shipping addresses, that the already limited anonymity, becomes even more limited (Reid & Harrigan, 2011, p. 3). Users can however protect their identity by several means, mostly by utilizing options available through the Bitcoin system. These options are listed here (Federal Bureau of Investigation, 2012, p. 5):

- They can create and use a new Bitcoin address for each incoming payment.
- Route all Bitcoin traffic through an anonymous proxy.
- Combine the balance of old Bitcoin addresses into a new address to make payments.
- Use a specialized money laundering service.
- Use a third-party e-wallet service to consolidate addresses. Some third-party intermediaries have the option of creating an e-wallet that allows users to consolidate multiple Bitcoin addresses and easily store and access their bitcoins from many different devices.
- Agents can create Bitcoin clients for increased anonymity (such as allowing users to choose which Bitcoin addresses to make payments from), making it easier for technically challenged users to anonymize their Bitcoin transactions.

2.6.1 Zerocoin - an innovative addition to Bitcoin

In 2011, the spending of 25,000 stolen bitcoins was traced (Reid & Harrigan, 2011). Although the possibility of tracing proved to be beneficial in this particular example, it is also a monument to the fact that it is possible to violate the privacy of Bitcoin users by tracing their spending habits (Lee, 2011). In the near future, there is even a remote possibility of network topology being applied to analyse the transaction record of Bitcoin, which might lead to partial de-anonymization of the Bitcoin network (Miers, Garman, Green, & Rubin, 2013, p. 1).

The users of Bitcoin are generally aware of this lack of true privacy and accept that even though their identity is relatively well hidden, their transaction history is not. Some users have therefore opted to use online crypto-currency laundry services, in which the service provider offers to exchange their coins with someone else's. The fact that

Bitcoin is decentralized becomes problematic in these situations since there is a lack of regulation. Without regulation, the service provider is not legally bound to respect the users' privacy, he has no legal responsibility of providing refunds in case of bankruptcy, and the users have no supporting regulation to prevent frauds (Miers, Garman, Green, & Rubin, 2013, p. 1). Perhaps because of this, many laundering services only operate for short periods, making it harder than ever to keep a transaction record anonymous. Zerocoin is in its essence an attempt to sever the link found between Bitcoin transactions while refraining from employing help of third-party intermediaries. This is done by using a distributed e-cash system that utilizes cryptographic designs. The design allows for strong user anonymity and security based on a distributed, append-only transaction online store (Miers, Garman, Green, & Rubin, 2013, p. 12). The store is essentially both the Bitcoin network and the backing currency used.

Zerocoin is different from most other solutions to Bitcoin's problem of privacy that applies e-cash protocols because there is no currency issuer that creates the coins with a blind signature scheme. A blind signature scheme is a cryptographic concept that was introduced by Chaum (1998). The concept revolves around taking a message and disguising it (thus making it a blinded message) and then digitally signing it (blindly). The blind signature can then be verified against the original message now unblended in a public setting, similar to a regular digital signature. This is particularly useful when handling digital privacy protocols involving different parties, one that is the signer and the other the messenger (Chaum, 1983, p. 3). However, all solutions involving a third-party intermediary have proven unsuccessful and inconsistent with what the Bitcoin system inherently is; a network of untrusted nodes that regularly enter and exit the system (Miers, Garman, Green, & Rubin, 2013, p. 1). Although Bitcoin was not designed with anonymity as a goal in itself, it seems as if Bitcoin users are willing to go to drastic lengths to protect their identity, such as risking their money, and paying transaction fees to an intermediary (Reid & Harrigan, 2011, p. 2) (Miers, Garman, Green, & Rubin, 2013, p. 4).

Through complicated algorithms that utilize RSA accumulators and non-interactive zero-knowledge signatures of knowledge, the creators of Zerocoin have managed to ingrain the idea into Bitcoin with astounding results (Miers, Garman, Green, & Rubin,

2013, p. 12). If two Zerocoins are minted and one of them is then spent, it is impossible to know which one of them was spent; guesswork is the closest thing to actually knowing it (Miers, Garman, Green, & Rubin, 2013, p. 9). It is however problematic in certain circumstances. When n coins are minted such as $n = N$ where N is the total number of Zerocoins in existence, and N coins are spent, then the next coin created and subsequently spent does not have the anonymity of the previous coins but the same anonymity as if only one coin was minted to begin with. This increase in anonymity comes with a cost, the need for a double-discreet logarithm proof leads to longer verification times. This cost however is mainly to withstand the strict requirements of counterfeit protection. Similar to the Bitcoin's dreaded 51% attack where the cost of obtaining over 51% of the entire Bitcoin network is higher than what is to be gained from doing so, it is highly likely that the cost of counterfeiting Zerocoins is much lower than the cost of computing a discrete log. Therefore, it might be possible to follow the weaker premise that there is no financial incentive to counterfeit coins instead of the notion that computing discrete logs is infeasible (Miers, Garman, Green, & Rubin, 2013, p. 12). The fascinating paper on Zerocoin sheds light on how crypto-currencies are constructed with a trade-off between accountability, security, and anonymity, although the trade-offs can be different between systems. A way to use the innovations of Zerocoin (without having to utilize Zerocoins themselves) would be to modify some protocols of Bitcoin regarding anonymity, such as using anonymous credentials (Camenisch & Lysyanskaya, 2001, p. 93). This could reduce the amount of money laundering that is facilitated partly by the design of Bitcoin (since it can bypass laws that require a certain level of financial reporting) and the user's need for privacy (Miers, Garman, Green, & Rubin, 2013, p. 13).

2.7 Peercoin – Alternative Bitcoin design

Many other systems have been invented by modifying the open-source Bitcoin code, such as Peercoin, Dogecoin, Kanyecoin, and recently, Auroracoin. Peercoin in particular is noteworthy because it uses a unique verification system called proof-of-stake instead of the proof-of-work system Bitcoin uses. This proof-of-stake system furthermore addresses the never-ending deflation of Bitcoin that some have criticized harshly.

Ever since the concept of Bitcoin was invented in 2008, a verification system termed proof-of-work has been the dominant choice for crypto-currency systems. The concept of proof-of-work has been used for security by incorporating it in the verification process and, by definition, the mining process.

Another verification system called proof-of-stake was invented in October 2011 and was made public in 2012 (King & Nadal, 2012). Proof-of-stake utilizes a source of verification created in 2010 called coin age that had previously been glossed over by innovators and only used to determine relatively trivial matters such as prioritization of transactions. Coin age can facilitate the proof-of-stake verification system and effectively create a new kind of crypto-currency that relies on both proof-of-stake and proof-of-work systems. Coin age is simply a measurement of the number of days a coin has been in the possession of someone. For example, suppose that Alice gave Bob 100 coins and Bob then proceeded to hold on to the coins for 10 days before spending them. By holding the coins for 10 days, Bob accumulated 1000 coin days. By spending the coins Alice gave Bob, Bob managed to destroy, or consume, the coin age he had amassed. This measurement of turnover has become useful when determining the traction of Bitcoin over a period (King & Nadal, 2012, p. 1).

2.7.1 The proof-of-stake verification system

Proof-of-stake can be summarized as an improvement over the more traditional proof-of-work that is used to verify Bitcoin transactions, among others. The proof-of-work system relies on energy usage, which means that there is some overhead cost in operating networks dependent on proof-of-work, which eventually becomes a cost the users have to pay for with transaction fees. With the inevitable deceleration of mint rate in Bitcoin and an increased want of transaction prioritization, transaction costs will become higher in order to maintain the profit incentive of mining and sustain the level of security the Bitcoin system has already established (Levine, 2014). It then becomes necessary to keep power consumption up to maintain crypto-currencies and that partly defeats the purpose of having crypto-currencies in the first place. Peercoin attempts to rectify this situation by using proof-of-stake.

Proof-of-stake could take the place of proof-of-work in many cases if the design of coin creation and the security model of Bitcoin were altered. In many regards, Peercoin

is a hybrid between proof-of-work and proof-of-stake, an innovation that highlights the qualities of both verification systems. In Peercoin, blocks are separated into proof-of-stake blocks and proof-of-work blocks (King & Nadal, 2012, p. 3). A special transaction called *coinstake* is then needed in the new type of blocks to serve as a proof-of-stake. The coinstake is a concept used for when the owner of a transaction block pays himself by consuming his coin age. In return, he gains the right to generate a new block for the network and minting for proof-of-stake. The first input of the coinstake is called a *kernel* and must meet a certain hash target protocol (a hash function maps data of arbitrary length to data of a fixed length), thereby making the generation of proof-of-stake blocks a stochastic process, like the proof-of-work blocks (King & Nadal, 2012, p. 3). The difference between these two blocks is that the hashing operation itself is conducted over a limited search space while the proof-of-work is done in an unlimited search space. That means that there is little to no consumption of energy in the proof-of-stake process. The hash target protocol is a non-fixed value based on a target per unit coin age (measured in days) used in the kernel. Because the operation is done over a limited search space (one hash per unspent wallet output per second), the ease of meeting the hash protocol depends on the amount of coin age destroyed in the kernel (King & Nadal, 2012, p. 3). Conversely, the proof-of-work target is a fixed value that is applied to all nodes. In general, this means that if Alice has amassed 10 coin-years she can expect her wallet output to generate a kernel in four hours while Bob, who has amassed 20 coin-years, can expect his wallet output to generate a kernel in only two hours (King & Nadal, 2012, p. 3).

In order to incorporate proof-of-stake and coin age into the design of Peercoin, a new minting process was created specifically for proof-of-stake blocks. This process is dependent on destroyed coin age in the previously mentioned coinstake transaction. A mint rate of 1% was chosen to help induce a low inflation rate. This is a great alternative for those who are sceptical about the deflationary nature of Bitcoin. It furthermore shows that it is possible to sustain an inflationary medium of exchange by using a peer-to-peer crypto-currency network.

An important question regarding proof-of-stake is how it decides who mined each block (and gets to claim the coin reward of verifying the block). The answer is that the

highest coin age replaces the highest work effort as the determining protocol, proof-of-stake instead of proof-of-work. What this means is that the Peercoin system is safer against a 51% attack than Bitcoin.

Firstly, the effort it takes to hold a significant stake is likely higher than holding a majority of the mining operations. Secondly, if someone would be able to amass such vast amounts of holdings, his coin age would be destroyed after the attack, making it increasingly harder to continue the attack (preventing transactions from entering the block chain) (King & Nadal, 2012, pp. 3-4). It must be noted that although the effort it takes to hold a significant stake is likely higher than holding the significant portion of the mining power, it is only so because of an addition that was later applied to ensure the safety of Peercoin. Because the destroyed coin age is used to determine which block chain enters the main chain, it has the disadvantage of lowering the cost of attack when attacking the entire historical block chain. Bitcoin, which has a significantly strong protection against these types of attack, still added checkpoints to counteract this potential liability. Checkpoints are a mechanism added to Bitcoin in 2010 to clarify the block chain history and thereby preventing changes to the pre-checkpoint block chain. Peercoin, in order to combat this threat, also installed a checkpoint system that freezes block chains and finalizes transactions. These checkpoints are broadcasted centrally and function in a similar way to Bitcoin's alert system (King & Nadal, 2012, p. 4).

It has been argued by some that Bitcoin has not provided an answer to the distributed consensus problem, since the system used for check pointing is somewhat centralized (Laurie, 2011). The creators of Peercoin tried to create a distributed checkpoint system and concluded that it is hard to make it immune to network split-attacks (the 51% attack for example splits the block chain and makes a new, manipulated block chain the default one). The checkpoint broadcasting system used in Peercoin is therefore centralized until a distributed checkpoint system that is secured against network split-attacks becomes available (King & Nadal, 2012, p. 4).

2.7.2 Energy Conservation of Proof-of-Stake

The creators of Peercoin went through the trouble of introducing a proof-of-stake system to ensure that even when the proof-of-work mint rate approaches zero, there will not be a harmful incentive to raise the transaction volume or the fee to sustain the

inevitable rise in energy consumption. Being long-term energy efficient is a term that can be used about crypto currencies if their energy consumption used doing the proof-of-work is allowed to approach zero without major repercussions (King & Nadal, 2012, p. 5).

Babaioff and others (2012) argued that miners have an incentive to be uncooperative because of the transaction fee integrated into Bitcoin (Babaioff, Dobzinski, Oren, & Zohar, 2012). The incentive is that if a miner refuses to acknowledge the blocks of another miner, he is more likely to reap the transactions fees himself. With proof-of-stake, this problem of incentives is even greater. The transaction fee was removed from Peercoin to combat the problem of perverted incentives and partly to combat the inflation that arises from the minting process linked to proof of stake (King & Nadal, 2012, p. 5). The removal of transaction fees battles inflation because the fee has not been removed at the protocol level, insisting a 0.01 Peercoin fee that is destroyed after payment.

As of January 2014, around 90% of all mining in Peercoin is done via proof-of-work and the energy consumption is around 30% of what Bitcoin uses because of the increased incentive to utilize the proof-of-stake rather than proof-of-work (King & Nadal, 2012, p. 6). This provides a solution for those who are worried about the energy usage of Bitcoin that is, in a way, arbitrary (although it does provide the means to sustain a verification system, that verification is relatively costly when compared to a centralized authority).

3 Origin of Money

The origin of money is a phenomenon where it is necessary to look further than the scope of individual incentives. There is no clear incentive for the individual to accept something inherently worthless (notes) or relatively worthless (metal coins[5]) in exchange for their goods, in the hope that others will do the same. It is plausible that the state could through means of collective coercion, force its citizens to accept a specific currency, pre-existing or created by the state. If that were the case, a few problems that arise that threaten the viability of that notion.

If the currency is decided by the state instead of the market, it is likely to be less efficient than what would happen in a market controlled scenario. If the chosen medium of exchange were pre-existing it would be morally reprehensible to make some individuals rich overnight and others poor. If a medium of exchange were to be created to solve said problem, how would the state distribute it? Furthermore, there is no historical evidence that this ever occurred. Menger instead proposed that money is a result of the free market (Menger, 1892, pp. 48-49). In a pure barter economy, different goods have different degrees of liquidity or marketability. An example would be if someone owns a few specialized tools. These tools have low marketability but if the owner waits long enough, he will probably get full value for it, if the demand is sufficient. The owner of the tools is hungry and wants to buy bread. It does not necessarily follow that he must find a man, with an interest in these specific tools and happens to be a baker or otherwise own loafs of bread that he is willing to part with[6]. The only thing the tool-owner has to do is sell the tools to anyone interested – as long as the goods he gets in return possess more liquidity than the tools had to begin with. When this principle is applied over long periods, the most saleable goods will be traded more frequently, which increases their marketability further. At some point, the most saleable good will become universally acceptable as a medium of exchange and thus carry the highest liquidity (Murphy, 2003).

[5] Assuming a time before gold was used as a conductor.

[6] That would however be an example of a problem called *the coincidence of wants* (Jevons, 1875, pp. 3-7).

Menger stated that money emerges from entrepreneurial perceptions that are subjective in nature. It then proceeds to form a basis for the price indexes (Centi & Bougi, 2004, p. 264). It can be asserted that money provides a function of communicating economic information to agents by acting as a medium of exchange, thus establishing prices (Elias, 2013, p. 28). Ludwig Von Mises agrees with this assertion, stating that the framework of calculations by the entrepreneur and the consumer rests on a process of valuing commodities by their monetary prices (Mises, 1953, p. 47).

The Austrian perspective of the origin of money is a catallactic one, meaning that the best money emerges on top through the effects of market forces. Thornton (1991) is in agreement with Menger, stating that a market economy creates solutions to the problems of society and takes the emergence of money as an example of an attempt to lower transaction costs (Thornton, 1991, p. 77). Although this catallactic process can be used to describe the introduction of money, it can also be used to explain how money can replace other money in a competitive environment. Three factors decide what money prevails; store of value, liquidity, and transaction costs. These factors will be discussed in depth, as they are the same factors that make up the three functions of money, in classical economic theory at least. For now, they will be addressed to demonstrate their role in choosing the ruling medium of exchange.

3.1 Store of value

The regression theorem, which will be analysed further, demonstrates in some ways that a medium of exchange can only work if there is some sufficient level of expectations about its value in the future. Krugman (1984) states that if a dollar is considered a good store of value then the costs of making markets against the dollar is lower, which encourages the use of dollars as the medium of exchange (Krugman, 1984, p. 269). What this means is that liquidity is definitely not the only factor deciding the medium of exchange and can in fact become a deciding factor (over liquidity). This goes both ways; if the demand for a medium of exchange, which is mostly caused by liquidity, declines it can affect the mediums' store of value function negatively. Bitcoins and fiduciary media rely greatly on liquidity and are therefore at a higher risk of value depreciation because of this. This has been a short summarization of the demand side; the supply side of the store of value function is composed of its physical integrity

coupled with the changes in the supply. Menger indirectly defined the physical integrity of commodity as their suitableness for preservation (Menger, 1892, p. 31). Bitcoin, being a cryptographic pair of keys, is not limited to physical durability of objects. The block chain is kept on an extensive peer-to-peer network that makes it near impossible to disintegrate. It can be deduced that physical preservation is not a real problem for any cryptographic online currencies. Fluctuations in the money supply also influence the money supply.

The effects of mining new bitcoins have been covered elsewhere but the effect of a fixed money supply has perhaps not. A fixed final supply of 21 million bitcoins, where the last coin will be mined in approximately 2140, has been a debated topic among Bitcoin critics and followers alike. Mises states that as the quantity of money increases, those who create the added quantity, whether it be the issuers of the fiat money or the producers of the commodity money's substance, will obtain relative superfluity of money and therefore by definition a relative shortage of other goods. The superfluity occurs because the ratio between the demand and the stock of money has changed for the creators of the money. The result is that the marginal utility for holders of this now inflated money will be diminished (Mises, 1953, p. 139).

A fixed money supply from the Austrian perspective is therefore not necessarily detrimental. It has been discussed at other points in this thesis how this might work, both today, where the money supply is still expanding, and later, where the need for expansion has receded and every coin can be divided into Satoshi units. This will be argued further, later in this thesis.

3.2 Liquidity

Liquidity, or marketability, can determine which medium of exchange wins the competition of monies. However, liquidity is more often than not decided from network effects (discussed later in detail), inherent qualities, and other factors.

Hoppe (1996) argues that agents will always prefer the universal medium of exchange (Hoppe, 1996, p. 55). When faced with conducting payments, international traders might for example use a currency that is native to neither one of them just because it is more liquid (The US dollar comes to mind). The casual observer might

remark that this situation is simply a rather metaphysical coincidence of wants, as described by Menger (1892).

3.3 Transaction costs

Bitcoin based transfers can be acted out in two ways. Firstly, by transfer of balances, this is nearly identical to electronic fund transfers widely used by financial instruments and are therefore usually connected to online payment methods. Secondly, by transfer of keys, which can be done both online and offline, pseudo-anonymously and in person. The transfer of keys has typically been associated with offline payments (albeit not necessarily with a public-private key system), with Bitcoin however, it is possible to trade them offline as well. It could be explained in a crude manner by comparing the transfer of balances in the Bitcoin system with the transferring of funds between private bank accounts and the transfer of keys with a situation where a person could give someone else access to a limited part of their private bank account. The abstract aspect of Bitcoin combined with the technology employed in the Bitcoin system allows it to possess the feature of a medium of exchange that has a built in clearing system and record keeping. These two factors are separated in present currency systems.

Menger (1897) states that transaction costs (*economic sacrifices* is the term he uses) usually gets progressively lower with increased economic development. He also states that it is hard to find an exchange that does not include some type of transaction cost (Menger, 1897, pp. 189-190). The multitude of costs take away some of the economic profits of exchange opportunities but more interestingly, the costs can differ between monies. This means that one would be hard pressed to find money that is superior in every way regarding transaction costs. These costs therefore give an opportunity for many different monies to be dominant for different purposes (Menger, 1897, p. 189). Even so, it can be argued that Bitcoin offers a transaction system that is better than the ones currently available in many aspects. Transaction systems necessarily need to be able to provide either transacting services that can be done online, or offline. The Bitcoin system provides both services (through transfer of keys and transfer of balances).

3.3.1 Storage costs and the transfer of bitcoins

On a practical level, the storage cost of bitcoins is minimal. Actual bitcoins are nothing more than key pairs connected to a block chain that is stored over a peer-to-peer network, both of which are digital in nature. This means that the storage cost is nearly zero; computers do not need to be turned on to store Bitcoin wallets and addresses.

The upkeep of the peer-to-peer network is minimal as well, since it theoretically only needs a single, continuously online computer to operate, which might even be used for other purposes at the same time. If this situation is put to contrast with the storing cost of gold or gold backed currency, it is clear that the storage costs of bitcoins are lower. Even fiat money has a higher storage cost, as even if the physical storage cost is marginal (but still higher than the cost of storing bitcoins), the risk of losing paper note currency is relatively high while it is possible to engrave Bitcoin keys in durable metals for example. Another example can be made that counters this one however, as it is possible to invest in diamonds for instance, which are in a way the most durable storage of value in existence, although not particularly liquid (and often vulnerable to market fluctuations to a greater extent than currencies). Other forms of money rest on reserves that must be stored, which means that those forms of money can at most transfer the cost of storage onto others that can do it more efficiently, thus creating an incentive to offer their services.

Bitcoin is therefore superior to other media of exchange when it comes to storage costs and convenience. In a similar vein, transporting of bitcoins, whether it be the transferring of balance (operated through the clearing system; the block chain) or keys (either a physical move or a digital one), is superior in the sense that it has one of the lowest transaction costs. However, it is does not possess the fastest transfer times but theoretically it is possible to make them very fast, at least as fast as other methods of payment. The transaction costs of Bitcoin can be lowered further by the cost efficiency of its authentication system. Where other transaction systems need to verify physical properties of gold and cash, and authenticate the holders of money substitutes in comparison to the issuer, Bitcoin manages to be authenticated by cryptography, which makes it an instantaneous and an automated process. Money substitutes could theoretically implement asymmetric cryptographic encryptions, which would make the

authentication process similar to that of Bitcoin but that has not been done yet (Surda, 2012, p. 34).

3.4 Summary

The inherent transaction fees of Bitcoin are generally around 0.0001 to 0.0005 bitcoins, a much lower amount than the competition can offer. In the future when the rate of new bitcoins from mining has slowed considerably, transaction fees will generally be around a state of equilibrium, where the transaction fee would amount to the marginal cost of maintaining a transaction network. Other types of monies need to counteract the costs of authentication, storage, and transport in addition to maintaining a clearing system which makes Bitcoin at the worst highly competitive. It seems that Bitcoin can be measured up against other currencies, at least partly, and the results are surprising. It can provide a significant improvement over other systems. For Bitcoin to evolve into money however, more than a competitive advantage is needed. Network effects and a plethora of other problems have an adverse effect on Bitcoin as an evolving medium of exchange. These factors can prove detrimental to Bitcoin becoming full-fledged money. Disregarding these problems, we can see that it is necessary for Bitcoin to keep a growth of liquidity so it can compete with other monies on an even playing field (or even a playing field rigged in Bitcoin's favour). If the liquidity Bitcoin has obtained already is not sustainable, it will be hard for it to evolve beyond being a medium of exchange (Surda, 2012, p. 37). At most, Bitcoin will remain a secondary medium of exchange, where *secondary medium of exchange* is a term used by the Austrian school to describe media of exchange that are not universal.

4 Mises' Regression Theorem

We have learned from Menger how money originated, Menger however did not explain adequately what created prices, in essence how money got its inherent exchange value. The regression theorem however, does.

Bitcoin has been criticized because the fundamental concept of Bitcoin does not adhere to the regression theorem from a general viewpoint. The theorem, laid out by Ludwig von Mises (1912), attempts to explain how media of exchange acquire their prices. From the theorem, it is apparent that it should be possible to trace back the price of a medium of exchange to some origin. It can then be inferred that media of exchange arise from a commodity that has inherent uses and is liquid.

In short, it states that "before an economic good begins to function as money it must already possess exchange-value based on some other cause than its monetary function" (Mises, 1953, p. 111). This short theorem supports Menger's theory about the origin of money and contributes to a refutation against theories stating that the value of money comes from a, in a way, centralized agreement to give valueless things value (Mises, 1953, p. 110).

The regression theorem states that money has value today because it is expected to have similar value tomorrow. At first glance, this seems like an application of circular logic at best and in many ways, a similar approach as the marginal utility theory incorporates. There were a few complications with the marginal theory of utility. It did not explain the nominal prices of goods and services adequately which resulted in generic theories of money quantities being used. By doing so, the economists relied on aggregate variables such as $MV = PQ$, which created a myriad of problems such as trying to account for unstable money velocity and sticky prices. Factors that ultimately make the direct relationship defined in the equation less than perfect. The theory also does not account for the demand of money sufficiently (Mises, 1953, pp. 384-386). The marginal utility theory itself also tried to explain how money became to have a certain exchange value by referring the fact that people have a marginal utility for money because it has a certain exchange value (Murphy, 2003).

While it is true that people have greater marginal utility for monies than other goods, which is the essence of how they became monies in the first place, it does not

adequately explain the origin of value. This is because money does not derive its value directly from the medium itself but rather its purchasing power; this is fundamentally different from other goods and services (Mises, 1953, pp. 108-109). The regression theorem states that the expected purchasing power of money gives it value and people are willing to sacrifice goods today in exchange for money that they can use tomorrow (Mises, 1953, p. 121). The expected purchasing power of money tomorrow imbues the money with value today. If the explanation ceased there, one might think that the same circular logic is at play here.

However, Mises managed to circumvent this by including the element of time. People today (t) expect money to keep their value tomorrow (t_{+1}) because it had value yesterday (t_{-1}). In this sense, we get a weak notion of money as memory, which will be useful later in this thesis. From there we can use regression to assert that people yesterday (t_{-1}) thought their money had value because they had memories of it having value at (t_{-2}) (Mises, 1953, p. 121).

This type of regression lends itself to criticism involving the infinite nature of the regression. It is thankfully unfounded as we can adopt Menger's explanation of the origin of money. By using the regression theorem, it is possible to trace the value of money backwards until we get to a point where money first emerged from a pure barter economy. From there it is easy to analyse where the exchange value of money originates, as it is the same process as with any other goods. Gold for example was valued for its intrinsic beauty and scarcity (Murphy, 2003). It is important to note that if the premises of the regression theorem are to be followed, it is essential that in order for commodities to become money, they must have been in demand for other reasons than their exchange value at some point. However, Bitcoins seem to have amassed demand long before it acquired value because of its liquidity and convenience.

4.1 Origins of the demand for Bitcoin

Bitcoin is currently being employed as a medium of exchange as well as an, albeit highly speculative, investment so there is certainly demand for it from both sides. One explanation is that the demand is created by the effects of speculation on the future of Bitcoin, which in turn creates justification for Bitcoin's exchange demand. The speculative investors think that bitcoins will increase in value if the network effect, falls

in the favour of Bitcoin. They are therefore creating a demand for bitcoins without having an immediate plan to exchange them or otherwise sell them. This interaction effectively provides a relatively stable exchange between bitcoins and traditional fiat money.

The demand is in fact the initial demand for direct use as propositioned by the theorem to begin with, the link between bitcoins and the USD, for example, creates a link from which the regression theorem can work through, like with all other goods bought with fiat monies (The Voluntaryist Reader, 2012). An exchange demand for Bitcoin has thus been created from a non-exchange demand by employing established fiat monies.

This situation is reminiscent of the gold certificates that were sometimes used in the 19th century. The certificates were made of paper but still held the value of gold, since they were redeemable for gold. These certificates grew popular, as they were lightweight and easier to manage. The Bitcoin system, with its pseudo-anonymity, encryption, and global reach is an attractive option for facilitating the use of established fiat currencies and therefore a viable competing medium of exchange in the modern marketplace (The Voluntaryist Reader, 2012). It is interesting to note that the design of Bitcoin, accidentally or on purpose, incited early adopters to hoard their coins, thus creating the non-exchange demand, that eventually the exchange demand, through an established bond between bitcoin and the USD. This is only a speculative theory but is set forth mainly to show the possibilities of crypto-currencies coexisting with the regression theorem, since it is clear that there is a demand for Bitcoin without any consideration to the traceable origin of value.

The subjective theory of value states that the value of a good is determined by the importance of a good (that is determined by the individual in question) for the achievement of the desired end of the individual (Mises, 1998, p. 96). From this, we can gather that even though Bitcoin is not yet considered money, it is getting closer. The main reason for this, in the context of this chapter, is the issue of Bitcoin as a final payment. A final payment for goods and services is most often money, money being risk-free for counter parties, highly liquid, and a tradable object, properties that are necessary to solve the barter problem. Bitcoin is seldom used as a final payment today

and when used it is because of a direct relationship with established fiat currencies such as the USD.

4.2 A Reformation of the regression theorem

It is not hard to see why many economists and non-professionals alike have taken a stance against Bitcoin for the sole reason that the design of Bitcoin seems to defy the regression theorem at best, or defeat it at worst. According to the regression theorem, the progression of Bitcoin is in violation of the traceable origin conclusion of the theorem. Many would say that Bitcoin has rendered the theorem unnecessary; there is no need to do so if one understands the reasons for this seemingly ludicrous demand for bitcoins. Others, like Murphy, admit that the regression theorem applies not only to money, but to media of exchange as well. Krugman has criticized Bitcoin for being an unreliable store of value, thus denying the validity of Bitcoin as money, although he concedes that Bitcoin is (likely) a successful medium of exchange (Krugman, 2013). As Bitcoin has been stated to be at least a secondary medium of exchange in this thesis, then it could be inferred that the theorem is either wrong, or misunderstood. This thesis proposes that a new adaptation of the regression theorem is needed to encompass the technical, unforeseen nature of Bitcoin.

For the theorem to work, a medium of exchange must already have the attributes necessary for a medium of exchange, having a price and be accepted on the market. Both price and liquidity (being accepted on a market) are elements of the market. If the prospective medium of exchange possesses these elements then it points toward a demand for it (a demand that must exist before it becomes a medium of exchange) that is then by definition a non-monetary demand. A medium of exchange might eventually cease to have non-monetary demand but continues to be sustainable. Even though Mises sees non-monetary demand as being necessary for the emergence of price and marketability, he still states that money only provides utility for obtaining other goods and services in exchange for it (Mises, 1953, p. 101).

This essentially means that even though non-monetary demand is necessary for the emergence of money, it is not necessary to sustain it. Rothbard (2004) further clarifies what Mises stated by saying that it is not necessary that the direct use of the money as a commodity continues, as long as the money has been established (Rothbard, 2004, p.

275). He states this by writing that even if gold were to lose its value as an aesthetically pleasing, easily controllable metal that doubles as a fantastic conductor, it would not necessarily mean that gold would lose its value as money (Rothbard, 2004, p. 275).

Rothbard however uses the premise that all monies must necessarily originate as commodity with direct uses, a claim that is difficult to accept. It is difficult to accept because of Murphy's earlier statement in this chapter that Mises' regression theorem applies not only to money, but to media of exchange as well. Mises' view is that any media of exchange that does not adhere to the regression theorem cannot possibly exist (Mises, 1998, p. 407). Any talk of sustainability of media that does not adhere to the theorem is therefore meaningless at best. This, in conjunction with Murphy's and Rothbard's statements creates a difficult position where the regression theorem must be either wrong or misunderstood if Bitcoin is a medium of exchange and frankly, that seems to be the case.

Although this is a harsh conclusion, it does offer ways to make amends. First, it deters criticism of Bitcoin from the Austrian economists who argue that Bitcoin is not sustainable because it is not money from an Austrian perspective, as it violates the regression theorem. The argument falls flat when the earlier notion, that media of exchange that do not comply with the theorem are impossible rather than unsustainable, is considered (Mises, 1998, p. 407). Secondly, it offers a way of reformation, in which the regression theorem can be reconstructed to adhere to technical advances such as Bitcoin. The statements, especially from Rothbard, offer the premise that as long as a medium of exchange possesses the qualities of liquidity and price it is irrelevant whether or not it originally existed as a commodity with non-monetary value, regardless of whether or not that is possible.

From there a reformulation can be done that permits Bitcoin to exist as a medium of exchange from the Austrian perspective, without being regarded as impossible because of its origin. It has already been stated that as long as a medium of exchange has price and liquidity, both of which are qualities with essential ties to the market and as such must be established through market elements, whether it be through catallactic laws, price signals, the theory of value, or speculation does not matter. Therefore, once a medium of exchange has become sufficiently liquid to garner a certain level of publicity

and the positive externalities that follow (network effects) that make it highly valuable for its inherent liquidity, it can sustain itself without being useful as anything other than a medium of exchange. Before this can happen, a price must be determined in some way. The price of fiat money is established through its origin as a money certificate with ties to commodity money. The price of commodity money is established by its non-monetary uses. Some media of exchange, like Bitcoin (albeit a secondary medium of exchange), have a harder time tracing their value back to some origin and therefore it can be challenging to see how a price can be determined for such media. One way to do so is by using the ties between Bitcoin and established currencies, as that does not violate the original regression theorem. A different, more practical, perspective of this problem yields an approach where the price can be determined by a simple equation using electricity and other non-abstract factors.

4.3 A practical analysis of Bitcoin‘s price

The first available record of the price of bitcoin can be found at New Liberty Standard, a website that sold self-mined bitcoins in 2009, where one dollar was worth 1309.03 bitcoins in early October 2009 (New Liberty Standard, 2010). The price was found by dividing US$1 by the average amount of electricity required to run a high CPU computer for a year, which at the time was 1331.5 kWh. This was then multiplied by the average residential cost of electricity in the US for the year before, which was US$0.1136, divided by 12 months and divided again by the total number of bitcoins generated by their computer over the past 30 days (New Liberty Standard, 2010).

In a sense, the variable cost of production was used to determine the selling price of bitcoins. This explains the price level from the perspective of the supply side, although it could have used an arbitrary price in theory, which leads us to the demand side. It has been argued, that bitcoins have attractive qualities that generate demand for them like low transaction costs and ideological benefits (which remain generally subjective) such as no central authority, pseudo-anonymity, and others which are examined in this thesis (Matonis, 2011). This clearly shows that bitcoin had demand and supply before it became widely used as a medium of exchange and furthermore that the supply side was competitive, although the demand side was partly formed from ideological, non-

monetary reasons (and partly because of the possible profit of such low transaction costs) (Surda, 2012, p. 42).

The price was thus established. From price, liquidity can form and with an increasing demand, a Bitcoin exchange was finally formed on February 6th 2010, which marks the beginning of an era where Bitcoin reached liquidity (Bitcoin Wiki, 2013). The phrase *reached liquidity* is defined here as even if the users of Bitcoin abolished their ideological principles and in fact, all non-monetary reason for using bitcoins, Bitcoin's liquidity would still keep it afloat as a secondary medium of exchange. The first real world transaction using bitcoins took place in 2010 on May 22, where a programmer offered 10,000 BTC (around US$25) for a pizza. That pizza purchase is worth around US$4,340,000 today. While Bitcoin is capable of providing comparative advantage in transaction costs over other forms of currencies currently in use over their advantage of network effects, Bitcoin can sustain itself as a medium of exchange (Surda, 2012, p. 43).

A counter argument to this is that even though electricity and computational power (and at least some fraction of the computer's lifetime) is used to mine bitcoins, it is inherently a waste of resources if Bitcoin would not be accepted as a medium of exchange.

5 What is money?

Functions of money can be divided into three segments. It is a medium of exchange, a unit of account (also called a measure of value) and a store of value (Mankiw, 2009, pp. 80-81) (Krugman, 1984, p. 263). This segmentation does not answer the question of what money really is unless money is a term for the functions of itself.

The Austrian school of thought offers a definition of money as a single commodity that is universally employed as a medium of exchange. This single highest marketable commodity becomes universally accepted after other competing marketable goods are rejected, as they cannot offer the same utility as the previously mentioned commodity (Mises, 1953, pp. 32-33). The Austrian school therefore considers the other two standard functions of money, unit of account and a store of value, as secondary functions of account of money being accepted as the medium of exchange (Schlichter, 2011, p. 43). Menger even goes as far as stating that the subcategories of money, defined here as unit of account which is the same as a measure of value, and a store of value, are accidental and not essential to the concept of money (Menger, 1897, p. 280).

Standard of deferred payment has been used as a fourth segment but for the intents and purposes of this thesis, it can be subordinated within the other groups. If it were to have a separate standing from the three main functions of money as defined by Krugman, it could then be argued that it falls under *money as a medium of exchange*. Salerno for example has stated that standard of deferred payment as a function of money can be classified as a subsidiary just as easily as the other two subcategories (Salerno, 2010, p. 66).

Money necessarily needs to be able to function as a medium of exchange so it can be used in trade to avoid the problems of a barter economy, in particular the problem of *coincidence of wants* (Jevons, 1875, pp. 3-7). Money, as a unit of account, functions to provide a standard unit of measurement of the cost, and therefore value, of goods and services. Money can function as a store of value since it can function as an asset that can be saved and retrieved easily.

5.1 Bitcoin as applied memory

Kocherlakota and Wallace (1998), among other economists, have argued that there are apparent similarities between money and public record-keeping devices (we can assume that public record keeping devices are interchangeable with memory as defined here) (Kocherlakota & Wallace, 1998, p. 273). Following the idea of memory, we can define memory as a technology that records the past actions of agents and makes this information public (this notion has been used very often) (Araujo & Camargo, 2010, p. 2).

The similarities between money and memory exist to such an extent that it is plausible that memory could be used as a substitution to money; indeed, those who adhere to that view might say money came into existence as a necessary solution to our memory's limitations (Kocherlakota, 1996, p. 3). From that view, it is possible to construct a justification of how modern monies are accepted despite having no intrinsic value. Bitcoins fall under this category, as money without intrinsic value but bitcoins also suffer from having no original set value either (as it could be argued that the electricity used to mine bitcoins is fundamentally wasted). It could be argued however, that since agents will choose not to use money, as it is less manageable than simply observing an up-to-date record when the probability of observing such a record is sufficiently high, Bitcoin has some intrinsic value (Luther & Olson, Bitcoin is Memory, 2013, p. 3).

The question then becomes, whether bitcoins can be used as a practical application of memory even though they do not possess original value. An attempt has been made to redefine Mises' regression theorem so it can account for Bitcoin, instead of becoming obsolete because of it. It must be taken into consideration that Mises could not have foreseen the technological framework required for crypto-currencies such as Bitcoin to exist, if he could have, he would perhaps have adjusted his regression theorem accordingly.

Money as memory is essentially money as record keeping. Consider a tiny economy where everyone is in hearing range of everyone at all times and everyone has been blessed with a perfect memory. An economy like that would have no need for money, as they would simply shout: "I gave [name] X amount of [product/service]" and

everyone would know and remember. If that person wanted something from someone else later, he could just ask for it, because the giver would know that when he shouts that he has given something away, he will be reimbursed the next time he needs something himself. Although the idea of bargaining stated here is similar to traditional economic examples, aside from the lack of physical commodities, the perspective is refreshing.

Kocherlakota and Wallace show that money is not an essential need if memory, as defined earlier, is perfect. Memory can be divided into two parts, a record-keeping device (records past transactions) and a coordination device (disclosing the records to every other agent) (Kocherlakota & Wallace, 1998, pp. 272-273). The Bitcoin design is capable of delivering a medium of exchange capable of both functions.

Kocherlakota (1996) writes that, even though economics can answer the question *why money exists*, it can be answered differently. The classical approach would immediately refer to the fact that money is a store of value and a convenient medium of exchange. The perspective of money as memory offers an answer that includes the earlier definition of money; it is simply an ability to keep track of the past (albeit in a limited fashion).

From that notion, we can gather that money might simply be an imperfect substitute for high quality information storage (or access to that kind of storage). If that is the case, it might be concluded that as information access and storage costs get lower, in essence, as monies get more efficient, the maintenance of the seigniorage[7] monopoly the authorities yield might be at risk of depletion. Kocherlakota comes to a rather radical conclusion that is highly relevant to Bitcoin. Bitcoin and other crypto-currencies currently have the possibility of offering transaction costs, liquidity, and access to information, at a rate more efficient than competing monies (Kocherlakota, 1996, p. 28).

Luther and Olson (2013) show that in regards to the notion of money as memory (and memory as money conversely), Bitcoin most definitely is money (in that sense).

[7] Means the difference between the value of money and the cost to distribute and produce said money.

Every peer, or user, on the Bitcoin peer-to-peer network has a complete copy of all transactions that have occurred in the past and furthermore updates it in such a way that new transactions are compared to the existing ledger before authorization can be completed. The system does not give a complete overview of the transactions of individual agents, since the transactions shown are those of accounts and not agents and a single agent can have more than one account. Each account is protected by pseudo-anonymity, which makes it even harder to do so. Even though this system does not follow the general theoretical framework of connecting transactions to agents but instead uses transactions, it can fulfil its role as an imperfect form of memory (Luther & Olson, Bitcoin is Memory, 2013, pp. 9-10). Perfect and imperfect memory, where memory functions as information in the same sense as it does in game theory, are concepts used to describe properties of memory. Perfect memory means that all agents know all past transactions of other agents. Imperfect memory applies when agents are not aware of all past transactions that have aspired (Gibbons, 1992, p. 55). There is no easily discernible role for money when perfect memory is available to observe. If there were a role, it would be reserved for special circumstances at best, since money would hold no value, except for perhaps novelty. For money to be relevant, some form of imperfect record keeping is needed (Sanches & Williamson, 2010, pp. 1535-1536).

There is a low probability of systematic manipulation by external users made possible by the coding of Bitcoin. The manipulation, in the form of possible double spending, is possible out of necessity for the Bitcoin system to work, however, for the double spending to occur the malicious user must have a computational power composed of at least 51% of the entire Bitcoin network. Although theoretically possible, it is extremely difficult and it has been calculated that the incentive to do so is next to non-existent since the expected value is negative, compared to using all that computational power honestly within the Bitcoin system (Luther & Olson, Bitcoin is Memory, 2013, p. 10). To explain in detail, a malicious user would have to redo all the proof-of-work needed between two transactions and subsequently hash a new forged block before other users hash legitimate blocks (Luther & Olson, Bitcoin is Memory, 2013, p. 10).

5.2 Summary

It is clear that both memory and money can facilitate exchange. If the memory is imperfect, and the money expensive to store or verify, there must exist some middle ground where both memory and money are used simultaneously (Luther & Olson, Bitcoin is Memory, 2013, pp. 2-3). Sanches and Williamson (2010) show in great depth why memory is imperfect in practice. If that balance is disrupted because the money gets overly costly compared to memory it is obvious that memory will become more likely to be used (Sanches & Williamson, 2010). If we assume for the time being that Bitcoin can function as imperfect memory, its role in current markets makes sense. Bitcoin has not conquered established currencies but is rather an alternative payment method for those who value anonymity, decentralization (idealists), or even something as simple as digitalization and convenience. As the expected cost of storing and verifying traditional currencies increases, as has somewhat been the experience in recent times, Bitcoin will be used more frequently as the earlier theory of balance between money and memory suggests (Luther & Olson, 2013, p. 16).

It is evident that, at least in some aspects, the theoretical concept of memory, that has traditionally been used to justify the existence and usage of conventional monies, has certainly some applications in the real world. Crypto-currencies based upon the system designed by Nakamoto such as Bitcoin are an example of practical memory. According to theory, it should be feasible to strife towards mutually inclusive economy, which embraces both bitcoin (memory) and traditional currencies (money).

6 Is Bitcoin money in a general sense?

Bitcoin is, as of now, not a universally accepted medium of exchange even though it is theoretically as liquid as currently established media of exchange. As Bitcoin is not universally accepted, it is not money from the standpoint of the Austrian school of thought. From that notion, an awkward situation presents itself. It is clear that Bitcoin is not money from the Austrian perspective, but it is still a medium of exchange. This situation is resolved by classifying Bitcoin as a secondary media of exchange, a term used by the Austrian school and throughout this thesis to describe media of exchange that are not universal. Mises further describes this class of media as goods that have a demand because they make cash holding a more feasible option. The prices of these goods are higher than they would be partly because of this specific demand. It can then be said that the exchange value of these secondary goods emerges from two factors; the demand of the services the secondary media of exchange provides, and the demand for other services the secondary media of exchange provides (Mises, 1998, p. 460). Rothbard (2004) calls this secondary medium of exchange quasi-money, goods that are so liquid that they become money from a practical standpoint (Rothbard, 2004, p. 827).

6.1 The concept of money categorized

The Austrian view of money, defined as the most universally accepted medium of exchange, can be said to be a broad sense of the notion. This broader sense of money can be divided into two categories. Firstly as money in the narrower sense, which is the notion mainly used throughout this thesis, and secondly as money substitutes, which consist of money certificates on one hand and fiduciary media on the other. Fiduciary media can be further classified as token money in general and uncovered bank deposits and notes (Mises, 1953, p. 483). Other schools of economic thought have classified money in the narrower sense as the monetary base while the term *money substitutes* have been described as other forms of money, or inside money (Mises, 1953, p. 483).

The concept of money used in this chapter will predominantly refer to money in the narrower sense. Mises divides money in the narrower sense into three subcategories: fiat monies, credit monies, and commodity monies. An interesting historical observation can be made toward the classification of credit money, which is defined as claims against legal, or a physical, person that can be used to purchase goods and services.

When these definitions were written, true fiat money did not exist so only commodity money and credit money were used in practice. This has changed drastically and in present times, national currencies have become true fiat monies and credit money is not practically feasible. Credit money in general includes any financial instruments or bank money market account (MMA) certificate that are not both payable on demand and perfectly secure (Investopedia, 2014). If they possessed both qualities, there would be negligible difference between their value and the sum of money they referred to, which leads to a risk of the valuation process being dependent, therefore biased. Because of this risk there needs to be some form of delay of the claims' maturities (Surda, 2012, p. 23).

From this, it can be inferred that credit money is not of great relevance to the discussion presented in this thesis and will therefore be mostly avoided. Fiat money and commodity money will be discussed further but for a short introduction on each category, it can be said that fiat money consists of things with a special legal qualification while commodity money consists of commercial commodities that can be used as money as well.

6.2 Commodity money and fiat money

6.2.1 Commodity money

Commodity money is composed of commodities that have some intrinsically useful qualities besides that of fulfilling the role of an exchange medium (Selgin, 2013). It must also be scarce so that it holds a positive value in a state of equilibrium. This positive value is assumed equal to its marginal cost of production, given that there are competing suppliers in play) (Selgin, 2013, p. 2).

Commodity monies such as gold still have flaws. They are vulnerable to shocks that shift the supply of the commodity money-base schedule. For example if a huge supply of easily accessed gold were found today or if a revolutionized technology that revamps the mining process were to be discovered. This has happened many times in the past and might even have been a good thing in some cases, since the existing commodity money slowly wears down in addition to a rising marginal cost of prospecting, thereby battling a secular deflation (Selgin, 2013, p. 4). Commodity monies can also be costly; Friedman said that the fundamental defect of commodity money was that it needed

resources to increase its stock supply (Friedman, 1960, pp. 4-8). This has been shown to be an overstatement by White but it is still just as true that a fiat system can have a lower resource cost than a commodity money where it is employed as a medium, by means of circulation or bank reserves (White, 1999, pp. 48-49) (Selgin, 2013, p. 5).

Because of these flaws, representative money was sometimes used instead. Representative money is essentially fiat money with something akin to a gold standard. When representative money was abandoned, fiat money (representative money without any anchor to real goods) became prevalent. There are other types of money such as bank notes but for this thesis, the focus will be on commodity money on one hand, and fiat money on the other.

6.2.2 Fiat money

Fiat money is composed of paper notes without any inherent value or bank deposits that can be converted into said notes. These notes have value that is considerably higher than their marginal cost of production. The paper notes' only intrinsic value is the economy's acceptance of them as a medium of exchange. Since the marginal cost is remarkably low, compared to their value, it is easy to see that the supply must be controlled by some authority. If the free market were to decide, the value of each note would quickly approach the marginal cost of making a paper note. Therefore, the scarcity of fiat money is manufactured. It is the nature of fiat money that there cannot be a competitive market with it, since the value would quickly approach the value of printed paper notes (Friedman, 1960, p. 7). When this argument is taken further, there is reason to expect that the value of the fiat currency will approach zero as there is no need to create additional paper notes when expanding the nominal quantity of fiat monies; it can be done by supplying larger denomination notes than before (Selgin, 2013, pp. 2-3). The risk of having fiat money stems therefore mostly from the risk of mismanagement (Selgin, 2013, pp. 3-4).

Bitcoin is mathematically guaranteed to be scarce and with a greater certainty than gold, since the supply of gold is susceptible to fluctuations if vast goldmines or a great gold collection would be discovered. A common solution to the problems associated with great expansions in the supply of a commodity, such as gold, is competing fiat currencies that are privately issued (Hayek, 1990, p. 24). Even then, the temptation of

the issuers to issue large quantities of their notes or electronic deposits, once they have become a ruling media of exchange, is always present (Murphy, 2013). Bitcoin, as synthetic commodity money, solves this problem.

6.3 Money substitutes

Mises defines money substitutes as claims that are perfectly secured and immediately payable, which, along with their standing in law and commerce, makes them prime candidates for facilitating indirect exchanges (Mises, 1953, p. 50). Mises himself does not seem to follow his own definitions to the letter, since he later in the same text writes that "those who wish to spend money will find that these claims answer their purpose just as well" (Mises, 1953, p. 53) and that "such claims are complete substitutes for money, and, as such, are able to fulfil all the functions of money" (Mises, 1953, p. 267). These quotes imply that he is only referring to the suitability of money substitutes to facilitate indirect exchanges and not that they are secure and immediately payable claims (Surda, 2012, p. 28).

It seems as if there are two concepts of money substitutes. One of them is defined as claims on narrow sense money with zero maturity that is considered absolutely secure, and the other is defined as things that act as substitutes to narrow sense money from an economic perspective (Salerno, 2010, p. 70). The earlier definition is clearly from a legal perspective while the latter one is from an economic one. Mises clarifies that, although not identical, the definitions are treated as such in commercial practice (Mises, 1953, p. 54). Surda proposes a definition that combines the legal and the economic aspect: as a good linked to money in the narrower sense that acts as an almost perfect substitute to it, from an economic perspective (Surda, 2012, p. 25).

Money substitutes are divided into fiduciary media (which is further divided into token money and uncovered bank deposits and notes) and money certificates (Mises, 1953, p. 483). Fiat money traditionally starts out as money certificates, but the difference between fiduciary media, such as uncovered bank notes, and money certificates is the backing reserve ratio. Money certificates are completely backed by reserves while fiduciary media does not have to be backed fully.

6.4 Synthetic commodity money

So in what category does Bitcoin fit? The immediate answer must be that it does not fit at all, however, alternative categories exist that can provide a suitable solution. Bitcoin falls somewhere between commodity money and fiat money and this cross-sectional category has been called synthetic commodity money (Selgin, 2013, p. 1). In essence, the intricate quality of synthetic commodity money is that it needs no centralized monetary authority to create a macroeconomic stability by being adjustable.

Schlichter states that the most important difference between commodity money and fiat money is the level of elasticity of the money supply (Schlichter, 2011, pp. 42-46, 136). In that regards, it is clear that Bitcoin more closely resembles commodity money than fiat money, but Bitcoin still falls into neither of those categories. Fiat currency as described here refers to a currency that relies on government fiat to define what counts as legal money (Murphy, 2013).

Whereas fiat money does not hold any non-monetary uses and is contingently scarce, commodity money is naturally scarce and does hold some monetary uses. This dichotomy of premises gives way for a 2-by-2 matrix classification system, although not necessarily useful on a practical level.

The other categories are money that is contingently scarce but still has non-monetary uses, named Coase Durables by Selgin, and money that does not have any non-monetary uses but is still naturally scarce, called synthetic commodity money (Selgin, 2013, p. 5).

Coase (1972) made an argument called the Coase conjecture. The Coase conjecture states that when a monopolist sells a durable good, in a market where it is impossible to resell with consumers that have different valuations, the monopoly is in competition with itself from other periods. This means that if the monopolist does not know the preferences of the consumers, he has to set the price of the good low, which means that patient consumers can hold out for the lowest price. The argument only holds in an infinite framework (Coase, 1972).

A fine lithograph with the engraved plates owned by a monopolist is an example of a Coase Durable. In the example set by Coase, the monopolist will find it difficult to maintain a Coase Durable standard, since he can profit by creating more units of

standard money until the exchange value of the money will be equal or less to its trivially small marginal cost of production. The consumers anticipate this and are therefore unwilling to pay more than the marginal cost of production, even for the first units supplied. Coase Durables are therefore at risk of a collapse despite being based on something with non-monetary use value under the control of a monopolist (Selgin, 2013, p. 6). The Coase Durables in this example will eventually deteriorate into a traditional commodity standard where the utilized scarce commodity is the paper used in the lithographs.

Selgin theorizes two solutions to this problem. Firstly, it is possible to resort to a money back guarantee, where the buyers are promised that they get their money back if the price of lithographs falls below the amount they paid. Secondly, the engraved plates can be publically destroyed, which results in the lithographs becoming ordinary commodities, as they are no longer only temporarily scarce, but irrevocably so (Selgin, 2013, p. 7).

What synthetic commodity money hopes to achieve is an optimal middle ground between two opposites. On one hand, there is a central banking system, on which Friedman asserted that money was too important to be left in the hands of central bankers (Friedman, 1962, p. 219). On the other, there is a free market of money, on which Keynes claimed that money is too important to be sacrificed to blind forces (Keynes, 1936, p. 339). Synthetic commodity money is advantageous because it circumvents both the blind forces and the central bankers by having its supply determined by resource constraints that are artificially arranged. The result is a synthetic commodity money which works in many ways like fiat money but with one major difference; the marginal production costs are not zero or close to zero but real costs that gradually rise (Selgin, 2013, p. 11).

Since the true cost of resources of synthetic commodity money does not have to be any greater than that of similar fiat money, it is free from the disadvantages of the natural commodity standard, especially regarding costs. It is also free from supply shocks such as technical innovation or discoveries of commodity supplies such as large amounts of previously undiscovered gold. Furthermore, it does not have any varying non-monetary demand that could, and probably would, alter its market value and

thereby its purchasing power. It is also free of the political influences that persistently prove to be an unwelcomed complication for fiat money (Selgin, 2013, p. 11). Indeed, synthetic commodity monies, like Bitcoin, seem to have the best of both worlds.

There can be two types of synthetic commodity money. Inelastic money, such as happened with the Iraqi Swiss Dinar where fiat money essentially became frozen, and elastic money (Selgin, 2013, p. 12). Inelastic money can come about in a few ways. It is perhaps easiest to destroy the original engraved plates in a public setting, in much the same way as if creating Coase Durables. That would effectively fix the supply of lithographs since the paper notes representing fiat money consist of small lithographs that are impossible to replicate. The marginal resource cost would then rise from zero, or close to zero, to near infinity (Selgin, 2013, pp. 11-12). An emergence of an automatic regime in which the scarcity of base money is unchangeable and the regime freezes the stock of paper currency. It would still be necessary to prevent the future creation of reserve credits that are not fully backed with currency somehow; destroying the plates alone cannot achieve that (Selgin, 2013, p. 12). Let it be noted that by destroying the plates it is meant in a general context such as dismissing the bureaucratic system that creates new money. The same problem would then afflict this money as natural commodity money; the eventual deterioration of the currency supply would be inevitable and thus create a secular deflation (Selgin, 2013, p. 12). This is relevant to Bitcoin, both to provide a perspective on how the category least like Bitcoin functions and furthermore to create a context for a deflationary design and its effects on a decentralized medium of exchange.

Elastic synthetic commodity money means a stock of money, which is capable of both growing automatically and in accommodation with the increasing demand of money (Selgin, 2013, p. 19). Peercoin is a great example of elastic synthetic commodity money while Bitcoin is an example of inelastic commodity money, since the supply of Bitcoin will become completely inelastic eventually, and in a gradual transparent manner.

Friedman proposed a computer controlled monetary rule, which relied on a *k*-percent rule, to create an elastic synthetic commodity standard. The *k*-percent rule is a monetarist proposal that a central bank should increase the money supply by some

constant *k* percentage rate each year, regardless of business cycles or other financial disturbance. This computer controlled monetary authority could not be shut off or tampered with (Friedman, 1960). Bitcoins not only embody this vision, but also improves it in a way Friedman would perhaps not have thought possible at the time, since Bitcoin manages to solve the double-spending problem, a problem that must have been hard to predict at the time. In a way, Bitcoin also responds to a common criticism of the *k*-percent rule that the policy does not allow for any feedback or interference of a central bank, since there is not a central bank of Bitcoin that can respond to financial fluctuations in any case.

7 Austrian Business Cycles and bitcoins

Business cycles are considered an important proponent of macroeconomics. Different economic schools of thought have differing opinions on how the business cycle of the economy functions. Even when there is an agreement of how it functions, the interpretations of what each part of the cycle stands for are wildly different. To demonstrate the differences between perspectives more clearly, an Austrian perspective is pitted against a Keynesian one. Although Keynesian economics are outdated in some ways, the Keynesian school of thought still offers many valid arguments for this chapter. The Austrian theory of how the business cycle works was originally defined by Mises and was later explained in more detail by De Soto and others (Mises, 1953) (de Soto, 2012, pp. 347-503).

A Keynesian view of business cycles is that there is a probability of short-run equilibriums in the economy where the unemployment rate is less than perfect, either too high, or too low. When the unemployment rate is higher than the natural unemployment rate, a change in fiscal and monetary policies can help reduce fluctuations of the business cycle. The natural unemployment rate is used here in from the perspective of Keynesian economics, as the lowest level of unemployment attainable without a rise in inflation (in mainstream economics this is known as the non-accelerating inflation rate of unemployment). The Keynesian school therefore states that the economic cycles are a result of endogenous factors, when *effective demand*[8] falls short of supply, leading to a recession. Neo-classical economists believe that the causes are exogenous, an explanation that emerges from the supply-side of the market and an acceptance of *Say's law*[9].

The Austrian economic theory states that business cycles are a result of banks utilizing fractional reserve banking systems to issue excessive amounts of credit. The

[8] Effective demand is used here because labour market disequilibrium (a shortage of labour) can result in a spill over, that influences the demand for goods.

[9] Say's law states that products are paid for with products and saturation can only happen when there are too many means of production applied to one type of product and not enough means of production to others (Say, 1803, pp. 178-179).

amount grows even higher when the monetary policies of central banks call for the interest rates to be kept artificially low. The money supply expands because of the excessive credit issuance and, in conjunction with the low interest rates, skews the market, creating a price structure disequilibrium that results in the misallocation of capital goods. Economic calculation is altered in the boom (a sustained growth in some economic indicators) because of the price structure disequilibrium, making bad investments (that are not profitable when looking at their real value) seem good (profitable when looking at their nominal value).

The boom cannot be sustained indefinitely because that would need a constant, exponentially growing credit expansion. This results in the bad investments being sold for less than their original cost and toward equilibrium, leading to a contraction in the money supply and eventually a bust. Fiscal and monetary policies of low interest rates prolong the bust. In short, Austrian economists reject the idea that an increase in the money supply, for other reasons than to decrease transaction costs, is helpful for the society. When the amount of some other goods is increased, the society benefits from the increase. When the money supply is increased, the price of money diminishes[10], leaving the public unaffected at best, poorer at worst (Mises, 1953, p. 17).

Mainstream economists believe that the boom is beneficial and that the bust is a problem that needs to be maintained while Austrian economists believe the opposite; the bust is a consequence of the boom that needs to be prevented in the first place. Fractional reserve banking is one of the tools necessary to make excessive credit expansion possible and the easiest way to prevent the booming phase (without considering any external problems) is to implement an inelastic money supply and limit fractional reserve banking.

7.1 The Austrian school definition of money supply

Before discussing how the money supply of Bitcoin functions, it must first be clarified what the money supply precisely consists of. Austrian economists use a strict definition of what constitutes as the money supply. The money supply is composed of money substitutes and money in the narrow sense used throughout this thesis. If the financial

[10] In accordance to the quantity theory of money, ignoring the theory's focus on the supply of money.

instrument is not used as a final payment in all transactions, it is not a part of the money supply from an Austrian viewpoint (Salerno, 2010, p. 116). Because of this, bank notes are not a part of the money supply, even though they are generally considered a money substitute.

7.2 Bitcoin substitutes and fractional reserve banking

7.2.1 Bitcoin substitutes

The expansion of credit by means of fractional reserve banking for example, requires money substitutes since commodity credit cannot be expanded, circulation credit however, can (Mises, 1998, p. 431). Saving deposits and other instruments that have zero maturity, but are not used as a medium of exchange, are not a part of the money supply from an Austrian perspective. When a withdrawal is made from a savings account, two things can happen. Either the bank's reserves decrease, which leads to an increase in circulation credit, or the credit is moved to another account, increasing the balance of a current account so the volume of transferable bank balances a type of money substitute, rises (Surda, 2012, p. 44).

What this means is that if a credit expansion is to happen, given the Austrian school is right, it will happen by utilizing money substitutes. These substitutes emerge in the same way other media of exchange does, by being a competitive, viable alternative to the monetary base. Money substitutes however, as the name implies, require already established money in order to exist. Therefore, they are unable to compete with the existing money in regards to liquidity or being a store of value. Money substitutes only possess possible advantage to the monetary base in one category, transaction costs (White, 1984, p. 705).

What does this have to do with Bitcoin? Bitcoin has low transaction costs compared to other, more traditional forms of exchange media. In fact, the transaction costs are so low it is highly unlikely a Bitcoin substitute will ever appear. This is especially true when considering that Bitcoin already possesses many of the qualities that the market searches for in money substitutes, such as convenience and speed of transfer (mostly regarding transfers between countries). The transaction costs, as has been argued, are very low but might get higher in the future as the natural incentive to mine (because of the bitcoin rewards) slowly disappears. However, counter parties could never offer

lower transaction costs without taking a loss because they need to maintain themselves. In addition, the counter parties would need to subsidize some of the transaction costs just to keep their services feasible for users. The simple fact is that there is not a single service that third parties can offer that lowers transaction costs or makes transacting more convenient than what users of Bitcoin are already experiencing. Counter parties that offer increased anonymity for some risk (and more often than not, payment) exist of course, but those parties are not *in it* to lower transaction costs.

The only plausible way for Bitcoin substitutes to emerge is through government intervention. If governments were to fix exchange rates, then it is possible that money substitutes could emerge. This however would require Gresham's law of bad money driving out good money to affect Bitcoin, which as will be shown in the next chapter, is not clear considering Bitcoin is not legal tender or a dominant medium of exchange and furthermore, technological advancement could make Bitcoin's transaction costs increasingly lower, minimizing the likelihood of substitutes.

Another scenario where government interaction could make way for money substitutes, described by Suede, is when the government directly or indirectly (through regulations for example) confiscates bitcoin reserves (Suede, 2012). However, when Suede argues that money substitutes, such as Bitcoin notes issued by banks, could emerge from government confiscation, he presupposes that the inherent practical value of Bitcoin alone (as set originally by New Liberty Standard using electricity and other factors) gives the government complete control over the monetary system when the coins are seized. This is wrong. Bitcoin's value has surged far beyond what their value is as a measure of physical labour (a clear demonstration of Bitcoin as synthetic commodity money). If all bitcoins in existence were confiscated by authorities, leaving common users with nothing but a number of how many bitcoins they can redeem through digital notes in their account, it would not matter. The digital notes would gain value through the regression theorem just as bitcoins did. Bitcoins themselves only gain value through their qualities of low transaction costs and convenience, which means that even if governments would confiscate the bitcoins, the network effects Bitcoin has already accumulated would be enough to drive transactions in a usual manner.

It just does not make sense for the government to use fractional reserve banking in this regard, as the digital notes that are tied to Bitcoin are not actually tied to anything with inherent value, unlike credit money. The natural progression, of tying credit money to gold and slowly convincing the public that bank notes are the equivalent of gold until the public perception allows the government to cut the ties (turning the credit money into fiat money) that can be utilized in fractional reserve banking, is simply not possible when using bitcoins. This is one of the differences between commodity money and synthetic commodity money regarding their connection to fiat money. Even if fractional reserve banking would be a theoretical possibility, it could not work in practice, since the operating payment systems used by both *bricks and mortar* businesses and online businesses are designed with direct Bitcoin payments in mind. Therefore, the network effects create a strong incentive for users to reject a paradigm shift such as the one government confiscation would produce.

7.2.2 Fractional reserve banking and Bitcoin

The Keynesian viewpoint is that fractional reserve banking is entirely possible using bitcoins. Banks are allowed to accept bitcoins and make them available for withdrawal while lending a large portion of their reserve for profit. The block chain would not change but the perceived amount of bitcoins in circulation would surely be altered.

The monetary base of Bitcoin is limited, so for fractional reserve banking to work from a Keynesian perspective, a credit currency linked to the Bitcoin reserve must first be created in order to use the money multiplier. According to Keynesians, if Bitcoin's price stays stable for long enough, fractional reserve banking of it will prove inevitable (Bitcoin Wiki, 2013). Although theoretically possible, this is improbable, since Bitcoin lacks a central bank, making bank runs a real threat to account holders. With no central bank and no Federal Deposit Insurance Corporation (FDIC) insurance system, the financial institution providing the fractional reserve banking will be hard pressed to find a way to *backstop*[11] their reserves (Suede, 2012).

[11] Meaning the act of providing last resort support or security in a securities offering for the unsubscribed portion of shares (Investopedia, 2014).

The Keynesian school of thought is right in the regard that it is *possible* to do fractional reserve banking using bitcoins, but to take part in it would be akin to invest in a stock of a risky company (Suede, 2012). Since there is no central bank insurance, agents would *invest* in a company called for example *The Bitcoin Bank* by depositing bitcoins with hopes of gaining interest on them. The Bitcoin Bank would proceed to issue Bitcoin notes guaranteed by themselves, allowing them to loan out a larger amount than their reserves can cover in case of a bank run, making them continually insolvent[12]. Ignoring the problems associated with issuing Bitcoin notes (money substitutes), it is hard to imagine that after The Bitcoin Bank has paid themselves a portion of the interest on the loans that do not default, that the profit gained by the *stockholders* is worth the risk. This question is especially relevant when considering that there is no need for such a company, as bitcoins can be divided into extremely small units. In fact, the only thing such a company does is accumulate bitcoins at the risk of others. It is therefore highly unlikely that a financial instrument like that will be successful unless it acts in an illicit manner such as disguising their operation or providing misinformation.

From an Austrian perspective, the only way for fractional reserve banking to affect the money supply is if the debt instruments used are money substitutes. Money substitutes have been accepted from an historical standpoint because they sometimes have a lower transaction cost (gold for example being too heavy to carry around) or are otherwise convenient.

Issuers that want to create a fractional reserve system need to create a demand for debt instruments (money substitutes) as a payment outside of the Bitcoin system. Bitcoin users do not generate enough demand for more convenient forms of media of exchange to warrant the emergence of money substitutes. There are exceptions, certain debt instruments such as e-wallets and stock-trading platforms for bitcoins are used for specific purposes but are not accepted as freely as bitcoins in general exchanges and are rarely seen outside of their particular niche (Bitcoin Wiki, 2013). Expected technological advancement within the Bitcoin community (distributed wallets and peer-to-peer

[12] Meaning that they cannot pay all debts if it comes to that.

exchanges are already being analysed) will decrease the need for money substitutes further (Bitcoin Wiki, 2013). Furthermore, when establishing a fractional reserve system within the Bitcoin network, the money substitutes must be used in payments outside of the network, meaning that the issuer would need to compete against all other payment methods, services, and currencies, along with Bitcoin. This also means that users that only have the basic Bitcoin client cannot utilize these substitutes. These problems affect both the Austrian and the Keynesian view of whether fractional reserve banking is possible or not.

For a fractional reserve Bitcoin system to function, three things must happen. There must be an excessive issuing of debt instruments, which must then become a part of the money supply (becoming money substitutes) by being accepted as a method of payment. Finally, the substitutes must be subject to inflation or deflation by having the reserve ratio of the issuer a different rate from the market price of them (Bitcoin Wiki, 2013).

8 Complications of Bitcoin

There are several problems with the design of Bitcoin. That is to be expected, considering that the design was the first one of its kind, in any case it is of great importance to list flaws as well as merits for the analysis to hold any value. By far the largest flaw of Bitcoin is a possibly problematic design choice. Since the total number of bitcoins is fixed at 21 million, Bitcoin has a severe weakness to money demand shocks. The demand of Bitcoin has a direct effect on Bitcoin's purchasing power if it changes, and will therefore increase fluctuation. This makes Bitcoin very volatile, as we have seen in the following years where, in hindsight, minimal problems crashed the value of bitcoins and speculators subsequently drove the price back up.

8.1 Network effects

Network effects have proven to be problematic to the emergence of Bitcoin. The status-quo bias is highly relevant in this scenario where the limited network of Bitcoin serves as a vicious circle. A very limited number of agents will accept bitcoin as payment for goods and services because of that exact reason. This might be the result even though bitcoin would be a superior currency, given that the value of holding the status quo is greater than the difference between the currencies (Luther & Olson, Bitcoin is Memory, 2013, p. 7) (Luther, 2013, p. 34).

Network effects and switching costs are likely the main reason for why Bitcoin and other crypto-currencies have yet to gain widespread acceptance (Luther, 2013, p. 4). A model developed by Dowd and Greenway (1993) can be used to predict currency acceptance. This is done by using the premise that money is subject to a network effect whereas the value conferred to a currency user partly depends on how many others are willing to engage in transactions using that currency (Luther, 2013, pp. 4-5). It is also based on the notion that there is an associated cost with switching from one currency to another, called a switching cost. This cost encompasses for example the cost of changing menus and transaction records, learning to think and calculate in terms of a new medium of exchange and retooling vending machines (Luther, 2013, p. 5). Based on two variables, it is possible to articulate whether users will switch to a different currency or keep the same one, a suboptimal choice (Luther, 2013, p. 5).

The model states that since agents within it are homogenous, no one will switch if switching costs are sufficiently high and everyone will switch if the switching cost is sufficiently low (Luther, 2013, p. 8). This is as straightforward as it gets, the model gets a bit muddier however when the switching cost lands between those two boundaries. On one hand, there is the possibility that some agents will use the old currency in a situation where maximization of social welfare would be a result of all agents switching to the new currency. On the other is the possibility that some agents will switch over to the new money while the maximization of social welfare occurs when all agents to reject the new money and keep using the old money (Luther, 2013, pp. 8-9). These two possibilities, that have been named excess inertia and excess momentum, will now be analysed further (Farrell & Saloner, 1986, p. 940).

8.1.1 Momentum and inertia

8.1.1.1 Excess momentum

Excess momentum is considered an unlikely scenario since historical record has shown that agents cannot learn beliefs that match fiat money equilibria by themselves because no agents accept intrinsically worthless items from the beginning, making it futile to believe that it will ever be accepted (Luther, 2013, p. 11). This is the result of agents behaving from historical precedence and being at least less than hyperrational. Hyperrational means that agents have unbiased beliefs, and the cognitive capacity to make optimal decisions from those beliefs. This means that any new fiat money is dependent on having been operationally linked to some other established money for it to be of any positive value at all (Selgin, 1994, p. 823). When looking at the situation, with historical acceptance in mind, it is easy to presume that when agents try to coordinate they will look toward the current official money as a default option (Luther, 2013, p. 12). This has been tested empirically with human subjects as well as agent-based computational models where agents are assumed to employ adaptive learning, and the results are consistent with these views (Luther, 2013, p. 13).

8.1.1.2 Excess inertia

Because of the prevalence of historical acceptance in the act of coordinating the adoption of new currencies, excess inertia proves to be a larger problem than the possibility of excess momentum. Historical acceptance allows agents to support

suboptimal monies when there are other superior choices available, as such, it may increase the problem of excess inertia (Luther, 2013, p. 15). When current money provides sufficient efficiency, it may be hard to persuade agents that others will switch to more socially optimal money, when available. Therefore, it seems as the status quo has a strong standing, given that it is sufficiently close to the superior alternative. The solution to excess inertia depends largely on the cost of coordination. It is more likely that agents will make the optimal switch if it is possible to coordinate in a cheap manner. If the possibilities of coordination are not powerful enough, too expensive or somehow cannot overcome the hindrance generated by the historical focal point, it is reasonable to assume that agents will not collectively make the optimal switch (Luther, 2013, p. 15). For agents to switch to superior money they must have some way to communicate and furthermore they must have some focal point that allows them to break from the status quo of, for example, historical acceptance (Luther, 2013, pp. 15-16).

8.1.2 Bitcoin and network effects

Selgin (2013) stated a problem called *the oyster problem*, after articulating that the first person to eat an oyster must have been exceedingly brave or crazy, maybe a bit of both (Selgin, 2013). The first person to accept Bitcoin as a medium of exchange in the vague hope that someone else can be fooled into accepting them in return for other goods must have been cursed with the same traits as the oyster eater (Selgin, 2013). The difference between accepting bitcoins and commodities, before they became a media of exchange, is that even if the person that accepted the commodity could never find anyone else to accept it, that person would still have a valuable commodity to be used (such as salt, spices, gold, silver, and so forth). The first person to accept Bitcoin as a medium of exchange had to take a leap of faith and hope that others would do the same (Selgin, 2013). This is akin to the greater fool theory that states that the price of something is often determined by the irrational beliefs and expectations of market participants (Investor Glossary, 2014). So how did Bitcoin manage to overcome the oyster problem? Selgin suggests that Bitcoin has three qualities that made a unique, desirable medium when combined. Bitcoin has an eventually inelastic supply with a steady, predictable growth until then. It offers almost untraceable transactions and it

can, and in most cases does, circulate electronically, leaving no paper trail and bypassing all face-to-face contact (Selgin, 2013).

These qualities were in demand but that did not guarantee that Bitcoin would be picked up as a medium of exchange, even though it fulfilled this niche (Selgin, 2013). A speculation is that those driven by ideologies, such as libertarian or anarchist viewpoints, were the first users. Another theory is that people originally mined bitcoins because it was easy, making the low effort almost certainly worth it. From there you have many people with accounts and bitcoins and a possibility of using the system the way it was designed to work. In truth it is hard to estimate what exactly made people accept Bitcoin to begin with, although speculations such as these might help establishing a broad perspective.

It is evident when the total transaction volume of Bitcoin is examined that although Bitcoin and other cryptographic currencies have gained some significant movement, especially within the young, tech-savvy community, they have not gained widespread acceptance, thus making Bitcoin a secondary medium of exchange at best (Luther, 2013, p. 16).

In February 2014, it has been estimated that the maximum theoretical number of Bitcoin users is around 2.5 million. The reality however is that many of those addresses are empty and a more realistic cap is around 1.2 million unique users. Of those possible 1.2 million unique users, almost a million of them own only around 87 thousand coins. The rest, around 250,000 addresses distribute the rest of the Bitcoins between them, where only 87 addresses own more than 10,000 coins and only two of them own more than 100,000 coins (Hurst, 2014). It is important to note however that many exchanges, such as the infamous Mt.Gox, probably held the balance of many users in a few wallets, making the guessing of the size of the user base just that, guesswork. If we accept the premise that Bitcoin has some very desirable traits that other monies lack, it is hard to welcome the notion that Bitcoin is inherently worse than official monies. The reason for the lack of widespread acceptance must stem from some other source, which follows the model Luther made based on the work of Dowd and Greenway adequately, as money being superior to alternatives does not render it automatically successful (Luther, 2013, p. 26).

The net benefits of switching must be large enough to warrant the cost of switching. That is however not the only condition that must be fulfilled for a medium of exchange like Bitcoin to become widespread (Luther, 2013, p. 27). An example can be made where the cost of switching is sufficiently low for agents to know that Bitcoin is a superior alternative to the official money and would switch to Bitcoin if they had knowledge of all other agents doing the same. In this example, Bitcoin should become the official medium of exchange; instead, it shares the same fate as if the switching costs were higher than the value of network effects because the agents in the example find it difficult to coordinate (Luther, 2013, pp. 27-28). The problem then becomes that there is not a sufficiently strong focal point that can compete with historical acceptance and from there overcome the status quo. It is therefore near impossible to find an agent that is willing to take the step ahead of everyone else, put in other words, no one wants to be the first to discontinue previous acceptance of the ruling money (Luther, 2013, p. 28).

8.1.3 The cost of switching

The imagined cost of switching is not necessarily as high. The technology to accept bitcoins is already used by vendors, although it is not used for that purpose yet. The amount of smartphones makes it easy to keep track of account balances and currency conversions. It is not a huge commitment for most to learn to think in terms of the new currency but even so, it is not of great importance to do so. Prices could simply keep being quoted in the traditional currency while the electronic payment system converts the prices to Bitcoin at the current exchange rate (Luther, 2013, p. 27). There are some ways for monetary transitions to arise in a successful manner. Government support is a huge factor. A centralized authority serves as an alternative focal point and diminishes the influence of historical acceptance of the official money. One way for governments to support a new currency and by doing so, a new monetary regime, is to link the official money to the new currency using a fixed exchange rate. When looking at the successful monetary regime transitions in the past, such as the South Sudanese pound in 2011 and the Somaliland shilling in 1994, this is exactly what happened. The governments tied the new currency to the old one using a fixed exchange rate, which has resulted in a general acceptance within the regions (Luther, 2013, p. 32).

There are empirical examples that support this from the notion that governments can effectively determine the medium of exchange if they conduct a sufficiently large portion of the total transaction volume (Aiyagari & Wallace, 1997, pp. 1-2). Ritter (1995) supports this but has stressed that it is important for governments, if they are supporting a monetary transition, to limit the supply of money (Ritter, 1995, p. 135). Another path for governments is to anchor expectations by either committing to the new currency in the form of a viable source of tax payments or refusing to accept the incumbent money as tax payments (Luther, 2013, p. 32). Government intervention can be both beneficial and detrimental; it can enforce excess inertia just as well as it can remedy it. Furthermore, it can endorse alternative money when the switching costs are sufficiently high to make it a worse option than historical acceptance, but not a strictly worse option. In these cases, some agents might switch even when their prospect lies in the continuous use of the traditional money. Government interventions can theoretically then make excess momentum a real problem if the focal point created is stronger than historical acceptance (Luther, 2013, p. 33).

Meddling governments are not the only prerequisite for a successful adoption of a new currency. Hyperinflation has been shown to encourage the use of alternative monies, both in scenarios where the government supported the transitioning and others where hyperinflation induced unofficial monetary transition. This change is near instant and a switch is made to superior money that is available. The change is spontaneous because hyperinflation makes the historically accepted money become strictly worse; this in turn lowers the switching costs and coordination costs, making it increasingly likely that the costs become sufficiently low. Finally, it is extremely hard for agents to fail to notice hyperinflation, effectively making the deterioration of the incumbent money common knowledge and thus a focal point (Luther, 2013, p. 33). This noticeable focal point serves as a coordination device, since agents are losing faith in the official money and individual agents know that agents as a whole are losing faith in the official money and so forth (Luther, 2013, p. 34).

8.1.4 Summary of network effects

Consider that an alternative focal point were to be found that would gather more trust than the one made of historical acceptance. Even so, historical acceptance might be the

dominant focal point if the coordination costs of Bitcoin are too high. Unfortunately, that seems to be the case for Bitcoin, a decentralized system has been praised throughout this thesis but ultimately becomes its tipping point into inertia. A lack of centralization in combination with a lack of communication between certain groups leads to a widespread failure to recognize Bitcoin as viable alternative money. This happens even though Bitcoin is a superior medium of exchange in many ways and has the technical possibility of global adoption (Luther, 2013, p. 28).

Bitcoin does not have to be flawed or otherwise inferior to other monies for this to be the conclusion. It is the decentralized nature of Bitcoin that does not function fully with the mechanics of monetary transitions from one currency to another. The discrepancies between the impact of excess momentum and excess inertia lead to a clear bias, a systematic one at its core, against monetary transitions, the status quo (Luther, 2013, p. 28).

In recent years, all occurrences of successful monetary transitions have been from unsustainable currencies to relatively stable ones. Bitcoin however tries to replace relatively stable currencies without any real governmental support. It is uncertain if Bitcoin's qualities of pseudo-anonymity, low transaction fees, and global presence outweigh the problems of volatility and instability it faces. Indeed, it is in many ways a subjective estimation based on factors such as whether the estimator is risk averse or risk seeking. Even if the benefits outweigh the flaws, it is still not certain whether that would be enough for a successful transition. It is likely that a significant monetary instability or government support, preferably both, is needed for Bitcoin and other crypto-currencies alike to find widespread acceptance in their quest to become a primary medium of exchange (Luther, 2013, p. 34).

8.2 Volatility and bubbles

Bitcoin has high amounts of volatility. This can be observed by looking at recent price crashes from 2011 until now, where it has dropped significantly in value at least six times (Lee, 2013). These crashes occur because investors treat Bitcoin as a speculative bubble, where something as innocent as positive news coverage creates a surge in bitcoin buyers that raise the price of bitcoins (Brito & Castillo, 2013, p. 20). Eventually the price plummets but bitcoins are still around even when the price has plummeted

after bubble-like surges a few times already. It must be noted that some critics think that Bitcoin is in a perpetual bubble state because it has no intrinsic value. However, even gold and other commodities used as media of exchange derive a large portion of their value from simply being a media of exchange. Therefore, it could be said that if Bitcoin is currently a bubble then gold has been a bubble every time its exchange value was higher than its industrial and ornamental uses could account for (Murphy, 2013).

One speculation is the composition of bitcoin, which is proving to be troublesome in regards to volatility. Bitcoins are composed of commodity and currency, stated earlier as synthetic commodity money. The commodity aspect of bitcoins gains value through the medium of exchange aspect, the problem is that as investors increasingly treat bitcoins as a commodity and by doing so, diminishing their uses as a medium of exchange (Salmon, 2013). The origins of bitcoins make this almost unavoidable, since network effects made sure that at the launch of Bitcoin, they were generally not accepted as a medium of exchange (even though Bitcoin has taken great strides of development toward becoming a currency) which encouraged their use as commodity. This was only exacerbated when investors figured out that bitcoins might eventually be accepted as currency, which drove their commodity value up in the present day. This volatility could either be the cause of Bitcoin's decline or simply a thorough stress test (Brito & Castillo, 2013, p. 21).

8.3 Spirals and babysitting

It could be argued that since crypto-currencies that follow the design of Bitcoin, and are not capable of expanding the money supply in a nominal fashion, they cannot stabilize the economy at a macro level in case of depression (Selgin, 2013, p. 1). A counter argument can be made to exemplify that Bitcoin's design possesses the ability to circumvent the traditional complications of fiat money. A classic example would be Capitol Hill Babysitting Cooperative (CHBC), a real life example, described by Sweeney and Sweeney (1977) and later popularized by Krugman (Krugman, 1995). Sweeney & Sweeney discuss how a babysitting cooperative fell into recession. Members of the cooperative earned scrip for babysitting for other members and could subsequently use the scrip to pay someone else to babysit for them. The scrip supply in circulation diminished slowly because of structural reasons, involving the collection and use of

dues that were paid in scrip, which worried the members of the cooperative, as they could not be certain of getting scrip anymore. This was because of a lack of babysitting opportunities. The members used their stored scrip more sparingly than before because of this and the result was a deep recession within the cooperative (Sweeney & Sweeney, 1977, pp. 86-88).

Krugman (1998) uses this example to show how deflation can hurt the economy (Krugman, 1998). The problem is that he assumes that scrip is the same as money; this might apply about fiat money but bitcoin is certainly not like a regular currency. It is possible to split bitcoin into fragments of 0.00000001. That means that even with deflation and prices getting lower, the true *final* amount of nominal bitcoin units is 2.1 quadrillion, or $2.1x10^{15}$. To put this amount into perspective, imagine where each satoshi, or the smallest unit of Bitcoin, represents a US penny. If all the satoshi units (or pennies) would be stacked in the form of a cube, it would be over 3,500 cubic feet. In other words, each side of the penny cube would span over a kilometre. This nominal amount is more than enough to satisfy the needs of the public and there would not be any need to tear scrip or otherwise change the value of individual pieces of scrip.

In Krugman's example, it could also have been possible to account for the actions of the market, namely that each unit of scrip would simply buy more than one-hour babysitting time or tear the scrip in pieces and make each piece worth an hour of babysitting. The practice of tearing paper notes is frowned upon in the real world, since a central authority has a monopoly over the total supply of notes; bitcoin however has the possibility of being divided almost at will.

Another criticism is that because of the nature of Bitcoin, it could succumb to a deflationary spiral. Since the supply is inelastic, bitcoins will appreciate greatly if the medium of exchange would gain widespread acceptance. Barber, Boyen, Shi, and Uzun (2012) take a modest example of a mature market with 99% of the US GDP transacted in dollars and 1% transacted in bitcoins. In that economy, the real purchasing power of bitcoins would still increase, thereby containing a fraction of the economy's growth. The Federal Reserve can issue more currency to accommodate for economic growth but Bitcoin does not have that option. Instead, all of the economy's growth must be

channelled through appreciation when Bitcoin is the ruling medium of exchange (Barber, Boyen, Shi, & Uzun, 2012, p. 404).

This can lead to a deflationary spiral that follows from moral hazard. Because of the constant appreciation, people have an incentive to hoard bitcoins instead of spending them, unlike most fiat currencies. Hoarding of bitcoins can lead to diminishing transaction volume, which then leads to fewer fees for block creation by proof-of-work. When circulation has dropped sufficiently low, interest in the Bitcoin system might dwindle, leading to increased probability of 51% attacks and a weak system that has a hard time staying relevant (Barber, Boyen, Shi, & Uzun, 2012, p. 404).

Peercoin solves this problem elegantly by using a built-in inflationary mechanism. Furthermore, an economy using appreciation as an outlet for growth is not inherently bad when taking into account how bitcoins differ from traditional currencies. Bitcoins can be divided freely, into very small units, for no cost.

8.4 Gresham's law

An economic concept called *Gresham's law*, states that bad money drives out good money, but good money cannot drive out bad money. Another way to put it would be to say that cheap money drives out expensive money (Fullenkamp & Nsouli, 2004, pp. 4-5). These are generalizations but rather accurate ones. Gresham's law is generally applied to explain why newly minted coins were so hard to get into circulation. People decided to keep the newly minted coins for smelting them, turning them into jewellery, or otherwise use them in other ways than intended. Meanwhile the old coins were kept in circulation because they were ugly and worn and the public saw no use for them other than as a medium of exchange. From Gresham's law we can deduct two pre-emptive measures when regulating a currency to avoid problems relating to it. Firstly, newly minted coins must be as close to identical as the standard coins in circulation to hinder arbitrage opportunities. Secondly, worn out coins that have deteriorated below the minimal legal weight must be taken out of circulation. Although this old theorem is only applied to metal coins it can be extended to successfully apply to all kinds of money in the same circulation, whether it is copper, paper, silver or gold (or something else entirely) (Jevons, 1875, pp. 79-82).

It has been argued that the Bitcoin system breaches Gresham's law. Botnets can be created through cyber-criminal activity, where malicious software infects computers so hackers can utilize the computer power of unsuspecting citizens. These botnets could theoretically then be used to mine bitcoins. Although this has not yet been done (as far as records show), it might exacerbate some of the problems Bitcoin has. Gresham's law originates from the principle that the most efficient resource is used. The proof-of-work of Bitcoin costs computational power, which would otherwise be used elsewhere. If these botnets mined bitcoins and put them into circulation, honest-mined-bitcoins would be circulating alongside stolen-electricity-bitcoins, both types having the same price. To modernize the terms used earlier; stolen electricity beats out honest mining (Grigg & Güring, 2012, pp. 4-5).

It is easy to refute these claims however; Gresham's law only applies when the government at hand sets the value of both the *good* and the *bad* currencies. This is not the case with bitcoins. Furthermore, if Gresham's law is followed, and a situation is imagined where a person has a choice of paying with a depreciating currency (fiat money) or an appreciating one (bitcoins as synthetic commodity money which will eventually become inelastic), that person will pay with the depreciating currency and choose to hold on to the appreciating one. This would limit the widespread use of the appreciating currency. This is often called the reverse Gresham's law or *Thiers' law* (Rolnick & Weber, 1986). Another rebuttal is that there is little empirical data that the cost of mining has an effect on either the price of bitcoin (the practical formula used to determine the original price of Bitcoin, shown earlier in this thesis, was created using general assumptions) or the quality of the coins.

The coins are indistinguishable whether they are made with stolen electricity or not, the only difference botnets would make is that the hash-difficulty algorithm would increase the difficulty at a faster rate since there would be more overall power used for mining. This would eventually make the final amount of bitcoins, 21 million, come about faster than it otherwise would, assuming that the efficiency of botnet usage grows faster than the hash-algorithm's difficulty for a sufficiently long period. What Grigg and Güring are really arguing about is a problem of externalities, externalities which exist

between the computer owner (victim) and the botnet owner (offender). It is true however that if anything poses a risk to the 51% attack, it is the utilization of botnets.

Rolnick and Weber set forth a critique of Gresham's law, especially regarding the universal applicability that the status of being a *law* implies. The article argues that there are too many unexplained exceptions to this supposed law. When a small portion of the history of US and English coinage reveals examples that do not conform to the predictions of the Gresham's law. Many of those instances showed both good and bad money being commonly used. A suggestion of improvement to Gresham's law is made, where bad money drives out the good in circulation, strictly when the costs of using good money at a premium are significant (Rolnick & Weber, 1986, p. 198).

8.5 Other risks

The Financial industry Regulatory Authority (FINRA) published a short list of risks associated with bitcoins on their website, which was updated on March 11th, 2014 (Mont, 2014). These risks include that Bitcoin is not legal tender, which means there are not any laws that require corporations or individuals to accept it as a form of payment. As such, Bitcoin might become worthless due to a lack of confidence in Bitcoin. The platforms used by the intermediaries can also be hacked and the digital wallets themselves can be hacked if precautions are not made. It is possible to pose as a Bitcoin exchange, third-party intermediary, or a trader in an effort to steal money; however, that is not different from frauds that occur in other currency systems.

Money substitutes in general are vulnerable to risks that stem from the (somewhat necessary) need of counter parties. Bitcoin, although not a money substitute, is also subject to some counter-party risk albeit not a legal one. If a user wants to obscure his identity further than the basic Bitcoin protocol allows for example, he must use a third-party laundering service, which solely relies on that service to operate within a certain moral framework. Bitcoin, along with gold, is however not subject to central bank policy like fiat money and other forms of money substitutes, which some might call a special kind of counter-party risk.

A great example of a counter-party risk is an infamous Bitcoin exchange Mt. Gox, which was launched in 2010. By 2013, it had become the largest Bitcoin exchange on the market, handling over 70% of all Bitcoin transactions (Vigna, 2014). In February

2014, it suddenly closed down and filed for a type of bankruptcy protection from creditors. In April Mt. Gox announced that 850,000 bitcoins that belonged to users of the exchange were missing and likely stolen. However, around 200,000 coins have been found since their statement, making the reasons for the shutdown unclear. It could be that the management behind Mt. Gox *cashed out* and proceeded to cover their tracks, or it could be hackers, it is simply unknown. The anonymity and lack of regulation to follow render this situation unlikely to be resolved in the near future (Abrams & Popper, 2014).

There is a lack of safeguards for digital wallets that provide guarantees of safety to the owners, unlike credit unions and banks, which can offer certain guarantees. Finally, the FINRA warns that Bitcoin has been used in illegal activity and abuses could harm the consumers and speculators if law enforcement agencies shut down or restrict the use of platforms and exchanges of Bitcoin (FINRA, 2014). As the director of FinCEN has said, Bitcoin transactions in illegal activities have yet to overtake more traditional methods for moving funds internationally (Mont, 2014). And since traditional methods such as fiat money have yet to be banned by authorities, there should be no reason why Bitcoin should be banned, even though they would overtake traditional currencies in illicit activities. After all, that would only put them in the same place as traditional currencies are in now.

Finally, governments have a monopoly of money in a narrow sense, they are the issuers of it and control to some extent the laws and regulations surrounding it. There are therefore barriers-to-entry because of banking regulations. Traditional e-money needs to amass huge capital before being allowed on the market for example. The users and innovators of Bitcoin are not affected by these barriers in a negative way. It could even be positive since the competition is weaker because of those regulations, allowing the qualities of Bitcoin, such as relatively free global transactions, to have a greater effect.

9 Regulating Bitcoin

Bitcoin has grown tremendously since its inception and following that growth in usage, some agents have shown concern and are looking toward a path of regulation (Bitcoin Charts, 2014). In April 2012, long before bitcoins surged in value in November 2013, The Federal Bureau of Investigation (FBI) published an intelligence assessment regarding the challenges that the unique features of Bitcoin present. It is hard for law enforcement agencies to observe and detect suspicious activity since there is no centralized authority within the Bitcoin framework. Even so, it is nearly impossible to identify smart users that know how to cover their tracks. The anonymous nature of Bitcoin makes it a suitable currency for illicit activity (Federal Bureau of Investigation, 2012, p. 4). Before Bitcoin and other similar cryptographic currencies, some criminals had used virtual payment schemes to launder money.

Bitcoin makes the same options as other electronic currency systems (Webmoney, Liberty Reserve, and Pecunix to name a few) such as laundering, transferring, and stealing, possible for criminals. Because Bitcoin is decentralized, it is at a greater risk of being used for illicit money transfers and, according to the FBI, manipulation using malware and botnets. Both points can be refuted to some extent. Bitcoin also differs from other electronic payment systems for many reasons, but it does so especially regarding anonymity. Other electronic payment systems operate as companies that must comply with the Bank Secrecy Act (BSA) through the enforcement of centralized organizations (Federal Bureau of Investigation, 2012, p. 5). Bitcoin however, as a decentralized system without an authoritative entity, does not have the capability of conducting the implementation of regulatory guidelines. It is further incapable of monitoring and reporting suspicious activity and has no systematic way of processing legal requests. It is also nearly impossible for the Bitcoin system to implement an anti-money laundering compliance program (Federal Bureau of Investigation, 2012, p. 5). The FBI states that as long as bitcoins can be converted into real money, criminal actors will have an incentive to steal them (Federal Bureau of Investigation, 2012, p. 10). This statement, along with the ones already made, are factually correct but seemingly irrelevant when trying to navigate within a specific frame, since the statements apply almost universally to all valuable media of exchange.

The exception would be the statement about botnet vulnerability, although that can easily be refuted simply by illustrating how the Bitcoin system works. Bitcoins can be used for illicit purchases, but then again, that is nothing new under the sun. Cash, electronic credit transfers, Paypal-like systems, and bartering of services and goods have all been used to for illicit purchases in the past. If anything, it would be odd if Bitcoin would not adhere to the same laws as other forms of currency. Even if bitcoins are pseudo-anonymous, the argument has been made that in order to use them, there has to be some revealing properties of the transaction. If the criminal agent could take such extreme precautions with bitcoins as to remain completely anonymous, rest assured, he could do it with other currencies as well. The manipulation involves bypassing the double-spending protection inherent to the Bitcoin system by making a 51% attack. It can be argued that the minimal risk of a 51% attack is a low price to pay for a currency that has a transparent transaction record keeping and solves a myriad of other problems, such as counterfeiting.

If the government were to regulate the utilization of bitcoins, the negative externalities it might evoke could prove to be disastrous. Current regulations and laws regarding currencies do not take into account the technological advances in recent times. Bitcoin is a prime example of a technological achievement that has not yet been defined by the law; it is not a currency and not a commodity, it is just Bitcoin (or as we have learned, synthetic commodity money, which also happens to be outside the scope of, seemingly, all regulation). The consequence is that bitcoins, and the framework around them, are enveloped in legal ambiguity where it is not certain which laws and regulation apply in any given circumstances involving them (Brito & Castillo, 2013, p. 27). This is a common side effect of disruptive technology (Brito & Castillo, 2013, p. 38).

If bitcoins are to be restricted by regulations, it must be done in a careful manner. A good example would be the legal surroundings of VoIP (Voice over Internet Protocol). VoIP was, similarly to Bitcoin, a cheaper option with increased efficiency. It emerged on a highly regulated market composed of a traditional telephone network. Although there are still issues with VoIP that are causing the US Congress and the Federal Communications Commission (FCC) headaches, much of the legal ambiguity has been cleared (Brito & Castillo, 2013, p. 27). This has resulted in innovation and fresh

competition to an otherwise stagnated market that has led to lower prices and improved access for customers.

The notion that should be taken from this example is that in order for Bitcoin to blossom, it is of the essence to impose restrictions and regulation in a limited and sensible manner (Brito & Castillo, 2013, p. 28). One of the biggest reasons Bitcoin will eventually be under some form of regulation is to prevent illicit activity such as drug trades through the deep web. It will be challenging to regulate Bitcoin in a way that it will remain useful while minimizing its potentially harmful uses (Brito & Castillo, 2013, p. 38). Just like any other medium of exchange, Bitcoin is not inherently good or bad, although its increased anonymity might encourage criminals to consider bitcoins above most other media of exchange. However, the same could be said of cash (as cash conceals the identity of the purchaser better than bitcoins when considering long-term transaction history).

A part of the problem with bitcoins is that it is much easier to observe illegal activity than with cash transactions. It is likely that as the Bitcoin user base grows, the illegal activity, as a ratio of total transactions, diminishes far below that of legitimate transactions similarly to what happened with fiat money (Brito & Castillo, 2013, pp. 38-39).

Another argument for the neutrality of Bitcoin can be made. It is a strange premise to assume that agents decide which medium to use based on what they want others to use the medium for. They base their decision on what preferences they themselves hold and not the preferences of others. Agents therefore choose the medium of exchange according to their own preferences, which implies that Bitcoin is not the problem, but the illicit users, just as it is with other types of media of exchange such as prepaid account cards and cash. The Recording Industry Association of America (RIAA) provides an example of an organization making a futile attempt to ban the internet. The RIAA failed partly because of how strictly they handled each case, charging illicit downloaders for thousands of dollars for sharing a few songs. It has been shown repeatedly that file sharing does not discourage artists from making their art (Elias, 2013, pp. 22-23).

Other technologies, such as digital rights management (DRM) have resulted in increased annoyance and problems for the average user while leaving the illegal users

and those with criminal intentions largely unaffected because the illicit users stop at nothing while the legitimate users will respect the laws and regulations in place. Bitcoin will be no exception if the regulations imposed prove to be too strict (Brito & Castillo, 2013, p. 39). Authorities must impose regulations because the alternative is to leave the Bitcoin system completely alone, since it is impossible to shut it down (almost impossible, as a peer-to-peer system it is subject to the same possibility of shutting down as other peer-to-peer services, which is about the same probability as of the internet shutting down). Furthermore, there is no entity responsible for Bitcoin, making it hard to impose regulations such as corporate restrictions. Those restrictions would have to be applied to the users themselves, a feat which would prove near impossible (Brito & Castillo, 2013, p. 39). The bond between the Bitcoin system and the foundation from which it was forged, the internet, is strong. Both are means of conveying information between agents. If Bitcoin is to be regulated, the regulators must expect an ongoing confluence of these forces (Elias, 2013, p. 28).

This results in the eventuality that if Bitcoin were to be made illegal it would not affect the Bitcoin network since the illegal users would keep it operating through the peer-to-peer system (Brito & Castillo, 2013, p. 39).

The regulation of third parties is another incentive for governments to regulate Bitcoin instead of trying to ban it. These third-party intermediaries such as money transmitters and exchangers can then be regulated further, making Bitcoin transactions less anonymous (A strictly correct term would be to say public instead of less anonymous, but as all transactions are public, the users themselves lose some of their anonymity). This would help authorities fight money laundering and other illicit activities while allowing the public to use bitcoins legally (since authorities cannot effectively forbid the public from using bitcoins as already stated) (Brito & Castillo, 2013, p. 39).

It is clear that if authorities were to ban Bitcoin, they would lose a lot of potential control over the intermediaries, as the intermediaries would essentially become illegal operations. Authorities could then not actively regulate certain aspects of the businesses, as they would normally do. If they regulate the then illegal operations the intermediaries were conducting, it would seem counter intuitive for the authorities and

undermine the strict policies against illegal activity they generally maintain. The conclusion is that any illicit intermediaries that would ultimately materialize would be completely unregulated (Brito & Castillo, 2013, p. 39).

A final point to consider is the competitive disadvantage of countries whose authorities fail to recognize Bitcoin as a legal alternative to current payment methods. If Bitcoin eventually becomes a stable payment option while retaining its qualities, of which most other transaction systems lack, it could be devastating for countries that prohibited the use of bitcoins (Brito & Castillo, 2013, p. 40).

9.1.1 A sensible approach to regulate Bitcoin

The best way to approach the regulation of bitcoins is by a sensible approach that highlights the possibilities of Bitcoin and thus allows it to grow further. To date, this seems to be the vision shared by policymakers. The Financial Crimes Enforcement Network (FinCEN) has recently issued a new guidance stating that certain activities related to virtual currencies and in particular Bitcoin, do not fall under the definition of money services businesses or money transmitter according to the Bank Secrecy Act (BSA) (FinCEN, 2013). Those activities are therefore not subject to the registration, reporting, and record-keeping requirements imposed by the BSA.

There are two rulings that were made public in early 2014 by FinCEN. The first ruling asserts that users who utilize software like Bitcoin to mine coins (or in general terms, any convertible virtual currency gathered for their own purposes) are not money transmitters under the BSA (FinCEN, 2014). The second ruling asserts that if a firm that is buying and selling virtual currencies as an investment that is exclusively for its own benefit is not a money transmitter either (FinCEN, 2014).

These rulings shed some light on a rather vague guidance that was issued in March of 2013 (Brito & Castillo, 2013, p. 40). With these rulings, a comprehensive system can be assumed, in which the position of FinCEN is reflected clearly in regards to Bitcoin and other cryptographic currencies. The earlier guidance states that if an exchanger/administrator of conveyable virtual currencies buys, sells, or otherwise accepts and transmits it in exchange for another virtual currency he is to be viewed as a money transmitter for regulatory purposes. This also applies if the exchanger or administrator uses conveyable virtual currencies for legal tenet for any reason or

intermediating between a seller and a user of services and/or goods the user is purchasing on the user's behalf (Mont, 2014).

The reasoning FinCEN has for establishing that a user that mines bitcoins is not considered a money transmitter is simple; when a user mines virtual currency, he is not accepting or transmitting any currency. This applies just as well to corporations and mining networks as individuals, since the nature of the situation does not change depending on who is mining.

A more controversial ruling from FinCEN is that even when users, individuals or corporations, who own bitcoins use them to purchase goods services for personal uses, or pay debts that were previously provoked in the traditional course of business, they are not utilizing money transmission services and are therefore not subject to FinCEN's regulations. The only way a user can possibly be engaged in money transmission, is by paying bitcoins to a third party at the direction of a creditor or a seller (FinCEN, 2014).

Another recent ruling from FinCEN issued in January 2014 states that if a company occasionally invests in virtual currency and the distribution and production of software to facilitate those investments does not constitute them as money transmitters under the BSA. This is supported by the notion that the distribution and production of software that facilitates virtual currency investments do not constitute transmission of value or acceptance, even though that is the purpose of the software itself. Similar to the earlier rulings, any transfers of virtual currency to intermediaries at the direction of the corporation's creditors, counter parties, or owners that are in any way entitled to direct payments should be analysed, as those transfers might constitute money transmission under the BSA (FinCEN, 2014). There is still a controversy whether or not corporations who were to provide investment or brokerage services to others that involved transmitting and accepting virtual currency are involved in money transmitting and it is clear that additional analysis is needed by institutions such as FinCEN to determine the regulatory status and obligations of such services (Carton, 2013).

FinCEN has helped virtual currencies such as Bitcoin to become approved in the regulatory world of finance while approaching the regulation and rulings regarding Bitcoin in a sensible manner. This has no doubt helped in promoting and establishing the Bitcoin system as a viable alternative payment method for users while deterring the

notion of criminalizing the use of them, thus guaranteeing that virtual currency systems can be regulated to some extent. It was revealed in a recent speech made by FinCEN's director, Jennifer Shasky Calvery, that a member of the virtual currency community will be included in the Treasury's Bank Secrecy Act Advisory Group (BSAAG) to enforce the interest of the community (Mont, 2014). The group aims to bring representatives from many different aspects of the market such as regulatory and law enforcement agencies, trade associations and financial institutions together to advise FinCEN on policy recommendations. The inclusion of Bitcoin in this advisory group demonstrates some acceptance of Bitcoin while at the same time highlighting just how far Bitcoin has yet to go in order to become a traditional method of moving funds internationally, whether that is for legitimate or illicit activities (Calvery, 2014). This can be seen by comparing the magnitude of processed transactions of bitcoins and other types of transactions. Bitcoin users managed to process transactions for roughly US$8 billion over a period of one year from October 2012 to October 2013. When compared to companies such as the Bank of America, which processed US$244.4 trillion in wire transfers or even Paypal, which transferred US$145 billion in online payments, Bitcoin dwarfs in comparison. It is to be expected that as Bitcoin becomes increasingly established among the general population, it will face greater resistance and increased regulation. Calvery herself pointed out that the niche market of Bitcoin is one of the reasons that regulators have not been stricter in their regulation (Mont, 2014). This has been further clarified by David Cohen, the Under Secretary for Treasury's Office of Terrorism and Financial Intelligence, who said that "despite a litany of potential risks, Bitcoin is not yet popular and stable enough to be a top concern" (Cohen, 2014).

FinCEN's statement of regulatory apathy toward Bitcoin is perhaps unsurprising. In 2009, FinCEN addressed some regulatory gaps that arose with the increased exposure of prepaid access cards, which are essentially just stored value, but did not finalize the ruling until 2011 (FinCEN, 2011). The gaps were addressed by introducing prepaid access cards into the Bank Secrecy ACT (BSA) and therefore increase the regulation surrounding these cards.

The justification for this change in the regulatory environment was to minimize the illicit uses of the cards. The prepaid cards can be obtained easily and are capable of

hosting a high velocity of money through accounts with relatively anonymous use. These qualities are similar to Bitcoin and faced the same criticism Bitcoin faces now; options that possess these qualities are particularly attractive to illicit users (Brito & Castillo, 2013, p. 23). FinCEN's new rule effectively brought prepaid access cards under the regulatory framework represented in the BSA and interestingly, came out in September 2011. This means that FinCEN let the prepaid access industry thrive for ten years without interfering until they suddenly pushed for the amendment of existing regulations in 2011 (Elias, 2013, p. 26). The concerns of law enforcement and other stakeholders about the anonymous use of access cards along with FinCEN's own evaluation of practicality are partly responsible for the interest FinCEN eventually showed prepaid access cards (FinCEN, 2011, pp. 5-8).

An attempt to regulate Bitcoin will be made in some way eventually. Two major considerations will be taken into account when that happens. Whether the regulation of Bitcoin can be justified and exerted under current laws or whether new laws have to be written specifically catered to Bitcoin and peer-to-peer currencies in general. Then it must be decided what agents related to the Bitcoin framework can be held accountable by those regulations.

These decisions will influence whether the regulation will be Kaldor-Hicks efficient or not (zhou, 2006, pp. 3-5). A regulation is said to be Kaldor-Hicks efficient when the gainers have sufficient gains to be able to hypothetically compensate the losers (by definition, since gainers and losers are mutually exclusive) and still have some leftover gains. Kaldor-Hicks efficiency is closely related to Pareto efficiency, since a Pareto optimal outcome can be reached by using the principles of Kaldor-Hicks efficiency of distribution. It is also not as strict as Pareto efficiency, as some participants are allowed to lose, given that the total gain is greater than the loss. It must be said that Kaldor-Hicks has been harshly criticized by opponents of the theory because of diminished marginal utility and the absolute level of income measurement used. Since distribution of wealth is not of importance in this criterion, it can lead to suboptimal utility in a social welfare sense of the word. A more technical criticism comes from Tibor Scitovsky, who demonstrated that when depending solely on the Kaldor criteria it is not anti-symmetric (Scitovsky, 1941, p. 88). When the criterion is not anti-symmetric, it can lead

to awkward situations where outcome A is an improvement over outcome B, which incidentally, can also be an improvement over outcome A. This is partly solved when using the combined Kaldor-Hicks criterion but that still offers situations where A is an improvement over B, which is an improvement over C, but C is still better than A (Scitovsky, 1941, p. 88). This result is paradoxical and is even called a Scitovsky paradox. It is paradoxical because the hypothetical example offers the possibility of the losers, after having been paid compensation by the gainers, compensating the gainers for going back to the original position (zhou, 2006, pp. 6-7).

10 Conclusion

Bitcoin is at the very least a technological achievement. It has provided an innovative solution the problem of double spending by utilizing peer-to-peer networks. It has revolutionised the idea of decentralized currencies by making them accessible to everyone that owns a computer that is connected to the internet. The idea to make the verification system decentralized, while utilizing the process itself as a minting mechanism is simply brilliant. However, this does not answer the question of whether Bitcoin is money or not.

The regression theorem states that an economic good cannot function as money until it first acquires exchange-value based on some other cause than its monetary function. This means that the regression theorem does not explicitly state that non-monetary demand is necessary to sustain money; it is only needed for that money to emerge originally. The theorem was then redefined and the original demand, therefore price, of Bitcoin articulated to originate from the link between bitcoins and fiat currencies. An exchange demand for Bitcoin was thus created from a non-exchange demand by employing established fiat monies.

By redefining the regression theorem it is evident that once a medium of exchange has become sufficiently liquid to garner a certain level of publicity, and therefore benefitting from network effects, it can sustain itself without being useful as anything else than a medium of exchange; the value it gains from its acquired liquidity is enough.

The Austrian school of thought offers the definition of money as a single commodity that is universally employed as a medium of exchange. As such, it can be said that Bitcoin is only a secondary medium of exchange, as it does not possess the liquidity necessary to be a universal medium of exchange. It is clear then that Bitcoin has yet to become money, both in the traditional sense and from an Austrian economic perspective. At best, Bitcoin is a secondary medium of exchange with great potential to become a universal currency, as long as it manages to overcome the inherent network effects currently at play.

It has been established that Bitcoin is an imperfect form of memory, although it resembles perfect memory more closely than other mediums of exchange, because of the peer-to-peer record keeping. When memory is imperfect, and the money expensive

to store or verify, there must exist some middle ground where both memory and money are used simultaneously where money in this context is defined as fiat money (in contrast to Bitcoin as memory). If the balance is disrupted because money gets overly costly compared to memory, the memory will be used more frequently. Bitcoin's role in present markets is to provide an alternative payment method for those who value the qualities it can offer.

Bitcoin exists somewhere between commodity money and fiat money. Whereas commodity money is naturally scarce and does have monetary uses, fiat money does not have any monetary uses and is contingently scarce at best. Bitcoin is artificially scarce (which is no different from being naturally scarce since the scarcity cannot be influenced or tampered with, it is a steadier state of scarcity if anything because it is immune to supply shocks) but still holds no non-monetary value. This leads to a category developed by Selgin, synthetic commodity money. Before this technological innovation, the existence and utilization of synthetic commodity money was an unlikely scenario. With Bitcoin, however this has changed, and Bitcoin has shown that synthetic commodity money is most definitely possible. The result is this: Bitcoin is a secondary medium of exchange, classified as synthetic commodity money with a future possibility of emerging as a universal medium of exchange, decentralized money in a way, given that regulatory authorities allow it.

Fractional reserve banking is theoretically possible within Bitcoin. However, to do so would require money substitutes for Bitcoin, in the same way as money substitutes are required to expand a money supply based on commodities such as gold, or simply fiat money in recent times. It is highly unlikely that Bitcoin substitutes will emerge, since there is little room for improvement over Bitcoin in terms of transaction costs, convenience or storage costs. Decentralized digital media of exchange can theoretically be used in fractional reserve banking, but it is unadvisable, as there is no incentive to do so.

Network effects have also proven to be one of the main reasons why Bitcoin is not yet money. An excess inertia, because of a focal point generated by historical acceptance of traditional currencies, raises the switching cost to Bitcoin to be higher

than the perceived benefits of switching. This is partly subjective and a case was made in this thesis that the switching costs are perhaps not as high as they seem.

There are some problems inherent to the Bitcoin system. One of the defining features of Bitcoin is the eventually inelastic money supply. This is in a way something inherently good from the Austrian perspective, since it is unlikely to make way for fractional reserve banking and with it, the possibility of exceedingly rapid expansion of the money supply. However, inelastic money supply makes Bitcoin vulnerable to money demand shocks, making the medium very volatile. Other criticism aimed at Bitcoin such as that it breaches Gresham's law or that it is doomed to failure by the deflationary design, are shown to be not as valid. Other risks present within Bitcoin mainly stem from a lack of regulation, or rather from the apathy and disinterest of policymakers. Any use of third-party intermediaries to accomplish goals such as increased anonymity or safekeeping is at risk of being fraudulent. It must be noted that as Bitcoin grows in popularity, so will the regulatory framework around it.

Finally it must be noted that governments have a monopoly of money in a narrow sense, they are the issuers of it and control to some extent the laws and regulations surrounding it. This means that it is exceedingly hard for Bitcoin to become money in practice if governmental authorities do not actively embrace it as such.

Therefore, it is important that regulators do not act in an excessively strict manner when providing legal limitations of Bitcoin through regulation. This seems to be the vision shared by policymakers, as FinCEN has recently issued guidance that mining, trading, or using bitcoins is not defined as money services business or money transmitting services, thereby clarifying earlier rulings about the subject. However, FinCEN is not known for making hasty decisions and issuing new rulings in a hurry. Bitcoin will eventually be regulated further if it manages to overcome the excess inertia apparent when the network effects are studied.

To summarize the conclusion, Bitcoin is not money according to either Austrian economics or mainstream economics. It is still a medium of exchange, although the Austrian perspective only allows it to be a secondary medium of exchange, since it is not sufficiently liquid to be a universal medium of exchange. Bitcoin can be said to represent an imperfect form of memory that coexists with traditional fiat money in a

balanced state that is slowly shifting toward the use of memory (Bitcoin) because of the qualities it offers over fiat monies, this development is still largely dependent on network effects. As Bitcoin is not money, it is redundant to place it as either commodity money or fiat money. Synthetic commodity money is not money in the traditional sense and describes Bitcoin perfectly.

11 Discussion

Bitcoin is an unexpected innovation, leading to a plethora of complications and intriguing possibilities that were hard to imagine before it came into existence. This can be seen by observing the effects Auroracoin had on Icelandic society. Auroracoin is a crypto-currency created by an anonymous identity. The concept of Auroracoin was simple: a fixed amount of Auroracoins, distributed evenly among the citizens of Iceland. The result was astonishing, digital numbers with no value attached to them acquired value, and fast. In a bubble-like fashion, the value of Auroracoin surged before dropping to a small fraction of what it was worth moments earlier. The difference between Auroracoin and Bitcoin for example, is that Auroracoins were 50% pre-mined, meaning that half of the total money supply was already in possession of someone. This interesting concept clearly did not work as intended in the end, but perhaps that was never the plan, as almost anything is legal when the subject is not defined by law. It is unknown what will become of Auroracoin in the future, as its value has been relatively stable for the past few months.

The next few years will decide whether Bitcoin can become a universal medium of exchange or if it will deteriorate into solely a speculative investment with no real exchange-value, rendering the original premise of how Bitcoin acquired its value irrelevant. If the latter happens, Bitcoin will surely disappear from the discussion, although it will probably never fully die, as long as someone keeps the peer-to-peer network running. However, it is clear that the rise of crypto-currencies has not reached its limit, as more and more crypto-currencies are being created, each with different innovative inspirations behind them. An example of some of the concepts are increased anonymity, increased resource efficiency, a community oriented fundraising medium, and an inflationary crypto-currency.

The biggest speculation that this thesis leaves behind is one of the initial demand of Bitcoin. As has been stated it could have come about because of computer geeks and libertarians wanted bitcoins for a novelty factor, similarly to how jewels, or rather some aesthetic appeal, generated the initial demand for gold. Although Bitcoin as synthetic commodity money is different from gold as commodity money in the regards that it is impossible to wear bitcoins like golden jewellery, it is still possible to show them off in

social situations (for example by talking about them) and, of course, online. This is similar to what happens in some computer games presently, as some games utilize a micro-transaction system where players can spend real money on online items. Items that are inherently worthless, but still seem to acquire value through their novelty, as players can brag about their items in the game, for example.

The notion of synthetic commodity money is almost as interesting as Bitcoin, and perhaps necessarily so. After all, it is able to account for the design of Bitcoin, a feat in and of itself. Further analysis of synthetic commodity money is needed, as little has been written about this fourth group of monies (the others being commodity money, fiat money, and Coase Durables respectively). Synthetic commodity money will surely become more prevalent as crypto-currencies increase in popularity and it will be interesting to discover what will come of the discourse.

Bibliography

Abrams, R., & Popper, N. (2014, February 25). *Trading Site Failure Stirs ire and Hope for Bitcoin*. Retrieved from The New York Times: http://dealbook.nytimes.com/2014/02/25/trading-site-failure-stirs-ire-and-hope-for-bitcoin/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1

Aiyagari, S. R., & Wallace, N. (1997). Government Transaction Policy, the Medium of Exchange, and Welfare. *Journal of Economic Theory, 74*, 1-18.

Andresen, G. (2012, May 1). *Neutralizing a 51% attack*. Retrieved from GavinTech: http://gavintech.blogspot.com/2012/05/neutralizing-51-attack.html

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating User Privacy in Bitcoin. In Sadeghi, & Ahmad-Reza (Ed.), *Financial Cryptography and Data Security* (pp. 34-51). Okinawa: Springer.

Araujo, L., & Camargo, B. (2010, June 25). *Limited memory and the essentiality of money.* Retrieved from EconPapers: http://econpapers.repec.org/paper/fgveesptd/221.htm

Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2012, June). On Bitcoin and Red Balloons. *ACM Conference on Electronic Commerce* (pp. 56-73). Valencia, Spain: ACM.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to Better: How to Make Bitcoin a Better Currency. *Financial Cryptography, 7397*, 399-414.

Bitcoin Charts. (2014, May 2). *BitStamp (USD)*. Retrieved from Bitcoin Charts: http://bitcoincharts.com/charts/bitstampUSD#tgSzm1g10zm2g25zv

Bitcoin Clock. (2014, May 11). *Bitcoin Clock*. Retrieved from Bitcoin Clock: http://bitcoinclock.com/

Bitcoin Wiki. (2013, July 10). *Fractional Reserve Banking and Bitcoin*. Retrieved from Bitcoin Wiki: https://en.bitcoin.it/wiki/Fractional_Reserve_Banking_and_Bitcoin

Bitcoin Wiki. (2013, December 31). *History*. Retrieved from Bitcoin: https://en.bitcoin.it/wiki/History

Bitcoin Wiki. (2013, December 25). *Network*. Retrieved from Bitcoin: https://en.bitcoin.it/wiki/Network

Bitcoin Wiki. (2013, December 28). *Weaknesses*. Retrieved from Bitcoin: https://en.bitcoin.it/wiki/Weaknesses

Bitcoin Wiki. (2014, March 20). *Scalability*. Retrieved from Bitcoin: https://en.bitcoin.it/wiki/Scalability

Bitcoin Wiki. (2014, March 28). *Transaction fees*. Retrieved from Bitcoin: https://en.bitcoin.it/wiki/Transaction_fees

BitPay. (2014, May 1). *BitPay*. Retrieved from BitPay: https://bitpay.com/

Blockchain. (2014, May 25). *Total Bitcoins In Circulation*. Retrieved from Blockchain: https://blockchain.info/charts/total-bitcoins?showDataPoints=false&timespan=all&show_header=true&daysAverageString=1&scale=0&format=csv&address=

Bradbury, D. (2013, June 14). *Colored coins paint sophisticated future for Bitcoin*. Retrieved from CoinDesk: http://www.coindesk.com/colored-coins-paint-sophisticated-future-for-bitcoin/

Brito, J. (2013, May 20). *The Top 3 Things I Learned at the Bitcoin Conference.* Retrieved from Reason: http://reason.com/archives/2013/05/20/the-top-3-things-i-learned-at-the-bitcoi

Brito, J., & Castillo, A. (2013). *Bitcoin - A primer for Policymakers.* George Mason University. Arlington: Mercatus Center.

Calvery, J. S. (2014, March 18). Prepared Remarks of Jennifer Shasky Calvery. *Association of Certified Anti-Money Laundering Specialists (ACAMS) 19th Annual International AML and Financial Crime Conference.* Hollywood: FinCEN.

Camenisch, J., & Lysyanskaya, A. (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. *Eurocrypt*, 93-118.

Carton, B. (2013, August 1). *Bitcoin? CFDs? SEC Shows Exotic Currencies and Securities Are Not Beyond Its Reach*. Retrieved from Compliance Week: http://www.complianceweek.com/bitcoin-cfds-sec-shows-exotic-currencies-and-securities-are-not-beyond-its-reach/article/305699/

Centi, J.-P., & Bougi, G. (2004). *Possible economic consequences of electronic money.* (J. Birner, & P. Garrouste, Eds.) London: Routledge.

Chaum, D. (1983). Blind Signatures for Untraceable Payments. *Advances in Cryptology*, 199-203.

Coase, R. H. (1972). Durability and Monopoly. *Journal of Law and Economics, 15*(1), 143-149.

Cohen, D. S. (2014, March 18). *Remarks From Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency"*. Retrieved from U.S. Department of Treasury: http://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx

de Soto, J. H. (2012). *Money, Bank Credit, and Economic Cycles.* Auburn: Ludwig von Mises Institute.

Elias, M. (2013, October 3). *Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy*. Retrieved from Social Science Research network: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1937769

Farrell, J., & Saloner, G. (1986, December). Installed Base and Compatibility: Innovation, Product Preannouncements, and Predation. *The American Economic Review, 76*(5), 940-955.

Federal Bureau of Investigation. (2012). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity.* Washington, D.C: Federal Bureau of Investigation.

FinCEN. (2011, July 29). *Bank Secrecy Act Regulations - Definitions and Other Regulations Relating to Prepaid Access*. Retrieved from Financial Crimes Enforcement Network: http://www.gpo.gov/fdsys/pkg/FR-2011-07-29/pdf/2011-19116.pdf

FinCEN. (2011, July 26). *FinCEN Issues Prepaid Access Final Rule Balancing the Needs of Law Enforcement and Industry*. Retrieved from Financial Crimes Enforcement Network: http://www.fincen.gov/news_room/nr/html/20110726b.html

FinCEN. (2013, March 18). *FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities.* Retrieved from Financial Crimes Enforcement Network: http://www.fincen.gov/news_room/nr/pdf/20130318.pdf

FinCEN. (2014, january 30). *Application of FinCEN's Regulations to Virtual Currency Mining Operations.* Retrieved from Financial Crimes Enforcement network: http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf

FinCEN. (2014, January 30). *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity.* Retrieved from Financial Crimes Enforcement Network: http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf

FINRA. (2014, November 3). *Bitcoin: More than a Bit Risky*. Retrieved from Financial Industry Regulatory Authority: Texas Becomes First State to Halt a Bitcoin Investment Deal

Friedman, M. (1960). *A program for monetary stability.* New York: Fordham University Press.

Friedman, M. (1962). *In search of a monetary constitution.* (L. B. Yeager, Ed.) Cambridge: Harvard University Press.

Fullenkamp, C., & Nsouli, S. M. (2004). *Six Puzzles in Electronic Money and Banking.* Washington, D.C.: International Monetary Fund.

Gibbons, R. (1992). *A Primer in Game Theory.* Essex: Pearson Education Limited.

Gibson, B. (2013, March 22). *Bitcoin & the Byzantine Generals Problem*. Retrieved from Expected Payoff: http://expectedpayoff.com/blog/2013/03/22/bitcoin-and-the-byzantine-generals-problem/

Grigg, I., & Güring, P. (2012, February 23). *Bitcoin & Gresham's Law - the economic inevitability of Collapse.* Retrieved from Financial Cryptography: http://iang.org/papers/BitcoinBreachesGreshamsLaw.pdf

Hayek, F. (1990). *Denationalisation of Money: The Argument Refined.* London: The institute of Economic Affairs.

Hoppe, H.-H. (1996). Banking, Nation States, and International Politics: A Sociological Reconstruction of the Present Order. *Review of Austrian Economics, 4*(1), 55-87.

Hurst, B. (2014, March 19). *Here's How Many People Actually Own Bitcoin*. Retrieved from Business insider: http://www.businessinsider.com/heres-how-many-people-actually-own-bitcoin-2014-3?IR=T&

Investopedia. (2014). *Back stop*. Retrieved from Investopedia: http://www.investopedia.com/terms/b/backstop.asp

Investopedia. (2014). *Credit Money*. Retrieved from Investopedia: http://www.investopedia.com/terms/c/credit-money.asp

Investor Glossary. (2014, May). *Greater Fool Theory*. Retrieved from Investor Glossary: http://www.investorglossary.com/greater-fool-theory.htm

Jevons, W. S. (1875). *Money and the Mechanism of Exchange.* New York: D. Appleton and Co.

Johnson, A. R. (2013, April 18). *Money Transfers in Bitcoins? Western Union, MoneyGram Weigh the Option.* Retrieved from The Wall Street Journal: http://online.wsj.com/news/articles/SB10001424127887324493704578431000719258048

Keynes, J. M. (1936). *The General Theory of Employment, Interest, and Money.* London: Institute of Economic Affairs.

King, S., & Nadal, S. (2012, August 19). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.* Retrieved from Peercoin: http://peercoin.net/assets/paper/peercoin-paper.pdf

Kocherlakota, N. (1996). *Money is memory.* Minneapolis: Federal Reserve Bank of Minneapolis.

Kocherlakota, N., & Wallace, N. (1998). Incomplete Record-Keeping and Optimal Payment Arrangements. *Journal of Economic Theory 81*, 272-289.

Krüger, M., & Godschalk, H. (1998). Herausforderung des bestehenden Geldsystems im Zuge seiner Digitalisierung - Chancen für Innovationen? *Fragen der Freiheit*(248), 40-50.

Krugman, P. (1984). The International Role of the Dollar: Theory and Prospect. In J. F. Bilson, R. C. Marston, J. F. Bilson, & R. C. Marston (Eds.), *Exchange Rate Theory and Practice* (pp. 261-278). Chicago: University of Chicago Press.

Krugman, P. (1995). *Peddling Prosperity: Economic Sense and Nonsense in an Age of Diminished Expectations.* New York: W. W. Norton & Company.

Krugman, P. (1998, August 13). *Baby-Sitting the Economy.* Retrieved from The Unofficial Paul Krugman Web Page: http://www.pkarchive.org/theory/baby.html

Krugman, P. (2013, December 28). *Bitcoin Is Evil*. Retrieved from The New York Times: http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?smid=pl-share

Laurie, B. (2011, july 05). *Decentralized Currencies Are Probably Impossible.* Retrieved from Ben Laurie Blathering: http://www.links.org/files/decentralised-currencies.pdf

Lee, T. B. (2011, June 15). *A risky currency? Alleged $500,000 Bitcoin heist raises questions*. Retrieved from Arstechnica: http://arstechnica.com/tech-policy/2011/06/bitcoin-the-decentralized-virtual-currencyrisky-currency-500000-bitcoin-heist-raises-questions/

Lee, T. B. (2013, April 11). *An Illustrated History Of Bitcoin Crashes*. Retrieved from Forbes: http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/

Levine, M. (2014, January 2). *Bitcoin Is an Expensive Way to Pay for Stuff*. Retrieved from Bloomberg View: http://www.bloombergview.com/articles/2014-01-02/bitcoin-is-an-expensive-way-to-pay-for-stuff

Luther, W. (2013, September 17). *Cryptocurrencies, Network Effects, and Switching Costs.* Retrieved from Mercatus Center, George Mason University: http://mercatus.org/publication/cryptocurrencies-network-effects-and-switching-costs

Luther, W., & Olson, J. (2013, June 7). *Bitcoin is Memory.* Retrieved from Socian Science Research Network: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2275730

Maltby, E. (2011, February 10). *Chargebacks Create Business Headaches*. Retrieved from The Wall Street Journal: http://online.wsj.com/news/articles/SB10001424052748704698004576104554234202010

Mankiw, N. G. (2009). *Macroeconomics 7th ed.* New York: Worth Publishers.

Matonis, J. (2011, June 26). *Why Are Libertarians Against Bitcoin?* Retrieved from The Monetary Future: http://themonetaryfuture.blogspot.ie/2011/06/why-are-libertarians-against-bitcoin.html

Menger, C. (1892). *On the Origins of Money* (2009 ed.). (C. Foley, Trans.) Auburn, Alabama, United States of America: Ludwig von Mises Institute.

Menger, C. (1897). *Principles of Economics* (1976 ed.). Auburn: Ludwig Von Mises Institute.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). *Zerocoin: Anonymous Distributed E-Cash from Bitcoin.* Oakland: Security and Privacy Applied Research Lab.

Mises, L. v. (1953). *The Theory of Money and Credit* (1912 ed.). (H. E. Batson, Trans.) New Haven: Yale University Press.

Mises, L. v. (1998). *Human Action.* Auburn: Ludwig von Mises Institute.

Mont, J. (2014, February 4). *New FinCEN Guidance Clarifies Corporate Bitcoin Requirements*. Retrieved from Compliance Week: http://www.complianceweek.com/new-fincen-guidance-clarifies-corporate-bitcoin-requirements/article/332667/

Mont, J. (2014, March 12). *Texas Becomes First State to Halt a Bitcoin Investment Deal*. Retrieved from Compliance Week: http://www.complianceweek.com/texas-becomes-first-state-to-halt-a-bitcoin-investment-deal/article/337881/

Mont, J. (2014, March 18). *Treasury Officials Welcome Bitcoin Onto BSA Advisory Group*. Retrieved from Compliance Week: http://www.complianceweek.com/treasury-officials-welcome-bitcoin-onto-bsa-advisory-group/article/338766/

Murphy, R. P. (2003, September 29). The Origin of Money and Its Value. *Mises Daily*.

Murphy, R. P. (2013, June 3). *The Economics of Bitcoin*. Retrieved from Library of Economics and Liberty: http://www.econlib.org/library/Columns/y2013/Murphybitcoin.html

Nakamoto, S. (2008, November 1). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from Bitcoin - Open source P2P money: https://bitcoin.org/bitcoin.pdf

New Liberty Standard. (2010, January 15). *2009 Exchange Rate*. Retrieved from New Liberty Standard: http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate

Olanoff, D. (2013, January 7). *BitPay Banks $510K In Investment To Become PayPal for Bitcoin, Already Has 2,100 Businesses On Board*. Retrieved from TechCrunch: http://techcrunch.com/2013/01/07/bitpay-banks-500k-in-angel-investment-to-become-paypal-for-bitcoin-already-has-2100-businesses-on-board/

Paul, A. (2013, May 24). *Is Bitcoin the Next Generation of Online Payments?* Retrieved from Yahoo Small Business Owners: https://smallbusiness.yahoo.com/advisor/bitcoin-next-generation-online-payments-213922448--finance.html

Reid, F., & Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System. *The Computing Research Repository*, abs/1107.4524.

Reutzel, B. (2013, November 8). *Some Risky Merchants Turn to Bitcoin Processor; Others Go It Alone*. Retrieved from PaymentsSource: http://www.paymentssource.com/news/some-risky-merchants-turn-to-bitcoin-processor-others-go-it-alone-3015974-1.html

Reutzel, B. (2013, May 21). *Why Some Merchants Accept Bitcoin Despite the Risks*. Retrieved from PaymentsSource - Payments Industry News and Analysis: http://www.paymentssource.com/news/why-some-merchants-accept-bitcoin-despite-the-risks-3014183-1.html

Ritter, J. A. (1995). The Transition From Barter to Fiat Money. *American Economic Review, 85*, 134-149.

Rolnick, A. J., & Weber, W. E. (1986, February). Gresham's Law or Gresham's Fallacy? *Journal of Political Economy, 94*(1), 185-199.

Rothbard, M. N. (2004). *Man, Economy, and State.* Auburn: Ludwig von Mises Institute.

Salerno, J. T. (2010). *Money, Sound and Unsound.* Auburn: Ludwig von Mises Institute.

Salmon, F. (2013, November 27). *The Bitcoin Bubble and the Future of Currency*. Retrieved from Medium: https://medium.com/money-banking/2b5ef79482cb

Sanches, D., & Williamson, S. (2010). Money and credit with limited commitment and theft. *Journal of Economic Theory*, 1525-1549.

Say, J.-B. (1803). *A Treatise on Political Economy.* Philadelphia: Lippincott, Grambo & Co.

Schlichter, D. S. (2011). *Paper Money Collapse: The Folly of Elastic Money and the Coming Monetary Breakdown.* New Jersey: John Wiley & Sons.

Scitovsky, T. (1941). A Note on Welfare Propositions in Economics. *Review of Economic Studies, 9*(1), 77-88.

Selgin, G. (1994, November). On Ensuring the Acceptability of a New Fiat Money. *Journal of Money, Credit and Banking, 26*(4), 808-826.

Selgin, G. (2013, April 22). *Bitcoin*. Retrieved from Free Banking: http://www.freebanking.org/2013/04/22/bitcoin/

Selgin, G. (2013, April 10). *Synthetic Commodity Money.* Retrieved from Social Science Research network: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118

Silver-Greenberg, J. (2012, june 1). *New Rules for Money Transfers, but Few Limits*. Retrieved from The New York Times: http://www.nytimes.com/2012/06/02/business/new-rules-for-money-transfers-but-few-limits.html?_r=1&

Simonite, T. (2013, May 22). *Bitcoin Hits the Big Time, to the Regret of Some Early Boosters*. Retrieved from MIT Technology Review: http://www.technologyreview.com/news/515061/bitcoin-hits-the-big-time-to-the-regret-of-some-early-boosters/

Southurst, J. (2014, January 14). *Get Paid in Bitcoin With BitPay's New Payroll API*. Retrieved from CoinDesk: http://www.coindesk.com/get-paid-bitcoin-bitpays-payroll-api/

Suede, M. (2012, March 9). *Fractional Reserve Banking With Bitcoins*. Retrieved from Libertarian News: http://www.libertariannews.org/2012/03/09/fractional-reserve-banking-with-bitcoins/

Surda, P. (2012, November 21). *Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?* Retrieved from http://www.economicsofbitcoin.com/p/publications-and-interviews.html

Sweeney, J., & Sweeney, R. J. (1977). Monetary Theory and the Great Capitol Hill Baby Sitting CO-op Crisis: Comment. *Journal of Money, Credit and Banking, Vol. 9, No. 1, Part 1.*, 86-89.

The Voluntaryist Reader. (2012, December 7). *The Voluntaryist Reader.* Retrieved from Bitcoin and the Regression Theorem of Money: http://voluntaryistreader.wordpress.com/2012/12/07/bitcoin-and-the-regression-theorem-of-money/

The World Bank. (2014, March 1). *An analysis of trends in the average total cost of migrant remittance services*. Retrieved from Remittance Prices Worldwide: https://remittanceprices.worldbank.org/sites/default/files/RPW_Report_Mar2014.pdf

Thornton, M. (1991). *The Economics of Prohibition.* Salt Lake City: University of Utah Press.

Vigna, P. (2014, February 25). *5 Things about Mt. Gox's Crisis*. Retrieved from The Wall Street Journal: http://blogs.wsj.com/five-things/2014/02/25/5-things-about-mt-goxs-crisis/

Warren, J. (2012, November 27). *Bitmessage: A Peer-to-Peer Message Authentication and Delivery System.* Retrieved from Bitmessage: https://bitmessage.org/bitmessage.pdf

White, L. H. (1984, September). Competitive Payments Systems and the Unit of Account. *THe American Economic Review, 74*(4), 699-712.

White, L. H. (1999). *The Theory of Monetary Institution.* London: Blackwell Publishers.

Willett, J. (2014, May 8). *The Second Bitcoin Whitepaper.* Retrieved from GitHub - mastercoin: https://e33ec872-a-62cb3a1a-s-sites.googlegroups.com/site/2ndbtcwpaper/2ndBitcoinWhitepaper.pdf?attachauth=ANoY7crXVPwjrH9P_omY4UTr2y4lsNPsJlwbFMjewksqX5QNh8NL6x2YcVUZp

xBIQbDPvnrlJeMRjwjY5kxVwZRfcXqIaZbtPVWg9Ek7ngkUeR1MeMjGtr2Xk69XwoAqQJAZ50F9-EBjTHSPcMx5

zhou, q. (2006, January). *the evolution of efficiency principle from utilitarianism to wealth maximization.* Retrieved from Selected Works of qi zhou: http://bit.ly/ujS93r