WU Vienna University of Economics and Business

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EFMD EQUIS ACCREDITED

Diploma Thesis

Thesis title:
Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?

Author:
Peter Šurda

Student ID no.:
9650205

Academic program:
Betriebswirtschaft J151

Advisor:
Univ. Doz. Mag. Dr. Peter R. Haiss

With this statement, I declare that this academic thesis:

was written entirely by me, without the use of any sources other than those indicated and without the use of any unauthorized resources;

has never been submitted in any form for evaluation as an examination paper in Austria or any other country;

is identical to the version submitted to my advisor for evaluation.

Date _____ Signature _____

Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?

by
Peter Šurda

Advisor:

Univ. Doz. Mag. Dr. Peter R. Haiss

http://ssrn.com/author=115752

Abstract

This paper presents an economic analysis of Bitcoin from a libertarian point of view. The theoretical part analyses the applicability of the Austrian School of Economics at Bitcoin. Of particular interest are the evolution of money, competition among media of exchange, and the concept of money supply. The empirical part analyses the following variables: price, price volatility, liquidity, visibility and velocity. I come to the conclusion that theoretically, Bitcoin can be closer to the Austrian ideal of money than either fiat money or gold, and it is possible that it will evolve into that position. The results of the empirical analysis are consistent with Bitcoin being a medium of exchange.

Keywords: Bitcoin, digital cash, currency competition, Austrian business cycle theory, Mises' regression theorem

JEL Codes: E390, E410, E420, E510, G210

Highlights:

- Bitcoin emerged as a market (catallactic) process and is evolving
- Bitcoin can evolve into money
- Bitcoin can prevent business cycles through inelastic supply of money
- Empirical analysis shows that Bitcoin may be an immature medium of exchange

Acknowledgements

I would like to thank my thesis advisor, Univ. Doz. Mag. Dr. Peter R. Haiss (http://ssrn.com/author=115752). He provided great guidance, kept me on track with proper scientific research and provided information sources outside of my own scope of specialisation.

I would like to thank the opponents of some of my views on Bitcoin that I debated, particularly: Niels Van der Linden, Smiling Dave, David Kramer, Atheros, DeathAndTaxes, Jorge Timón.

I would like to thank people for the Bitcoin community that I was in contact with or who provided interesting insights: Amir Taaki, Vladimir Marchenko, Meni Rosenfeld, molecular, MoonShadow, Marek Palatinus, deepceleron, Stephen Gornick, Pierre Noizat, Juraj Bednár, Iain David Stewart, Michael Parsons, Mike Hearn, Jeff Garzik.

I would like to thank the economists I talked to: George Selgin, Walter Block, Stephan Kinsella, Philipp Bagus, David Gordon, Peter G. Klein, Robert P. Murphy, Detlev Schlichter, Hans Hermann Hoppe, John Barrdear, Jon Matonis, Koen Swinkles.

A special thanks goes to Satoshi Nakamoto for designing Bitcoin.

John Tobey for Abe "Open Source blockchain explorer knockoff" which I used for analysing the blockchain data.

Mt.Gox for the trade data and historical exchange rates.

Felix Tendler for historical Mt.Gox order book data.

Last but not least, I would like to thank my mother, Doc. RNDr. Viera Šurdová, CSc., and my wife, Seah Lay Chee.

Contents

Chapter 1

Introduction

While there have been attempts to analyse the economic properties of Bitcoin, particularly from within the online Bitcoin community, such as Güring and Grigg (2011), Pattison (2011), Hamacher and Katzenbeisser (2011), Becker et al. (2012) or Babaioff et al. (2012), these follow very narrow paths and miss the broader context. My own goal was to analyse Bitcoin from a libertarian view and to answer the research question, whether Bitcoin is an alternative to fiat currencies and gold.

From the point of view of market actors, Bitcoin can be interpreted as a de-centralised clearing mechanism, based on a virtual unit (called "bitcoin" with a lower case "b"). The clearing is controlled by asymmetric cryptography, the public key identifying an account, while a corresponding private key allows sending balances from that account. In addition to clearing, Bitcoin also contains an inelastic production function. Clearing mechanism together with a defined supply allows Bitcoin to be used as a medium of exchange.

Several names have been proposed for such media of exchange, for example "virtual currency" (European Central Bank (2012)), "digital cash" (Tanaka (1996)), "cryptocurrency" (Elias (2011)). For the purposes of this thesis, the exact name is not important, rather the economic features are. I will use "fiat money" to refer to a monetary system similar to the one that exists now. I will used the term "gold" and "gold standard" to refer to a system based on a physical commodity chosen by a market to be a medium of exchange (it thus refers not only to gold directly but also silver or other physical commodities), for example historical gold standards, or hypothetical systems based on reforms such as the one described by Rothbard (2005) or Selgin (1988).

In Chapter 2, I present Bitcoin as it is, describing its workings and the historical and existing products and services associated with Bitcoin. I explain how Bitcoin can and is used. The information presented is of qualitative nature, and allows to build a mental picture of the "visible" part of the Bitcoin ecosystem. I attempt to provide answers to the questions "what was" and "what is". I attempt to put it in a broader context, so that the potential of Bitcoin is clarified. In Chapter 3 I follow up with interpreting Bitcoin through economic theory (mainly according to the Austrian School of Economics), attempt to classify it and formulate criteria which influence its evolution. Of particular interest are the evolution of money, competition among media of exchange, and the concept of money supply. This part is not strictly Bitcoin specific, it also applies to some hypothetical future types of money. I attempt to provide the answer to the questions "why" and "how", from a libertarian, rather anti-fiat-money, anti-fractional-

reserve-banking point of view and argue that the theoretical foundation of Bitcoin is closer to the Austrian's School ideal of money than either the fiat money or gold. Lastly, in Chapter 4, I analyse several aspects of Bitcoin quantitatively. The variables analysed are price, price volatility, liquidity, visibility (meaning how intensive the public perception of Bitcoin is) and velocity of circulation. The empirical analysis is an attempt to provide support for it. The thesis finishes up with a conclusion in Chapter 5 where I summarise my findings.

1.1 Methodological comments

Before approaching the topic in more depth, I would like to provide some background for the methodology used and my motivation.

Large parts of this thesis are based on the teachings of the Austrian economic school. There are several reasons for this. As for the subjective ones, it is the school I am familiar with the most, and that I find myself in most agreement with. But there is an objective reason as well. It is the same as presented by North (2011):

> "This theory of endogenous money is unique to Mises and his followers. No other school of economic opinion accepts it. Every other school appeals to the State, as an exogenous coercive power, to regulate the money supply and create enough new fiat or credit money to keep the free market operational at nearly full employment with nearly stable prices. *Every other theory of money invokes the use of the State's monopolistic power to supply the optimum quantity of money.*" [emphasis added]

Similarly, Salerno (2010) writes:

> "Needless to say, the three modern macroeconomic schools under examination all staunchly support the idea that supply of money needs to be centralized under a political monopoly."

In other words, with respect to the introduction of a money through market forces and people being able to voluntarily choose which money to use, economic schools other than the Austrian do not have much to say. Nevertheless, occasionally they break this trend and analyse some aspect of money under the assumption that these two conditions are present. But even then, they still tend to continue with the ideological trend of seeing this as something a priori problematic and something that needs to be addressed via a policy action. Examples would be Krugman (1980), Levy-Yeyati (2004) or Catao and Terrones (2000).

Furthermore, two of the economists who publicised the so far broadest research of Bitcoin, Jon Matonis and Michael Suede, subscribe to the Austrian School. Even though their Bitcoin-specific work has not been published by peer-reviewed journals, it is referenced by the European Central Bank (2012), noting that

> "The theoretical roots of Bitcoin can be found in the Austrian school of economics and its criticism of the current fiat money system and interventions undertaken by governments and other agencies, which, in their view, result in exacerbated business cycles and massive inflation."

Nevertheless, I do not make here the argument that the Austrians are correct (and conversely, other schools are wrong). I am merely analysing Bitcoin from a (mainly) Austrian point of view. Furthermore, as Mises (1999) argues:

> "There is no means to establish an a posteriori theory of human conduct and social events. History can neither prove nor disprove any general statement in the manner in which the natural sciences accept or reject a hypothesis on the ground of laboratory experiments. Neither experimental verification nor experimental falsification of a general proposition is possible in its field."

Therefore, scholars of the Austrian School should view my quantitative empirical research as an amendment, rather than an argument.

Chapter 2

Current status of Bitcoin

2.1 Components of Bitcoin (in the narrower sense)

In the narrower sense (as a clearing mechanism), Bitcoin consists of two virtual components. The first one is a ledger, called the "blockchain". This ledger is distributed, and every computer connected to the Bitcoin network directly (called a "node") has a full copy.[1] Clearing transactions are pooled into bigger chunks called "blocks". The blocks are ordered sequentially and this sequence is the ledger. Hence the term blockchain, a sequential order (or a chain) of blocks. The proper sequence as well as consistency is upheld by cryptography.

The other virtual components are "keypairs". A keypair consists of two large numbers ("keys") that are mathematically related. This relationship allows the a person who knows one of these numbers to perform an action that the knower of the other number can verify, but cannot recreate themselves (as that would require calculating the other key, which is prohibitively complex). An analogy would be a special lock which allows two keys to be inserted, key A only being able to lock it, and key B only being able to unlock it. If the holder of the key A locks the lock, the holder of the key B can unlock the lock, thus verifying that the holder of the key A locked it beforehand. But the holder of the key B cannot lock the lock themselves, nor does holding of the key B make it easier to recreate key A.

If one of the keys in a pair is kept secret while the other one divulged, this allows the holder of the secret key to prove to the general public that he has it. In such a case, the secret key is called "private key" and the divulged key is called "public key". This is often used to verify the authenticity of the other party. For Bitcoin, the public key identifies a Bitcoin "address" (similar to account number in a bank), while the private key allows to create transactions "belonging" to this address.

If Bitcoin only allowed clearing transactions, it could not work, as there would be no balances to transfer. Therefore, a special type of transaction is permitted once per block, which "creates" new bitcoins (colloquially referred to as "mining"). The allowed amount of new bitcoins in each block is predetermined and degressive over time. An amount different from the predetermined one is not consistent with the blockchain rules and is ignored. The duration of the creation of blocks is controlled by a mechanism called "proof

[1] Strictly speaking, it is not necessary for all the nodes to have a full copy for Bitcoin to work correctly. I am simplifying at the cost of inaccuracies, here as well as in most other technical descriptions, in order to concentrate on the economic factors.

of work" and is balanced to create a new block approximately every 10 minutes. These newly produced bitcoins subsidise the maintenance of the ledger, as the computers that maintain it are the ones that receive this newly produced bitcoins. As the production rate falls over time, an additional source of revenue for the miners are transaction fees, which the senders of the transaction may voluntarily specify. The miners, similarly, voluntarily choose which transactions to include in the block. Upon assembling of the block, the miner also collect the transaction fees of the transactions included in the block.

2.2 Socioeconomic effects of Bitcoin

As is evident from the description of Bitcoin system from the previous section, the Bitcoin system, in the narrower sense, is purely virtual. The account number (Bitcoin address), as well as its balance, are fundamentally merely numbers, and the control of the balance is achieved by another number. However, the consistency of the whole system is based on predetermined rules which are easy to verify (and from a practical point of view, enforced automatically), and shared across all the physical components of the Bitcoin network, and all the users interacting through Bitcoin. The users of Bitcoin can reasonably expect that the system will behave according to those rules. Users can reasonably expect that the supply of Bitcoin will continue according to a predetermined schedule, and that as long as they keep their private keys secret, they, and only they, can control the balance of their account, and can do with it whatever they want, as long as the activity adheres to those rules. The rules themselves are also purely abstract and based on mathematics. They are oblivious to social conventions, irrespective of their nature. Whether these social conventions are minor or major, local or global, political or apolitical, ethical or unethical, the users of Bitcoin can reasonably expect that Bitcoin (in the narrower sense) will ignore them.

On one hand, this can have an enormous impact on liberating the users of Bitcoin from social norms they disagree with. On the other hand, it also exposes them to potential risks associated with the absence of these norms. If however the users accept the *abstract rule* of Bitcoin, that "the holder of the private key has exclusive control of the corresponding balance" as a *social norm* (i.e., "the holder of the private key *should* have exclusive control of the corresponding balance"), the vast majority of the risks associated with social norms vanish. Such social norms have a high appeal among libertarians. A very clear statement to this effect is made by Suede (2011a):

> "In a hypothetical world where it is impossible to take another person's property through force or coercion, could a State exist? The obvious answer to this question is no. At least not as we know it today. There could necessarily be no coercively funded State since all transactions would have to be through voluntary trade. If we refine our question again, only limiting it simply to currency, could the modern State still exist? I think the answer to this question is also no. While a hypothetical world where violent and coercive looting could not exist is outside the realm of the possible, a situation where an "unlootable" currency exists is entirely within the realm of possibility."

On the opposite side of the spectrum, emphasising the consequence of the abandonment of existing social norms, Dellingshausen (2011) argues:

> "The usage of Bitcoin as a method of payment makes it impossible for the state to conduct the mandatory auditing in cases of tax evasion or money laundering. Therefore Bitcoins are outright dangerous and have the potential to deal damage to the whole society by tax evasion, money laundering or other illegal trade."[2]
>
> ...
>
> "We assume that 'replacement currencies' such as Bitcoin will sooner or later be forbidden by the legislature, as they evade its responsibility to protect its citizens and the society. Regulation of payments is necessary for the security and well-being of consumers, but also in the interest of merchants and operators of online-shops."[3]

This fundamental difference in ethical assessment of various social norms permeates from the ideological to the economic assessment of Bitcoin. While Keynesians (e.g. Vernengo (2012)) view its features negatively, Austrians (e.g. Matonis (2012a)) view its features positively. However, there is something particular about the dichotomy between the above quotes (Suede vs. Dellingshausen): they *agree* on what the economic consequence of Bitcoin are expected to be, they merely differ in the *appraisal* thereof.

What I tried to demonstrate in this section is that publicly available sources about Bitcoin expose a heavy polarisation in the society, and this has a tendency to skew the perception of the economics of Bitcoin as well. As economic analysis from a libertarian point of view must be strictly neutral, and value-free (including ignoring the [current] law), becoming aware of this heavy polarisation can help to recognise and avoid it. This is crucial for any economic treatment of Bitcoin.

2.3 Forms of Bitcoin

In this section various forms of media of exchange will be discussed, and it will be analysed how it is possible to implement them using Bitcoin. In many cases, these methods of payment already have Bitcoin-based implementations.

Bitcoin can be used as a method of payment in two basic ways. For the purposes of this thesis, I will call them "transfer of balances" (ToB) and "transfer of keys" (ToK).

ToB works by creating a transaction recognised by the Bitcoin network. This "debits" the account(s) of the sending party (inputs), and "credits" the account(s) of the receiving party (outputs). A single transaction can have more than one input and more than one output. This is functionally similar to electronic fund transfers (EFT) that are available by the current banking system. For this to work to full extent, the transaction needs to be injected into the Bitcoin network and become a part of a block. Therefore, this type of transfer is typically associated with online payment methods.

ToK works by making the keys that "unlock" the balance (private keys) of an account accessible to another party. The party can then initiate transactions that "debit" this

[2] Translated from "Durch die Nutzung von Bitcoins als Zahlungsmittel wird die notwendige Kontrolle durch den Staat in den Fällen von Steuerhinterziehung oder Geldwäsche unmöglich. Deswegen sind Bitcoins schlichtweg gefährlich und haben das Potenzial, der gesamten Gesellschaft eben durch Steuerhinterziehung, Geldwäsche oder andere illegale Geschäfte nachhaltig zu schaden."

[3] Translated from "Wir gehen davon aus, dass ‚Ersatzwährungen' wie Bitcoins über kurz oder lang auch durch den Gesetzgeber verboten werden, weil er sich in der Verantwortung sieht, seine Bürger und die Gesellschaft weitreichend zu schützen. Für die Sicherheit und das Wohl der Verbraucher, aber auch im Sinne der Interessen von Händlern und Betreibern von Online-Shops muss ein Regulativ für die Zahlungsmittel existieren."

account themselves. This is functionally similar (but not identical) to giving someone a bearer instrument, for example a bank note[4], or a bearer bank-book. The knowledge of the private key for the duration of the transfer is not necessary for this type of transfer to work, only the possession. They key itself can be obscured, for example, to prevent anyone from using it to create a new transaction. Of course, since the key is essentially just a number, this method is only suitable when the original holder does not have the private key after the transfer any more (or at least, if the new holder does not mind it), since anyone who has access to the keys can initiate transactions and thereby prevent other holders of the same key from using the same balance. Because of this, this type of transfer is typically associated with offline payment methods, i.e. exchange of a physical medium containing the (obscured) private key. Christin and Brito (2012) also use the term "out of band transactions" for such a method of transferring bitcoins.

The dual character of Bitcoin payment methods can be seen as a combination of the features of money (commodity) with a clearing system (service). The commodity provides a stable supply and physical control, while the service provides low transaction costs, clearing services and record keeping. Prior to Bitcoin, these two were separated.

2.3.1 Native forms

Because a Bitcoin keypair is just two numbers, it can manifest itself in many forms. In other words, Bitcoin is *form-invariant.*[5] A digital representation of the Bitcoin keypair contains 512 bits of data (two keys with 256 bits each), which is equivalent to 64 bytes, or 128 hexadecimal characters (in the range 0-9 and A-F). Having access to a keypair allows full control over an account (sending and receiving). *Any object that can safely store 64 bytes of data characters is hypothetically usable as a native form of Bitcoin.* Furthermore, the data can be protected by

- encryption: This prevents potential illegitimate possessors of the key from being able to use it.
- copying: Unlike many immaterial goods, copying of Bitcoin does not increase the amount of Bitcoins, nor does it allow the Bitcoin to be spent twice. This is a direct consequence of the public ledger. The ledger needs to balance, and an attempt to add new Bitcoins in violation of the protocol is rejected. Thus Bitcoin is said to solve the double-spending problem (even though Karame et al. (2012) argue that there are practical deficiencies in the implementation).
- splitting: Private keys can be algorithmically divided (split) into multiple components, and only a combination of those can "unlock" access. Multi-key signatures (m of n) are also possible.

[4] I mean bank notes as they used to exist prior to the states obtaining monopoly on the production of bank notes. In those times, bank notes were a bearer instruments issued by commercial banks. Private issuance of bank notes still exists in some countries, for example Northern Ireland, Scotland or Hong Kong.

[5] This is somewhat unusual when it comes to money, but it is easier to understand by the analogy of language. Language can exist in written or oral form. These forms have the same meaning, but are physically different and the preference to use one or the other depends on the context. From these two basic forms, other forms can be derived, such as ink on paper or digital written form. People in general have no problems switching between these two forms: they can read and write. Computerised methods for conversion exist, with varying degrees of success.

Coins

There are already physical coins as a form of Bitcoin. An example would be Casascius physical coin[6] (see Figure 2.1 on page 12). The coin is made from metal (in the case of Casascius, bronze, silver or gold are used, depending on the denomination), and contains a new keypair (public and private key) of a Bitcoin address. When manufactured, the amount of Bitcoins at that address is identical to the nominal value of the coin. The public key of the Bitcoin address is visible on the outside of the coin, and since its balance is publicly known, it can be verified online (for example using Blockexplorer[7]). The coin is constructed in such a way that the private key can only be decoded if the coin is visibly damaged. In the case of Casascius, the private key is on an inner side of a hologram. If one peels off the hologram from the coin, the surface of the coin changes so that it is distinguishable from an undamaged coin. The pair (private and public key) can be typed into a file and then imported into any Bitcoin wallet (e.g. one on a local computer). The requirement to destruct the coin is a method to make attempts at double-spending obvious.

Since the public key is visible on the outside, it is possible to send a balance to the coin after it has been created (leading to it having a higher balance than the nominal value). However, the only way to extract the balance is to obtain the private key, which is normally only possible by destroying the hologram.

Banknotes

Banknotes can be constructed similarly to coins. There are already forms of Bitcoin like this, for example Bitbills[8] (see Figure 2.2 on page 13). A Bitbill is a thin plastic card that has a public key in textual form and QR code[9] on the outside. When the card is broken (this requires considerable damage to the card), it reveals a hologram with a textual form and QR code of the private key.

Another form similar to bank notes are Printcoins[10]. They are a piece of paper with QR codes for the public key / address, textual descriptions, and a QR code for the private key hidden behind a hologram.

Cheques

There are attempts to create cheque-like Bitcoin at a very early development stage.

[6] Casascius coins can be purchased directly from the manufacturer, Mike Caldwell, at http://www.casascius.com (only by paying with digital Bitcoins), or from http://www.memorydealers.com (which also accept other payment methods, such as credit cards or cash).

[7] Blockexplorer can be reached at http://www.blockexplorer.com

[8] Bitbills could be obtained in the past from http://bitbills.com. Bitbills demonstrate the functionality of different forms of Bitcoin very well. They appear to have only been produced during a short period of time (I pre-ordered and was able to receive mine). The organisation behind the production claimed that they used MyBitcoin (http://www.mybitcoin.com) for payment processing. However, MyBitcoin ceased operations (and the website does not work anymore). Thereupon, the organisation producing Bitbills stopped taking new orders and did not reinstate them so far. Nevertheless, since Bitbills are merely a native form of Bitcoin rather than a debt instrument, the status of the producer has no effect on their functionality. If Bitbills were a debt instrument, like it is usual with money (and until Bitcoin, necessary), all produced Bitbills would have become unusable and as a consequence practically worthless.

[9] QR codes, or Quick Response Codes, is a type of matrix barcode (or two dimensional barcode). Through optical recognition the data embedded in the code can be transferred into an electronic device. A smartphone with a camera is usually sufficient to decode QR codes. Source: http://en.wikipedia.org/wiki/QR_code

[10] Printcoins can be obtained from http://www.printcoins.com

Figure 2.1: Casascius physical Bitcoins

Figure 2.2: Bitbills

I do not know of exact examples of cheque-like Bitcoin, but it is possible to create a similar instrument. The cheque issuer would use a computer to construct a combination of a newly generated keypair and a transaction message that transfers a specific amount of bitcoins from the issuer's wallet to the address represented by the keypair. Then the issuer would print out the message and the keypair as a textual form and/or QR code. The physical size of a cheque should be sufficient to accommodate this amount of data. Redeeming the cheque can be done at any computer connected to a wallet, similarly as with coins/notes, only in this case the transaction message would be injected into the Bitcoin network as well. If the transaction is not valid (e.g. insufficient funds at the sending address), the result would be equivalent to a cheque bouncing, only it would be discernible at the time of redeeming the "cheque".

The aforementioned Printcoins are also available with "open" denomination, which means that anyone can fund it in any denomination, and it will act similarly as a cheque.

Smart card (e.g. debit card)

A Bitcoin smart card would contain a public/private keypair, a chip with an implementation of the Bitcoin algorithms and a method of communicating (e.g. contact chip or RFID[11]). The card holder would insert the card into the merchant's terminal (or use some other method to communicate, such as an electromagnetic field in case of RFID) and type in the PIN code to unlock the transfer functionality. The terminal would transmit the destination address and the sum to be transferred. The card would construct an encrypted message to perform the transfer, and the terminal will inject the message into the Bitcoin network. If there are insufficient funds "on the card", the network will ignore the message and the terminal can provide feedback regarding this.

It is not necessary for the terminal to be a Bitcoin node directly, it can proxy the data to a real Bitcoin node, thereby reducing the requirements for data storage and transfer to only those specific for the transaction itself.

There are at least two developments currently publicly known that attempt to implement this. The Bitcoincard[12], see Figure 2.3 on page 15 and Ellet. Bitcoincard has working prototypes.

Wire Transfers / EFT

Wire transfers (or in UK terminology, "EFT" for Electronic Funds Transfer) are the "classical" type of Bitcoin usage and do not require special attention. A recipient gives one of his addresses to the sender, the sender creates a message to transfer the funds, and the Bitcoin network validates the transfer. An example would be the original satoshi client with its current graphical interface, Bitcoin QT (Figure 2.4 on page 15).

Some e-wallets also use native Bitcoin technology, by using client-side encryption (fully or partially). Examples are the blockchain.info wallet[13] and Strongcoin[14].

[11] RFID, or Radio-frequency identification is a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data. Source: http://en.wikipedia.org/wiki/RFID

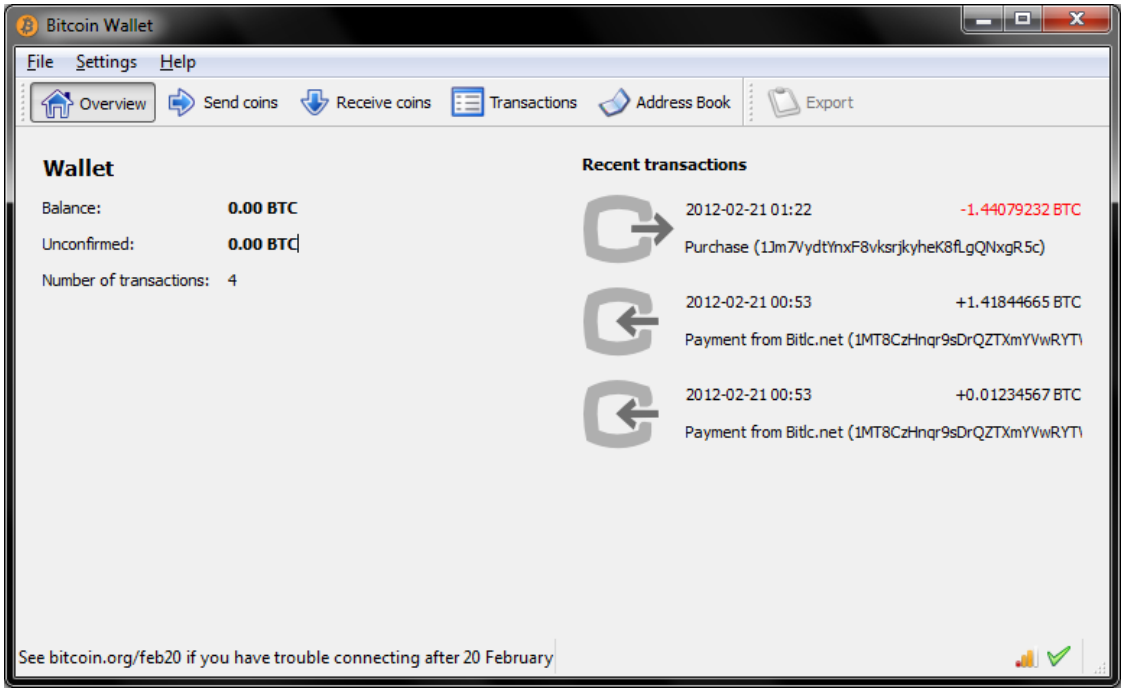
[12] Bitcoincard is currently being developed and not available to general public. Prototypes have been demonstrated on conferences, for example. More information and current status can be obtained at the company website, http://www.bitcoincard.org

[13] The blockchain.info wallet is accessible at https://blockchain.info/wallet/. Blockchain.info also provides a smartphone wallet application, web access to the data in the blockchain, and various statistical data about Bitcoin.

[14] Strongcoin is accessible at https://www.strongcoin.com/

Figure 2.3: Bitcoincard next to a generic club membership card

Figure 2.4: Bitcoin QT. Source: http://commons.wikimedia.org/wiki/File:Screenshot_of_Bitcoin-qt.png



Mobile phone

There are already several examples of using mobile phone as a payment system for Bitcoin[15]. Similarly as with smart cards, there are POS (point of sale) terminals available as well. The communication at the moment is implemented using screen/camera combination and NFC (near field communication), but other methods are imaginable (for example, audio signal transmission or RFID (radio-frequency identification). The client (on the phone) retrieves the recipient Bitcoin address and the sum, constructs the transaction message and transfers it over the internet to the Bitcoin network. The POS sees the transaction and can consider the payment completed. If one does not have a special POS terminal, one can use a mobile phone instead of it as well. It is imaginable that this can be implemented even for situations where the payee does not have internet access; he just transmits the message to the other terminal/POS.

High durability forms

In a forum discussion about protecting Bitcoins from electromagnetic fields, deepceleron (2012) suggested a highly durable medium in the form of a tungsten brick with laser-engraved keys and provided a photo montage of what it might look like (see Figure 2.5 on page 17). Tungsten is the element with the highest melting point and is also quite resistant to physical and chemical damage. Simultaneously, it is not excessively expensive either. A tungsten brick can survive a fire, for example.

Brainwallet

Another interesting form of Bitcoin is a Brainwallet. It is a metaphor for remembering the keypair (or at least the private key). The brain acts as a storage medium and becomes a form of Bitcoin. Such a form is highly resistant against theft and even detection. Brainwallet is analysed by Matonis (2012b) and Buterin (2012b).

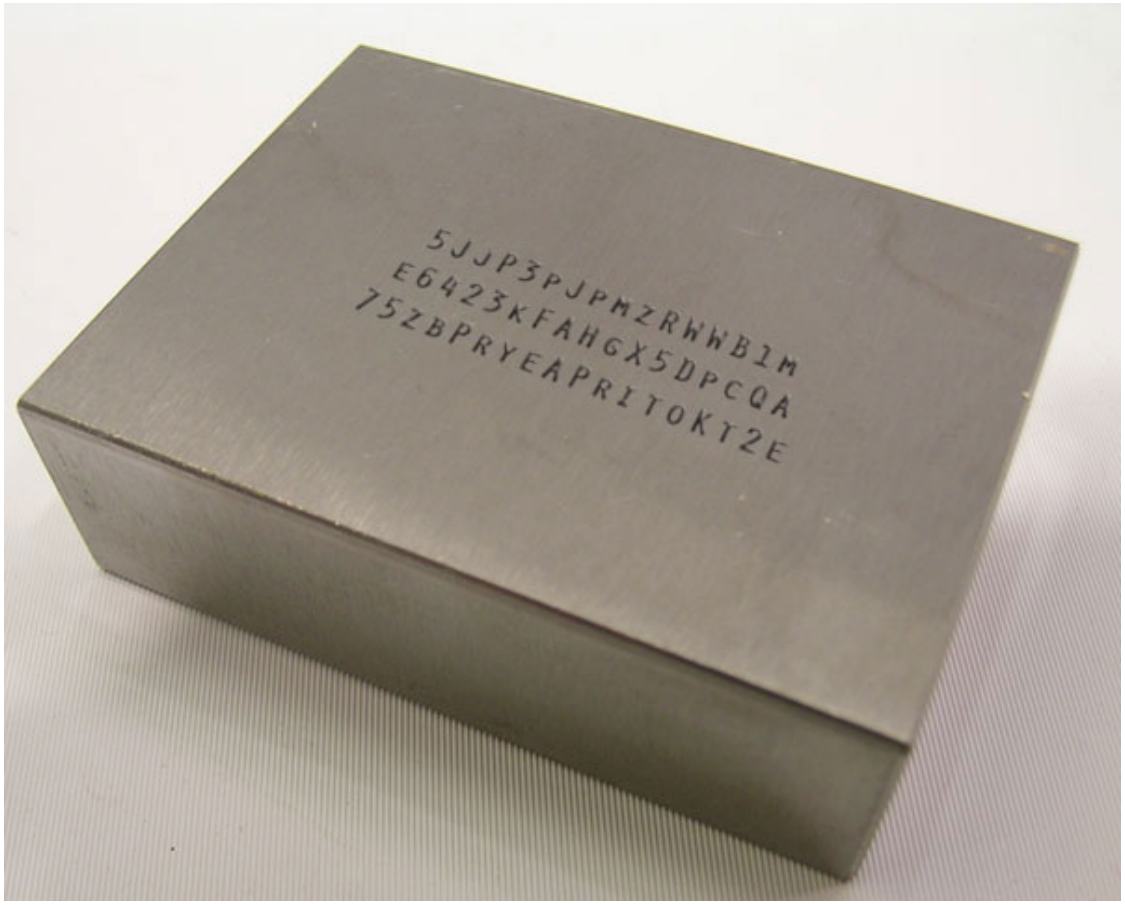
2.3.2 Financial instruments

I would like to reiterate that all the forms mentioned in the previous subsection are native forms of Bitcoin. Not only do those examples not require a separate clearing mechanism or a financial institution, they do not even require a middleman (other than the Bitcoin network itself). Some participants might prefer to store their Bitcoins at a third party facility (such as a Bitcoin bank or a Bitcoin exchange), but there is no separate payment processor or issuer of the payment instrument. Importantly though, their use depends on the functioning of the Bitcoin network itself.

Similarly as with almost anything else, it is possible to issue financial instruments denominated in Bitcoin. The issuer may, for example, keep the deposited bitcoins in reserve, and issue a financial instrument with the corresponding balance. Some of those already exist. In principle, it is possible to use them as a medium of exchange, however, not all Bitcoin denominated financial instruments support this feature. A more detailed elaboration is presented in Section 2.4.

[15] For example, BitcoinSpinner is an Android application, available through Android Market

Figure 2.5: High durability Bitcoin key laser-engraved on a tungsten brick. Photomontage by deepceleron, original image from Avery Tools website, http://www.averytools.com/prodinfo.asp?number=6004.



Issuers of these instruments implement the transferability for example through redeemable codes. This is just a unique string of characters and digits (i.e., from the point of view of a computer, a number) that identifies the instrument, and allows anyone using the same system to use this string to deposit the corresponding balance into their account. Often the issuer provides redeemable codes denominated in Bitcoin as well as other currencies. The recipient can also be another service provider that provides new services built on top of the first one.

Various (2012) explains that there is a potential demand for these redeemable codes as a medium of exchange:

> "A BTC-denominated redeemable code allows a transaction involving bitcoin-backed funds to be completed instantly. This contrasts with a withdraw of bitcoins using the bitcoin network because bitcoin transactions need to first confirm — a process that can typically take an hour or so. This might explain why some merchants have started to accept redeemable codes from various exchanges as an alternative payment method as well."

However, in the reference Various used, I could only find a mention the use of a USD-denominated code being accepted in payment, not a Bitcoin denominated one. The demand for Bitcoin denominated financial instruments as a medium of exchange will be analysed in more detail in 3.7.2.

2.4 Products and services of the broader Bitcoin ecosystem

Since Bitcoin in the narrower sense is purely abstract and mathematically complex, in order to work it requires a computer with Bitcoin software. The original software is referred to as "satoshi client". It contains a command line version "bitcoind" and a version with a graphical interface called Bitcoin QT. The original software is used as a reference implementation and is being developed in an open source model.[16] All the fundamental mathematical properties of Bitcoin can be verified in the source of the satoshi client.

Even though the original Bitcoin client contained all the functions (creating transactions, mining, storing keypairs, storing and distributing the blockchain) specialised software was later developed to facilitate specific functions. For example, it was discovered that graphics cards are more suitable for mining than main processors, so software that only mines and cannot create new transactions or manage accounts was developed. Because the chance of calculating the block decreased as more and more people started participating, mining pools emerged. These combine the mining capacity of participants and split the winnings. Statistically, the mean return of pool mining is the same as with solo mining, but has lower variance. Instead of having a chance of gaining 50 Bitcoins once every 50 days, for example, one can obtain one Bitcoin every day.

People wanted to obtain Bitcoins without having to mine them themselves, and therefore exchanges emerged. These work similarly to foreign currency exchanges also known as "forex": one transfers an accepted currency (including Bitcoin) to the exchange, and then sets up trade orders (exchanges of Bitcoin for another currency, either buying or selling). The exchange system matches the two sides together and performs the change.

[16] Satoshi client can be downloaded from http://bitcoin.org/clients.html

The balance can be then withdrawn. Some of the more widely known exchanges are Mt.Gox [17] or Intersango[18]. Mt.Gox is the market leader with the majority of publicly known exchange transactions occurring on it. Exchanges allow the establishment a market price for Bitcoin, and to provide liquidity to the market (Menger (1892) used the term "organised markets"[19] for such places or establishments). A financial data aggregator BitcoinCharts[20] lists Bitcoin trading against 18 currencies and 27 exchanges. The service operators, in particular the exchanges, often operate continuously, 24/7.

People started desiring more elaborate instruments. One of the service providers, MPEx[21], provides stocks, funds and options built on Bitcoin.

Many service providers only lasted shortly and stopped operating in the meantime. Examples are TradeHill (stopped operating due to unexpected losses), MyBitcoin (alleged hack), Bitcoin Savings and Trust ("BTCST") (appears to have been a Ponzi scheme), Bitcoinica (currently in liquidation), or Global Bitcoin Stock Exchange ("GLBSE") (reason for closure undisclosed, presumed to be regulatory risk). In extreme cases, the operators of these services vanished with customers' funds.

Services appeared that offer physical forms of Bitcoin similar to historical forms of money, such as coins and banknotes. There are also online wallets (they provide the ability to use Bitcoin without having to use a specialised program and rely on a web browser instead, such as are blockchain.info[22], strongcoin[23] (which also provides merchant services). A summary of other service providers is Table 2.1 on page 20.

The Bitcoin wiki page lists 838 (as of June 18th 2012, source Spekulatius (2012)) merchants and service providers that accept Bitcoin, and a couple of dozen organisations accepting donations in Bitcoin.

2.5 Advanced features of Bitcoin

In addition to a pure clearing function, Bitcoin has the ability to use more complex algorithmical structures through it own scripting language. This functionality is not yet usable to its full extent, as some of the uses require additional integrating infrastructure.

The term used for advanced transaction features of Bitcoin is "contracts". According to Hearn (2012), some of the possible uses are:

- Micropayments: pooling of smaller transactions into bigger ones for a further reduction of transaction fees.
- Dispute mediation: trading parties can elect a third party arbiter prior to transferring money. The arbiter does not take control of the balance, he can mediate between the trading parties. This decreases the level of trust in the arbiter.
- Automated mediation: the arbiter can even be fully automated, eliminating the dependence of arbitration on the human factor even further, if the data necessary to

[17] Mt.Gox can be reached at https://www.mtgox.com
[18] Intersango can be reached at https://intersango.com
[19] Menger appears to have used the term "organised markets" not in the sense of regulation and supervision, as it is now, but the degree of specialisation of the market participants. The term "specialised markets" might be more appropriate.
[20] BitcoinCharts is available at http://bitcoincharts.com/markets/
[21] MPEx is reachable at http://polimedia.us/bitcoin/mpex.php
[22] blockchain.info is available at https://blockchain.info/wallet/
[23] strongcoin is available at https://www.strongcoin.com/

Table 2.1: Assorted services and goods providers in Bitcoin ecosystem

Name	Description	URL
Coinapult	Sending of Bitcoins via SMS or email	http://www.coinapult.com
BitPay	Merchant services	http://www.bitpay.com
Paymium	Merchant services	http://www.paymium.com
Coinabul	Trading precious metals	http://www.coinabul.com
TorWallet	Anonymising	Only on TOR
Bitcoin Fog	Anonymising	http://www.bitcoinfog.com/
Chateau deCrypto	Erotica	see Taaki (2012)
Girls Gone Bitcoin	Erotica	see Taaki (2012)
OKpay	Integration with prepaid payment cards	http://www.okpay.com
Coindl	Digital goods sale platform	http://www.coindl.com
Cryptocurrency Legal Advocacy Group	Advocacy / legal research	http://www.theclag.org
Bitcoin Magazine	Journal	http://www.bitcoinmagazine.net
SatoshiDice	Gambling	http://www.satoshidice.com
Silk Road	Auction site for potentially illegal goods	Only on TOR

make the decision is available online. An example could be a postal tracking number as a proof of shipping, or bets based on sport results.

- Assurance contracts: allows pledging money for a pooled common goal. The balances are only transferred when the goal is reached. This makes it easier to create goods that are otherwise difficult to fund (such as public goods).
- Smart property: goods that contain electronics can use the Bitcoin network to verify their ownership. A buyer of a house, for example, can use Bitcoin as an electronic payment receipt, which the house would evaluate as a proof of ownership and unlock the door. In a case of a car, the receipt could start the engine.
- Other possible features are un-collateralised lending, P2P investment funds and P2P currency exchange.

A common factor of these advanced features is the decrease of the required level of trust in the human factor. The trust is replaced with a mathematical proof.

2.6 Summary

While Bitcoin is at a very early stage of evolution, it presents a fundamental innovation of money. Its ecosystem shows a wide variety of features, a high degree of specialisation, and a potential for even more innovation.

Chapter 3

Theoretical analysis of Bitcoin

3.1 Functions of money

Historically, money has been defined through its functionality, the three main functions being (Krugman (1984)):

> "Money, the classical economists argued, serves three functions: it is a *medium of exchange*, a *unit of accoun*t, and a *store of value*." [emphasis added]

The Austrian School however uses a more precise definition: money is the most universal medium of exchange, the most liquid good (Mises (1912)):

> "Thus there would be an inevitable tendency for the less marketable of the series of goods used as media of exchange to be one by one rejected until at last only a single commodity remained, which was *universally employed as a medium of exchange; in a word, money*." [emphasis added]

The other functions of money are considered secondary to the defining function as a medium of exchange. These other functions of money may emerge as money gains a higher liquidity. For, example Schlichter (2011) writes:

> "All additional functions that can be assigned to money are the result of money being the accepted medium of exchange."

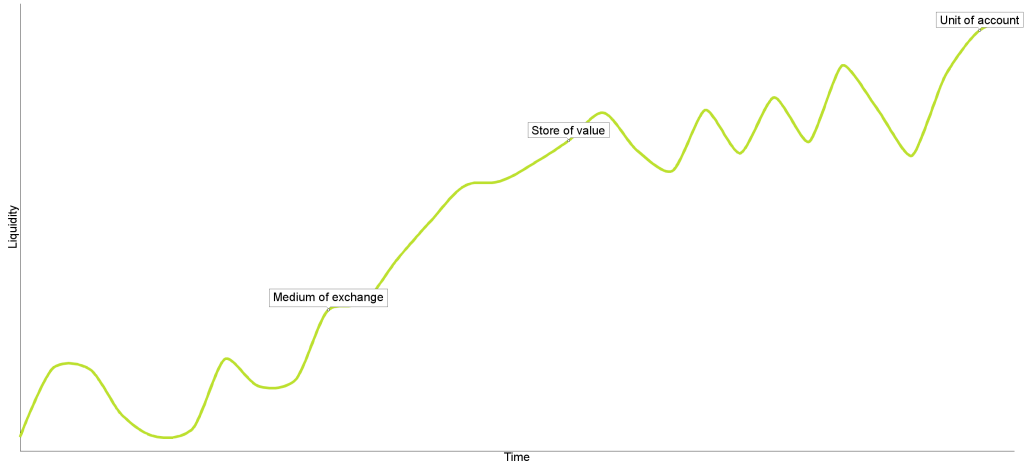
Similarly, it is argued by Menger (1871) that:

> "But it appears to me to be just as certain that the functions of being a "measure of value" and a "store of value" must not be attributed to money as such, since these functions are of a merely accidental nature and are not an essential part of the concept of money."

Alternatively, White (1984), making a direct connection between the secondary functions and liquidity:

> "It should be readily apparent by extension of this perspective on the origin of money hat a unit of account emerges together with and wedded to a medium of exchange. ... A non-exchange medium numeraire commodity would furthermore be subject to greater bid-ask spreads in barter against other commodities, as by hypothesis it is less saleable, than the medium of exchange."

Figure 3.1: Functions of money from the Austrian perspective. The chart is for illustrative purposes and does not represent actual data.



Yet another example is Salerno (2010):

> "All other functions of money, e.g. as a "store of value," "unit of account," "standard of deferred payments," are and must remain subsidiary to money's primary function as a medium of exchange."

A graphical representation of the functions of money from the Austrian perspective can be seen in Figure 3.1 on page 22. The graph does not allow pinpointing of the time when a medium of exchange becomes money, as that depends on its relationship with other media of exchange[24]. Also, the respective position of "store of value" and "unit of account" is incidental.

Bitcoin is not a universally accepted medium of exchange, therefore, from Austrian viewpoint, it is not money. Thus, Pattison (2011) asks:

> "But if Bitcoin is not money, what is it?"

Even though not money, Bitcoin is a medium of exchange. A non-universal medium of exchange is classified by the Austrians as *secondary medium of exchange*, as described by Mises (1999):

> "Consequently there emerges a specific demand for such goods on the part of people eager to keep them in order to reduce the costs of cash holding. The prices of these goods are partly determined by this specific demand; they would be lower in its absence. *These goods are secondary media of exchange*, as it were, and their exchange value is the resultant of two kinds of demand: the demand related to their services as secondary media of exchange, and the demand related to the other services they render." [emphasis added]

[24] In order to reflect this graphically, a three dimensional graph would be necessary and for the purposes of this thesis might lead to confusion.

A similar approach is taken by Rothbard (2004), who calls such media of exchange *quasi-money*:

> "We have implicitly assumed that there are one or two media that are fully marketable — always salable — and other commodities that are simply sold for money. We have omitted mention of the degrees of marketability of these goods. Some goods are more readily marketable than others. *And some are so easily marketable that they rise practically to the status of quasi moneys.*" [emphasis added]

If Bitcoin was to be positioned in Figure 3.1 on page 22, it would be on the line after the position "medium of exchange". Its position with respect to the other two positions "store of value" and "unit of account" is controversial. Further below, I will try to argue that hypothetically, Bitcoin can cross these thresholds, if it had not crossed them yet.

3.2 Austrian classification system for money

Mises (1912) introduced a classification system for money, here reprinted as Figure 3.2 on page 24. On the first level, "money in broader sense" is divided into "money in the narrower sense" (approximately corresponding to the terms "monetary base" or "outside money" used by other economic schools) and "money substitutes" (approximately corresponding to the terms "other forms of money" or "inside money" used by other economic schools).

3.2.1 Money in the narrower sense

Money in the narrower sense is further subdivided into "commodity money", "fiat money" and "credit money":

> "We may give the name *commodity money* to that sort of money that is at the same time a commercial commodity; and the name *fiat money* to money that comprises things with a special legal qualification."[25] [emphasis added]

3.2.2 Money substitutes

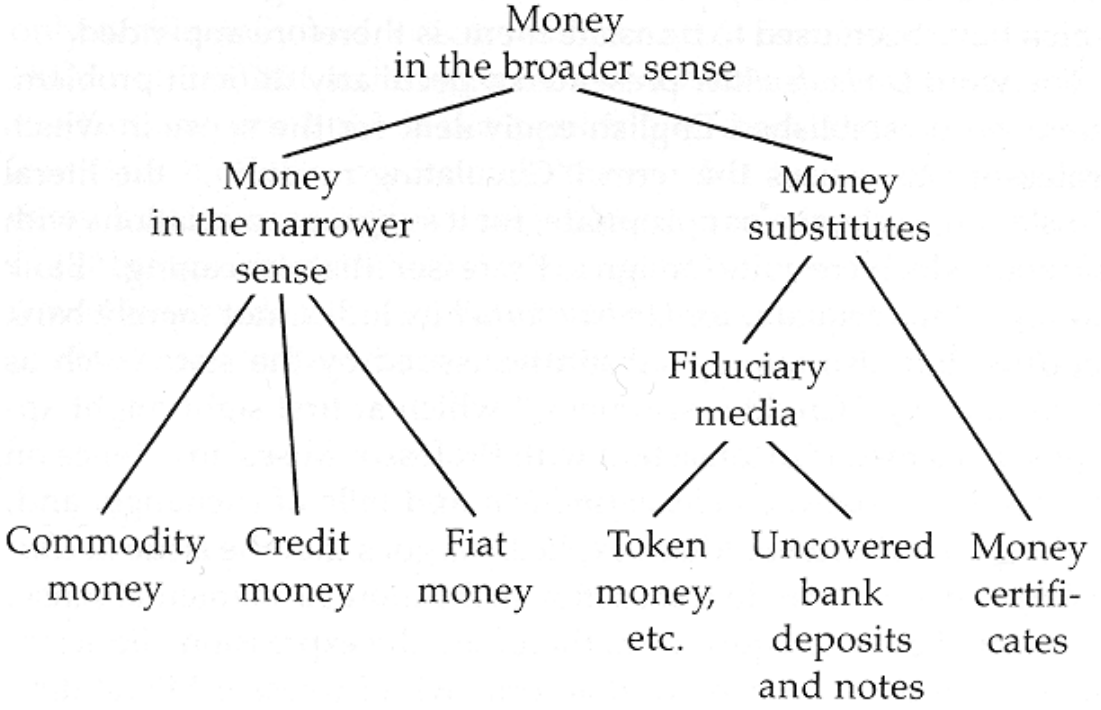
Money substitutes are defined as (Mises (1912)):

> "The special suitability for facilitating indirect exchanges possessed by *absolutely secure and immediately payable claims to money*, which we may briefly refer to as money substitutes, is further increased by their standing in law and commerce."[26] [emphasis added]

[25] Mises also defines a third category, "credit money", "... being that sort of money which constitutes a claim against any physical or legal person. But these claims must not be both payable on demand and absolutely secure; if they were, there could be no difference between their value and that of the sum of money to which they referred, and they could not be subjected to an independent process of valuation on the part of those who dealt with them. In some way or other the maturity of these claims must be postponed to some future time." When Mises was writing this, pure fiat money did not exist yet, only credit money. Currently, the situation is reversed: all national currencies are pure fiat monies and the concept of credit money is of little practical use. For the purposes of this thesis, I will therefore ignore the category credit money.

[26] I discussed this with Robert Murphy, since this was one of the questions on the test in his course "Mises on Money and Banking" at the Mises University. He said that this is the Misesian definition.

Figure 3.2: Classification of money according to the the Austrian School. Source: Mises (1912)



On its own, there is nothing wrong with this definition. However, in other places of the same book, Mises only uses the term money substitute to refer to only those things that act as substitutes from economic point of view, i.e. they are used as a medium of exchange directly. In other words, he uses the term "money substitutes" in the meaning of the first part of the sentence quoted above, "special suitability for facilitating indirect exchanges", rather than the second one, "absolutely secure and immediately payable claims to money":

> "It may be pointed out that those who require money will be quite satisfied with such claims as these, and that *those who wish to spend money will find that these claims answer their purpose just as well*; and that consequently the supply of money-substitutes must be reckoned in with that of money, and the demand for them with the demand for money." [emphasis added]

or

> "The fact that is peculiar to money alone is not that mature and secure claims to money are as highly valued in commerce as the sums of money to which they refer, but rather that *such claims are complete substitutes for money, and, as such, are able to fulfil all the functions of money* in those markets in which their essential characteristics of maturity and security are recognized." [emphasis added]

Even stronger example of this unclarity is Salerno (2010), who presents both of these definitions in the same sentence:

> "*. . . perfectly secure and immediately convertible claims to money*, such as bank notes and demand deposits, which *substitute for money in individuals' cash balances*."

Essentially, both Mises and Salerno each imply two definitions of money substitutes and use them interchangeably:

- secure claims on money in the narrower sense with zero maturity
- things that act as substitutes to money in the narrower sense from economic point of view

This dichotomy is apparent in many other Austrian writings, which also use these two definitions interchangeably. One of them is legal, the other one economic. However, Mises (1912) recognises that they are not necessarily identical and writes:

> "Besides strictly legal claims to money, we must also take into account such *relationships as are not claims in the juristic sense, but are nevertheless treated as such in commercial practice* because some concern or other deals with them as if they actually did constitute claims against itself." [emphasis added]

In order to avoid the whole legal aspect and concentrate on the economic one, I propose my own definition of money substitutes: money substitutes are goods which have a persistent causal link to money in the narrower sense, and act as a (near) perfect substitute to it from economic point of view.[27]

[27] Or in more colloquial terms, money substitutes are a *copy* of money in the narrower sense.

Money substitutes are further divided into "money certificates" and "fiduciary media". They differ in the amount of reserves backing them; money certificates are fully (i.e. 100%), backed by reserves, whereas fiduciary media are covered to a lesser extent. In the extreme case, since my definition allows for a money substitute that does not represent a claim at all, the reserve can be entirely absent.[28]

All fiat money begins as a money substitute. The US dollar, for example, was originally defined as a weight of gold. Mexican dollar was originally defined as a weight of silver. The link to a weight of a commodity can be traced for other names, for example, the Mark, Pound or Franc. Legislative intervention then eliminates this link, and the former money substitute becomes a new monetary base. Even the Euro started originally with pegged exchange rates among several European currencies. During a nationwide migration to the Euro, the old currency and the Euro circulate side by side, merchants being obligated to accept both. This obligation is only temporary, it lasts several weeks for normal merchants. Commercial banks are required to exchange the old currency for Euro for several months, while the deposit accounts and other financial instruments are centrally re-denominated. The central banks allow an even longer period for the exchange. During this time, from the perspective of the citizens of the country, the Euro is gradually to a smaller and smaller extent a money substitute and to a larger and larger extent money in the narrower sense, until the old currency all but vanishes from use and the process is concluded.

On the other hand, some other currency reforms are more strict, allow a much shorter time frame for conversion, or even invoke exchange limits or are accompanied by other forms of capital controls.

3.2.3 Classification of Bitcoin

As Bitcoin is not money yet, its classification as per Figure 3.2 on page 24 is, strictly speaking, not possible. However, should it develop into money, it could present a problem. Bitcoin is not and never was a money substitute, never had a special legal status, nor was it a claim against anybody, nor was a commercial commodity. Therefore, it would not fit into any of the subcategories of the classification. As a possible workaround, Selgin (2012) proposes the term "quasi-commodity money" for base money that does not have non-monetary uses, but is "naturally" (absolutely) scarce, and uses Bitcoin specifically as an example. For simplicity, I will refer to Bitcoin as (potential) commodity money with the justification that it has an inelastic supply, following Schlichter (2012b):

> "But equally it is commodity money because it is based on a cryptographic algorithm, which requires time and considerable computing energy to create Bitcoins and which is designed so that *the overall supply of Bitcoin is strictly limited*." [emphasis added]

Schlichter (2011) also emphasises the weight of this factor:

> "The *most important difference* between commodity money, such as a proper gold standard, and 'paper money', such as our present fiat money system, *is the elasticity of the money supply*." [emphasis added]

[28] An example would be the complementary currencies, analysed in 3.2.4.

As for other sources than that of the Austrian School, Wehinger (1997) provides classification systems for electronic forms of money. However, a similar problem occurs as with the Austrian classification mentioned above, as Wehinger assumes that electronic money is a debt instrument (a subset of money substitutes), rather than money in the narrower sense, as Bitcoin would be if it evolved into money. European Central Bank (2012) provides a classification system for virtual currencies, based on the level of openness. However, only one of the three categories actually classifies as money in the Austrian sense as the other two have their availability in trade heavily restricted, both through technological means as well as contractual restrictions.

3.2.4 Complementary currencies

In addition to the money categories mentioned above, there is also a phenomenon called "complementary currencies". An overview is presented by Greco (2001), while a more theoretical foundation for some of their aspects dates back to Gesell (1936) and a more current example is Andresen (2012). One of the more widely used examples is WIR[29], which was launched in 1934 and exists until now. Complementary currencies are neither money in the narrower sense, nor a claim against money in the narrower sense. Nevertheless, according to the definition of money substitutes used in this thesis, they are money substitutes.[30] They are persistently causally related to money in the narrower sense (e.g. the WIR is treated at par value with the Swiss Franc), and for their users, they act as nearly perfect substitutes (again, in the case of WIR, a substitute for the Swiss Franc). Calling them "currencies" is therefore, from the Austrian perspective, misleading, as they are not a separate money, rather they are a new form of existing money. Furthermore, not only are they merely a new form of existing money, their purpose is not to decrease transaction costs of trade (which, as I argue below, is in the Austrian perspective the only valid reason for a new money to appear), but to increase the money supply in a way that does not depend on fractional reserve banking or central banking. The Austrians, following Mises (1912), explicitly reject the notion that the increase in the money supply has a beneficial effect to the society:

> "Thus, we see that while an increase in the money supply, like an increase in the supply of any good, lowers its price, the change does not–unlike other goods–confer a social benefit. The public at large is not made richer."

Furthermore, conversion between complementary currencies and the national currency is often associated with high fees, or not available at all (in particular credit systems such as WIR or TEM[31] do not envision an exchange facility, and as far as I can conclude based on my research, there indeed is not any). This creates a "vendor lock-in", or an obstacle for a free choice and increases the transaction costs of trade. It compartmentalises the economy into smaller units, making them more autarkic, and more costly to conduct trade

[29] WIR is a credit system, implemented as a bookkeeping-only form (i.e. no scrip). "WIR" is both an abbreviation of *Wirtschaftsring* (economic circle) and the word for "we" in German, reminding participants that the economic circle is also a community. Source: http://en.wikipedia.org/wiki/WIR_Bank

[30] As a side effect, their existence emphasises the inadequacy of the definition of money substitutes used by other Austrian authors.

[31] TEM is a local exchange trading system (LETS) popular in Volos, Magnesia, Greece and stands for "Τοπική Εναλλακτική Μονάδα" ("Alternative Monetary Unit" in Greek). Source: http://en.wikipedia.org/wiki/TEM_(currency). Based on my research, it also appears to be a pure bookkeeping system without scrip, similarly as WIR.

among these units. It results in a devolution into a less complex economy. Whether this is beneficial or not is a normative question and outside of the scope of this thesis. My argument here is that such systems are neither economically similar to Bitcoin, nor are they viewed favourably from the Austrian perspective.

3.3 Evolution of money as competition among media of exchange

The important aspect of the Austrian approach to money is the the catallactic (emergent through market forces) origin of money. Out of the goods available on the market, the market actors voluntarily choose media of exchange according to their own preferences and use them in exchange. It should be noted that the process by which money is chosen by the market is, in the Austrian perspective, simultaneously also the normatively preferred one (in other words, good money is that which the market participants voluntarily choose as money).[32]

Also of importance is the realisation that the emergence of money from a non-monetary system is fundamentally the same process by which one money replaces other money: the same factors affect decisions in both cases. The same features that make money emerge also make it win (or lose) against other monies. On this, Thornton (1991) writes:

> "The market economy generates solutions to social problems; for example, the introduction (or evolution) of money reduces the transaction costs of exchange."

Extrapolating for the description of this process, as described by Menger (1892) as well as the broader context[33] of money, I abstracted the factors influencing the choice of a medium of exchange. This is summarised in Table 3.1 on page 29.

The diagram strikes with a wide variety of its components. Indeed, the transaction cost are heterogeneous. A medium of exchange that excels in one category might utterly fail in another one. It could also happen that none of the media of exchange can meet all the categories simultaneously, resulting in a more than one dominant medium of exchange. The heterogeneity is best captured by Menger (1871), who used the term "economic sacrifices" (which may be more explanatory than the abstract "transaction costs"):

> "But it is not easy to find an actual case in which an exchange operation can be performed without any economic sacrifices at all, even if they are confined only to the loss of time. Freight costs, loading charges, tolls, excise taxes, premiums for marine and other insurance, costs of correspondence, commissions and other sales costs, brokerage charges, weighages, packaging costs, storage charges, *the entire cost of the commercial banking system*, even the expenses of traders and all their employees, etc., are nothing but the various economic sacrifices which are required for the conduct of exchange operations and which absorb a portion of the economic gains resulting from the exploitation of existing exchange opportunities." [emphasis added]

While the emphasised passage is most relevant for Bitcoin, Menger manages to explain the broader context of transaction costs. A subsequent quote by Menger (1871) implies that transaction costs change over time:

[32] There are some minor exceptions to this, which I will address separately.
[33] Details about this context are further below in the analysis of the individual factors.

Table 3.1: Factors influencing the choice of medium of exchange

- Liquidity (network effect, double coincidence of wants)
- Store of value
  - demand-related (price volatility, trust, acceptance)
  - physical integrity
  - changes in the money supply
- Transaction costs in the narrower sense
  - Technological aspects (logistics)
    - storage
    - transport
    - manipulation
    - authentication
    - transaction fees
  - Transaction costs of property rights
    - Resistance to expropriation
    - Counterparty risk
  - Regulatory transaction costs
    - Barriers to entry
    - Price fixing
    - Capital controls

> "Economic development tends to reduce these economic sacrifices, with the result that even between the most distant lands more and more economic exchanges become possible which previously could not have taken place."

3.3.1 Liquidity (network effect, double coincidence of wants)

Normally, liquidity is the determining factor in the choice of a medium of exchange. Krugman (1980, 1984) argues, for example, that international traders may choose a highly liquid currency of a third country (for example, the US dollar) to conduct payments, even if none of the two countries use the dollar internally (and instead they use, for example, the currencies A and B, respectively). Even though this increases the number of transactions, as liquidity of the dollar/A market and dollar/B market is higher than the liquidity of the A/B market, overall transaction costs in the broader sense (or "friction", as Krugman calls them), are reduced. Similarly, Hoppe (1996) argues that:

> "Driven by no more than narrow self-interest, *man will always prefer a more general* and, if possible, a universal medium of exchange to a less general or non-universal one." [emphasis added]

What we see from both of these (Austrian and Keynesian) sources is that people do not choose the medium of exchange arbitrarily. There are factors influencing them. I will make the argument here that other situations where factors other than liquidity affect the transaction costs in the broader sense, and from the perspective of the choice of a medium of exchange take precedence over liquidity. I will call these factors transaction costs in the narrower sense.

3.3.2 Store of value

In order for a medium of exchange to work, people must have a certain level of expectations about its future value. Krugman (1984) argues, for example, that the store of value function can affect the decision about which medium of exchange to use:

> "In fact, there is some inter- dependence among roles. The links which seem clear are these: if the dollar is a good store of value, the costs of making markets against the dollar are lower, thus encouraging the vehicle role."

In other words, Krugman argues that value can, hypothetically, tip the scales and take precedence over liquidity as a deciding factor for the choice of a medium of exchange. The effect works in the opposite direction as well: demand for a medium of exchange can affect its store-of-value function. For a medium of exchange, a significant part of the demand is caused by its liquidity (as explained in 3.3.1), so media of exchange whose demand depends on liquidity to a higher proportion (for example, fiat currencies or Bitcoin) are subject to a higher risk from this point of view than other media of exchange (for example, precious metals or stones, or anything that can increase utility by direct consumption).

On the supply side, the store of value function is determined by its physical integrity and the changes in the supply.

Physical integrity

Menger (1892) writes that the saleableness of a commodity is affected by:

> "Their durability, i.e., their suitableness for preservation."

Since a Bitcoin keypair is just a number, it can, hypothetically, be preserved indefinitely in a wide variety of ways. It can be as durable or as brittle as the holder of the number wishes. The other component, the blockchain, is distributed. According to RowIT Ltd (2012), there are currently over 15.000 listening hosts (i.e. publicly accessible full copies of the blockchain) all over the world at the time of writing (November 10^{th} 2012).

It is difficult to imagine a system which would be more durable, in particular if we consider potential future developments of Bitcoin (e.g. storing the blockchain extraterrestrially).

Changes in the money supply

The production of new Bitcoins (generation of blocks) is determined by an algorithm. The probability of production follows Poisson distribution (Rosenfeld (2011)),[34] while the overall supply follows an approximately geometric (i.e. convergent) series[35]. Bitcoin thus has an upper limit of 21 million[36], i.e. 2.1×10^7. The lower size limit is 10 nanobitcoins, i.e. 10^{-8}, giving a total of 2.1×10^{15} transactable units[37]. The existence of the smallest transactable unit means that the supply of Bitcoin is discrete rather than continuous, therefore the production will not continue indefinitely, but eventually must fall below ten nanobitcoins, and effectively cease. A calculation reveals that this will occur around the year 2140.

Mises (1912) writes how the utility (value) of money decreases as its quantity increases:

> "*An increase in a community's stock of money* always means an increase in the amount of money held by a number of economic agents, whether these are the issuers of fiat or credit money or the producers of the substance of which commodity money is made. For these persons, the ratio between the demand for money and the stock of it is altered; they have a relative superfluity of money and a relative shortage of other economic goods. The immediate consequence of both circumstances is that the *marginal utility to them of the monetary unit diminishes*." [emphasis added]

It follows that ideally[38], the quantity of money should increase as little as possible, even not at all. Bitcoin's production function follows this ideal very closely. But a decrease in the quantity of money can increase the purchasing power too. Is it possible that a

[34] Hamacher and Katzenbeisser (2011) however dissent and argue that empirical data does not support the claim of Poisson distribution. They claim that the mean is not 600 seconds as it should be (I argue however that this is caused by the way the adaptation of production rate works and is expected behaviour). They furthermore claim that there are patterns in the production that are unexpected.

[35] This can be verified in the source code of the Bitcoin software.

[36] Due to rounding, discreteness and mining errors, it is slightly less than 21 million, but for simplicity I will use a more round figure.

[37] This 10 nBTC unit is also called "satoshi", in honour of the creator of Bitcoin

[38] Macroeconomic factors, such as changes in GDP or demography, are not considered in this evaluation, as these are relevant for policy decisions, not for the decisions of individual market actors. Market actors do not choose a medium of exchange based on aggregate variables, but on their microeconomic properties. However, sources analysing electronic money from macroeconomic point of view exist, and are to a certain extent applicable to Bitcoin. Examples would be Tanaka (1996); Wehinger (1997); Woodford (2000); Krüger (2001).

decreasing quantity of money is preferable? If the quantity of money was to decrease, the missing units must have had been in the possession of someone. This someone is then made poorer by the decrease of the quantity. A chance that their units of money will decrease makes it less likely for a potential owner to want to hold them.[39] A money with a decreasing supply is therefore suboptimal from this perspective.

Hamacher and Katzenbeisser (2011) argue that the Bitcoin private keys can be lost, which means that the balance associated with these keys becomes lost too (they cannot be used without the private key). They come to the conclusion that the loss of Bitcoins will eventually affect all Bitcoins and it would therefore cease to exist. For some reason which was not explained, they however appear to be using a linear progression in the predicted loss of Bitcoin, whereas I think a logarithmic progression is a more accurate model. With a logarithmic progression, there is no need for a complete disappearance, as long as the protocol is updated to allow for a more granular transactable units. Furthermore, the control of loss is fully in the hands of the holder of private key, he can make it as likely or unlikely as he wishes. As time progresses, methods of preserving the private key in an user friendly manner are expected to mature. The distinction between fundamentals of preservation of Bitcoin keys and the implementation thereof is explained by mndrix (2011):

> "One of gold's major strengths is that it has stood the test of time. Through thousands of years, it has shown itself a resilient store of value and a useful currency. Bitcoin has less than three years under its belt. If Bitcoin were gold, we'd still be in the early stone age carrying gold flecks in a leather pouch."

Summary

The demand-side causes of the "store of value" depend on liquidity to a large extent. Bitcoin is more sensitive in this respect than commodity monies, and is rather similar to fiat money. On the supply side, Bitcoin has more common with commodity monies and its production rate relative to that of total supply is expected to fall below that of gold.[40]

3.3.3 Transaction costs in the narrower sense

Economists have recognised since before the existence of Bitcoin that a system like Bitcoin is possible, and mention transaction costs in relation with it. Krüger and Godschalk (1998), for example, realise that innovation could not only occur as a form of existing money, but in a form of of a separate numéraire:

> "Technological progress and innovation in payment systems lead to a significant decrease of transaction and information costs. Subject to this decrease, economising can even lead to a viability of alternative currency units."[41]

Tanaka (1996) argues that

[39] Indeed, this is the motivation for demurrage-based monetary systems such as those proposed by Gesell (1936).

[40] On the supply side, Bitcoin is "harder" than gold. I would like to thank John Barrdear for this point.

[41] Translated from: "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."

> "Digital cash will make transactions more efficient in several ways. First, digital cash will make transactions less expensive because the cost of transferring digital cash via the Internet is cheaper than through the conventional banking system."
>
> ...
>
> "Second, since the Internet recognizes no political borders, digital cash is also borderless. Thus, the cost of transfer within a state is almost equal to the cost of transfer across different states."
>
> ...
>
> "Third, digital cash payments potentially can be used by anyone with access to the Internet and an Internet-based bank. While credit card payments are limited to authorized stores, digital cash makes person-to-person payments possible."
>
> ...
>
> *"The consequence of these effects is an enlargement of new business opportunities and an expansion of economic activities on the Internet."* [emphasis added]

Technological aspects (Logistics)

On a theoretical level, Bitcoin presents a model with the minimum possible costs. Any system needs to at least allow the user to send and receive money. This can be either achieved by physically moving objects (which Bitcoin actually allows through ToK transactions) or through a clearing system (which Bitcoin allows through ToB transactions). Physically moving objects requires that the "money" is representable as movable object, and clearing requires that the payer can exert control over the clearing process. The model of Bitcoin is very close to the abstract representation of these two processes.

Storage

Bitcoin has two components: the keypairs and the blockchain. The keypairs are just numbers, and can be stored in any object capable in storing 64 bytes, even the brain. The blockchain is stored in a distributed manner, and their operators cover the costs of its maintenance through the Bitcoin mining process. Theoretically, this is the minimum possible requirement for such a system. Gold requires to be physically stored as gold, and fiat money only through cash. Even if we consider other forms of money, these are based on reserves, which need to be stored. So at best other forms of gold money or fiat money shift the burden of storage onto those that can perform it more cost-effectively, but they persist. From this perspective, Bitcoin is superiour to both gold and fiat money.

Transport

Bitcoin can be transported as a ToK transaction (physical move) or ToB (clearing system). Again, this is superiour to both gold and fiat money. While Bitcoin does not have the theoretically lowest possible duration of transfer (an average expected time for a verified transfer is 1 hour), this is not an inherent problem in a Bitcoin-like system. Lower times are, hypothetically, possible. Again, Bitcoin has an advantage over gold.

Fiat money might be able to reach such fast clearing times, but so far, there are no products with this feature.

Manipulation

The control over the payment process is done by the control over the private key. The owner can send his balance or any proportion of if with practically the same effort. Bitcoin is here superiour to gold and also fiat cash, as these cannot be easily divided on demand (it is possible to divide gold by cutting, but this process is relatively more complex and inaccurate). Electronic money substitutes might be able to match Bitcoin on the easiness of manipulation.

Authentication

The authentication of Bitcoin is performed by cryptography. Control over the private key authenticates the payer. From practical point of view, authentication is instantaneous and automated. Gold and cash require the verification of the physical properties of the money, which is time consuming and inaccurate. Money substitutes require the authentication of the holder of the substitute vis-a-vis the issuer. Hypothetically, this can be also implemented purely by asymmetric encryption, thus matching Bitcoin, but so far, such systems do not exist.

Transaction fees

As the production of new Bitcoins progresses, it will decrease over time, until all the income of the miners would only consist of transaction fees that they collect. This will mean that the system will be in equilibrium state: the transaction fees would be at the level of marginal cost of maintaining the transaction network. On a theoretical level, this is the minimal level possible.[42] Gold or fiat money, in addition to covering the maintenance of the clearing system, also need to offset the costs of storage, authentication, manipulation and transport through the transaction fees.[43] This means that Bitcoin has an advantage over these systems on transaction fees.

Transaction costs of property rights

As explained before, the holder of the private key has exclusive control over the balance. From the point of view of the holder, this is hypothetically the best possible result. Even if someone argues that certain types of transactions should be forbidden (e.g. drug trafficking), or enforced (e.g. payment of taxes), this argument is not relevant in this context. People do not choose a medium of exchange based on what they think that others should or shouldn't be permitted to do. They choose it based on their own preferences, not on preferences they would like to see in others. All other things being equal, they would not voluntarily and knowingly choose a medium of exchange that would prevent

[42] There are minor issues about the distribution of costs among the components of the Bitcoin network in such an equilibrium state, as pointed out by Babaioff et al. (2012). However, this is an implementation issue and not inherent in all possible Bitcoin-like systems.

[43] Other systems are hypothetically possible. For example, the clearing network can sell the clearing data for data mining purposes (e.g. marketing). Whether this is sufficient to offset the other costs of the clearing network is outside of the scope of this thesis.

themselves from using it according to their own preferences, whatever those preferences may be.

Resistance to expropriation

Since the private key is form-invariant, it can be stored in almost any way imaginable, making it difficult to find the key, or even locate its owner. Bitcoin is pseudonymous, which means that the identity of a holder of a private key is not in a direct relationship with the key.[44] Scripting functionality in the Bitcoin network allows even proactive and adaptive defences. For example, a kidnapping for ransom could trigger evasive actions and make the balance inaccessible. Of course, that does not prevent the kidnapping, only prevents the kidnappers from looting. Such features are not available either for gold or fiat money.

In fact, as per Executive Order 6102,[45] the possession of gold was not permitted in the USA between 1933 and 1964. While it is certainly possible to forbid the use of Bitcoin, it is doubtful how large an effect it would have. First of all, the Executive Order 6102 depended on the existence of gold substitutes (paper money and deposit accounts). An execution of a similar act would therefore require the existence of Bitcoin substitutes. Furthermore, there are logistical obstacles to performing such an action. Krüger (2001) argues:

> "Technically, it is conceivable that banks (or even non-banks) that are based in offshore centres can issue e-money and distribute it via the Internet all over the world. For national governments, there seems to be *no practical way to prevent* its citizens to *use such e-money balances for payments*." [emphasis added]

In addition to the use of Internet, Bitcoin is decentralised and even more virtual than the system described by Krüger, making it even more difficult to enforce such a ban. Other authors have a different opinion, for example Dellingshausen (2011) argues:

> "An intrusion of the state can devalue a collection of Bitcoins as a monetary reserve with little forewarning."[46]

Similarly, Pattison (2011) argues:

> "Even if it could survive, precedent suggests that Bitcoin would not be allowed to survive unregulated if at all, which would ultimately destroy the subjective value of the commodity."

However, they entirely ignore the logistical difficulties of implementing such measures. They simply assume that once regulation is decided, it will automatically work.

[44] Bitcoin is not completely anonymous, but depending on its practical use, it can be made more anonymous, or more exposed. Reid and Harrigan (2011) attempt vector analysis of Bitcoin data, while Hamacher and Katzenbeisser (2011) argue that data mining can reveal information like pricing strategies. On the other hand, anonymisers (e.g. the aforementioned Bitcoin Fog or TorWallet) are available, and proposals for protocol changes, such as the one by Ladd (2012), to increase anonymity have been made.

[45] This can be viewed at http://en.wikipedia.org/wiki/Executive_Order_6102

[46] Translated from: "Eine Ansammlung von Bitcoins als monetäre Reserve könnte von einem auf den anderen Tag durch den staatlichen Eingriff entwertet werden."

Counter-party risk

All money substitutes are subject to counter-party risk. Fiat money is subject to a special type of counter-party risk, the central bank policy. Only physical gold is immune to this. Selgin (1997) argues that hypothetically a central bank policy can abstain from reliance on the human factors:

> "Getting nominal income to grow at some predetermined rate then becomes a relatively simple matter of having the central bank expand the stock of base money by that rate. As monetarists will be especially quick to see, enforcing this kind of central bank rule does not take a Board of Governors, a Chancellor of the Exchequer, or a caucus of economists. A computer will do, provided it is fed the necessary information regarding changes (or predicted changes) in factor supply. This adds to the beauty of the reform, because a computer, unlike a person or committee, will not change its mind, or go back on its word."

However, this is unlikely for political reasons (public choice theory), i.e. the broader context. Central bank has a special legal privilege, and is thus subject to pressure. Putting a computer in charge of the central bank does not eliminate this pressure.

Bitcoin has an advantage over gold-based money substitutes and fiat money.

Regulatory transaction costs

Barriers to entry

The banking system is regulated, and so are other financial services. This creates barriers to entry. For example, according to The Publications Office of the European Union (2000), e-money issuers in the EU, need to have a capital of at least one million euro.[47] This creates obstacles for competition to Bitcoin. As reported by GoWest (2011), GoldMoney, for example, a system providing precious metal warehousing (i.e. 100% deposit banking), had to discontinue the ability to provide transactions among its users for regulatory reasons and only allows such feature for residents of Jersey, which is a small fraction of the world population. Bitcoin, on the other hand, can be used for transactions by residents of any country. Competition to Bitcoin, whether existing or potential, therefore has it more difficult to compete.

Price fixing

Through Gresham's Law, price fixing can cause a replacement of one money by other. This works among similar systems (for example gold vs. silver) as well as between money substitutes and fiat money (e.g. replacing of gold-backed bank notes through unbacked fiat money). However, historical data suggests that this happened when the systems were technologically similar (for example, a gold coin is technologically similar to a silver coin, and an gold-backed paper note is similar to an unbacked fiat paper note). To what extent this works across a technological gap is unclear. It may be possible that it does not work in such a case, so Bitcoin has a potential advantage here too.

Capital controls

Matonis (2012a) argues that Bitcoin is particularly well suited to avoid capital controls:

[47] Bitcoin does not fall into this particular regulation, as there is no financial contract between the issuer and the holder.

> "Bitcoin is not about making rapid global transactions with little or no fee. Bitcoin is about preventing monetary tyranny. That is its raison d'être. Monetary tyranny can take many ugly forms. It can be deliberate inflation, persecutory capital controls, prearranged defaults within the banking cartel, or even worse, blatant sovereign confiscation. Sadly, those threats are a potential in almost any jurisdiction in the world today."

While the extent to which Bitcoin can actually avoid this is unclear, all that is needed is that it has a sufficient comparative advantage in this area.

Summary of transaction costs of Bitcoin (in the narrower sense)

Across the whole spectrum of transaction costs in the narrower sense, Bitcoin is at least comparable to other systems, and in many areas presents a significant improvement over alternative systems, whether they are based on gold or fiat money.

3.3.4 Summary of Bitcoin competing with other currencies and payment systems

On the supply side, the function of store of value is solid, however the demand side highly conditions depend on the rest of the factors (liquidity and transaction costs in the narrower sense). Liquidity of Bitcoin is at the moment lower than that of money, however as long as Bitcoin has a significant advantage over the alternatives on transaction costs in the narrower sense, this is expected to have a positive impact on liquidity as well. It is therefore possible that, as time progresses, Bitcoin will out-compete both fiat money and gold as a medium of exchange, and become money. However, this presumes that liquidity of Bitcoin will evolve positively, as its function of store of value is highly dependant on the acceptance of Bitcoin (liquidity). Without sufficient liquidity, Bitcoin will face significant obstacles to evolving into more mature stages of media of exchange and into "money".

3.4 If Bitcoin fails, what would replace it?

Since there is an omnipresent attempt to reduce transaction costs of exchange, if people stop using one medium of exchange, it must be because they switched to another medium of exchange. If therefore someone argues that Bitcoin would cease to be a medium of exchange, one also must also answer the question "what would replace it?". This process would need to follow the same rules as other situations where one medium of exchange replace another, in other words, provide a comparative advantage over Bitcoin sufficient enough to motivate people to switch. Either it would need to undercut Bitcoin on transaction costs, or it would have to out-compete its liquidity.

Since Bitcoin is, so far, unchallenged in its transaction costs (in the narrower sense), it is unlikely that it will be replaced by fiat money or gold. However, circumstances could change and, for example, a new currency with even lower transaction costs could appear. It also logically follows that this would not be either a new fiat currency or a new physical commodity. It would be another abstract medium of exchange. Alternatively, occurrences disadvantageous to Bitcoin could increase its transaction costs, or raise the required critical mass required for it to be self-sustaining. This could be, for example, an effectively enforced ban on the use of Bitcoin, or a particular failure of the software

Table 3.2: Possible reasons for the collapse of Bitcoin and what would replace it

	Cryptocurrency	Fiat money or gold
Transaction costs (in the narrower sense)	Significant improvement over Bitcoin, or technological failure of Bitcoin	Deregulation
Liquidity (critical mass of network effect)	Leverage of a big market actor	Regulation

comprising the Bitcoin network. There could also be a new virtual currency that does not have a significant technological advantage over Bitcoin, but is supported by multiple large companies or governments. For example, PayPal could, hypothetically, launch a new cryptocurrency and use its leverage over the market on online payments to out-compete Bitcoin on liquidity.[48]

Increased regulation of payment processing could decrease the liquidity of Bitcoin too far to be sustainable (for example by making it too difficult for Bitcoin exchanges to operate). On the other hand, if this increased regulation affects other payment systems too, this could turn out to provide native Bitcoin transactions and informal exchanges a comparative advantage over other payment systems, as Bitcoin is more resistant to the effects of regulation. Alternatively, deregulation would allow existing media of exchange to undercut Bitcoin on transaction costs in areas where it now has a comparative advantage, and again lead to unsustainability. So an attempt to control the acceptance of Bitcoin is a double-edged sword: it can shift the acceptance either way. A summary of the possible ways Bitcoin can end is presented in Table 3.2 on page 38.

3.5 Mises' regression theorem

3.5.1 Introduction

The purpose of the regression theorem is to explain how money (or media of exchange in general), achieve prices. A short version of the regression theorem is presented by Mises (1912):

> "Before an economic good begins to function as money it must already possess exchange-value based on some other cause than its monetary function."

The point Mises is making is that the origins of money are a market phenomenon:

> "This provides both a refutation of those theories which derive the origin of money from a general agreement to impute fictitious value to things intrinsically valueless and a confirmation of Menger's hypothesis concerning the origin of the use of money."

The common interpretation of this has so far been that money must originate as a highly marketable (liquid) commodity. Thus, a very common Austrian critique of Bitcoin is that it does not adhere to the regression theorem. Pattison (2011), for example, writes:

[48] However, Goldman (2012) reports that Google wanted to create something similar to Bitcoin, but decided against it for regulatory reasons. Google is a larger company than PayPal, so such a possible alternative to Bitcoin appears to be unlikely.

> "When these characteristics are analyzed against Austrian monetary theory, Bitcoin does not hold up as a legitimate money, as many in the popular literature have suggested, because it did not begin as a commodity money and therefore has no intrinsic value and violates Mises' Regression Theorem."

What is important to realise is that the regression theorem does not say that media of exchange that do not adhere to it are unsustainable. It says that media of exchange that do not adhere to it are impossible and cannot exist. Mises (1999) writes:

> "... no good can be employed for the function of a medium of exchange which at very beginning of its use for this purpose did not have exchange value on account of other employments. *And all these statements implied in the regression theorem are enounced apodictically as implied in the apriorism of praxeology.* It must happen this way. Nobody can ever succeed in constructing a hypothetical case in which things were to occur in a different way."[49] [emphasis added]

Economists that claim that Bitcoin violates the regression theorem cannot argue that this means it is unsustainable, as, for example does Pattison (2011):

> "While Bitcoin exhibits some of the qualities of money, it is not money in the Austrian sense and *therefore is not sustainable.*" [emphasis added]

On the other hand, Murphy (2012) admits that the Mises' Regression Theorem applies to media of exchange in general, not only to money. So if Bitcoin is a medium of exchange, then either the regression theorem is outright wrong, or is misunderstood and Bitcoin adheres to it. Murphy dismisses the claims that "Regression Theorem refutes Bitcoin" outright. So even if the regression theorem is used as a method to oppose Bitcoin, the methodologically correct argument would have to be that Bitcoin is not a medium of exchange.[50]

If we ignore the term "commodity" and instead concentrate on the rest of the interpretation, we can see the theorem as requiring that a medium of exchange must already have a price, and must already be accepted on the market (be liquid). It must already have both, otherwise it cannot act as a medium of exchange. And since both price and liquidity are market phenomena, there already must be a certain level of demand for the prospective medium of exchange before it can act as a medium of exchange, i.e. a non-monetary demand.

3.5.2 Self sustainability of media of exchange without non-monetary demand

While a non-monetary demand is seen by Mises (1912) as a necessary requirement for the emergence of price and liquidity, it is not seen as an obstacle for its persistence:

> "In the case of money, subjective use-value and subjective exchange value coincide. Both are derived from objective exchange value, for *money has no utility other than that arising from the possibility of obtaining other economic goods in exchange for it.*" [emphasis added]

Similarly, Rothbard (2004) writes:

[49] I would like to thank David Gordon for this quote.

[50] While it sounds absurd to me, there indeed is one vocal opponent of Bitcoin, Smiling Dave (2012), who even in October 2012 proclaims that "... bitcoin has never been used as a medium of exchange, not even once...".

> "On the other hand, it does not follow from this analysis that if an extant money were to lose its direct uses, it could no longer be used as money. Thus, if gold, after being established as money, were suddenly to lose its value in ornaments or industrial uses, it would not necessarily lose its character as a money. Once a medium of exchange has been established as a money, money prices continue to be set. If on day X gold loses its direct uses, there will still be previously existing money prices that had been established on day X – 1, and these prices form the basis for the marginal utility of gold on day X. Similarly, the money prices thereby determined on day X form the basis for the marginal utility of money on day X + 1. From X on, gold could be demanded for its exchange value alone, and not at all for its direct use. *Therefore, while it is absolutely necessary that a money originate as a commodity with direct uses, it is not absolutely necessary that the direct uses continue after the money has been established.*" [emphasis added]

In other words, once a good is money, it does not need non-monetary uses to be usable as money. Nevertheless, even though both Mises and Rothbard use the term "money", their arguments do not actually require a most common medium of exchange. In particular Rothbard's argument appears to be applicable to any medium of exchange. As long as it has a price, and liquidity, the argument of Rothbard holds. However, this needs to be evaluated cautiously. Rothbard does not argue about sustainability, merely of the logical requirements for existence. Rothbard's argument does not mean that all media of exchange are automatically sustainable.

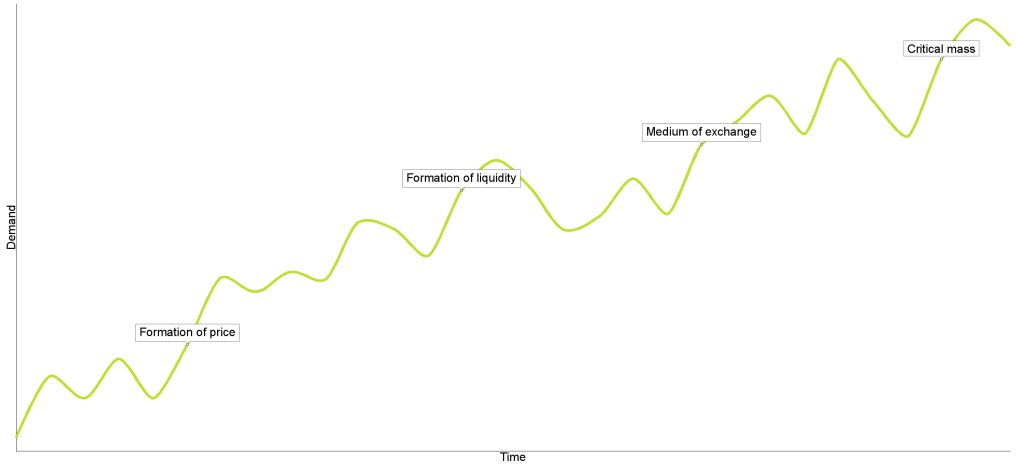
This leaves the question open, what is the necessary level of liquidity for a medium of exchange to be sustainable even if it does not have non-monetary uses? If we view liquidity as the network effect, the term for such a threshold is called "critical mass". If the competing media of exchange are fundamentally similar and only differ in liquidity, liquidity would take preference (as explained in Section 3.3). In such a case, a medium of exchange would survive only if it was the most liquid one (i.e. money). If other factors (transaction costs in the narrower sense) are considered however, this can shift the comparative advantages around.

3.5.3 Summary and reformulation of the regression theorem

Based on the previous paragraphs, I present here my own formulation of the regression theorem. I formulate it chronologically backwards, to match the way Mises (1912) argued. I also amend it for the sustainability analysis (which is highly relevant for Bitcoin).

1. Once a medium of exchange is sufficiently liquid, it can, hypothetically, sustain itself through the network effect even if it does not have non-monetary uses, as liquidity creates demand
2. Before a medium of exchange is a medium of exchange, it must be liquid
3. Before it is liquid, it must have a price
4. Both of these are fundamentally market phenomena, i.e. both price and liquidity must be established as a catallactic process

Figure 3.3: Mises' Regression Theorem (own re-interpretation)



Commodity money adheres to the regression theorem, as the initial price and liquidity are determined by its non-monetary uses. Fiat money adheres to the regression theorem, because it begins as a money substitute: its price is determined by the pre-existing money, and its liquidity is achieved through Gresham's Law. A visual representation of the theorem is presented in Figure 3.3 on page 41.

Once again I would like to reiterate that according to the Austrian School, a medium of exchange not adhering to the regression theorem isn't unsustainable, rather it cannot exist.

3.6 The origin of the price of Bitcoin (application of the regression theorem)

3.6.1 Supply side

The first available records for trades occurring with Bitcoin are provided by NewLibertyStandard (2009). The record shows that on October 5th 2009, one USD was priced at 1,309.03 bitcoins.[51] It appears that NewLibertyStandard was a producer of Bitcoins, and was selling them. (S)He writes:

> "During 2009 my exchange rate was calculated by dividing $1.00 by the average amount of electricity required to run a computer with high CPU for a year, 1331.5 kWh, multiplied by the the average residential cost of electricity in the United States for the previous year, $0.1136, divided by 12 months divided by the number of bitcoins generated by my computer over the past 30 days."

In other words, NewLibertyStandard used the (variable) costs of production as a basis for the price (s)he was asking for the bitcoins (s)he produced.

[51] At that time, there were 1,220,900 bitcoins in existence, which results in the total value of all Bitcoins in existence (market capitalisation) of 932.68 USD. Currently (June 19th 2012) the price for one bitcoin is 6.47 USD. With 9,268,400 bitcoins in existence, that creates a market capitalisation of 59,966,548 USD, i.e. approximately 60 million.

3.6.2 Demand side

As explained in the previous section, in order to adhere to the regression theorem, there must have existed demand for Bitcoin prior to its use as a medium of exchange.

Murphy (2012) argues that ideological (e.g. libertarian, anti-fiat-money, anti-fractional-reserve-banking) bias of Bitcoin's proponents, and speculation could have created the initial demand.[52] Similarly, Matonis (2011) argues that opposition to fiat money and/or current banking system and the economic depression as the most important reason for the rise of Bitcoin. jahabdank (2011) argues that transaction costs are the reason why Bitcoin has utility and this also could have affected initial demand.

3.6.3 Emergence of market price

As shown above, the two components of markets, supply and demand of Bitcoin, existed even before Bitcoin was a medium of exchange. Even though it was not a-priori clear that Bitcoin would actually be able to provide satisfaction of the demand in the future, the buyers probably came to the conclusion that the chance is higher than zero, and that compared to the sellers, the buyers cannot produce Bitcoins cheaper and/or in the quantities they desired. According to my opinion, the rational expectations of the potential utility of Bitcoin for the potential buyers exceeded the price demanded by the producers, and trade emerged.

Since there was more than one producer, there was already a competition on the supply side, which means that a price significantly above the production costs would have been undercut. The initial price therefore already conforms to the concept of supply and demand. Since the initial prices and the total trade volume were minuscule, this did not place a high burden on any of the market participants, so they could have treated it as a hobby, and it was not necessary that they aim for profit in the narrower sense, so a high level or risk of loss was acceptable for them.

3.6.4 Emergence of liquidity

Already at this very early stage, Bitcoin was a system with very low transaction costs, and unlike anything that has existed before. A part of the demand was already met by it, i.e. a part of the expectations was fulfilled. The total demand appears to have been increasing until a more liquid stage was reached. A possible time for such an threshold could be the emergence of bid and ask order books (aforementioned Menger's organised markets). The first historical record of a Bitcoin exchange (which would have an order book) I could locate, Unknown (2012), shows Bitcoin Market[53], opened on February 6$^{\text{th}}$ 2010.

With respect to the foundation of the regression theorem (the emergence of price and liquidity as a necessary precondition for an existence of a medium of exchange), the usual interpretation of the theorem (that it refers to a process that takes place over thousands of years) appears to be an exaggeration. It might be so in some cases, but as Bitcoin presents a significant technological innovation that did not have competition at that time, the process could have been much quicker. Since Bitcoin was launched on January 3$^{\text{rd}}$

[52] Menger (1892) already mentioned speculation as one of the factors determining a demand for a commodity

[53] In the meantime, Bitcoin Market ceased operations.

2009, it means the process to reach liquidity took about 13 months (10 months for the emergence of the price).

3.6.5 Critical mass

In order for Bitcoin to show that it crossed the critical mass, its level of liquidity would have to satisfy the full demand for Bitcoin. In other words, if the users of Bitcoin abandoned their libertarian biases and speculation for the future price of Bitcoin, would the liquidity be sufficient to serve as a medium of exchange? As I argued in Section 3.4, a failure of Bitcoin must mean that something would replace it. In other words, to answer this question, the status of the competition of Bitcoin is at least as important (if not more), than the status of Bitcoin itself.

With respect to Bitcoin then, as long as it continues to provide comparative advantage in transaction costs over other currencies to the extent that it outweighs their advantage in liquidity, it will sustain itself.

Based on the existence and status of the broader Bitcoin ecosystem I lean towards a cautions yes.

3.7 Austrian Business Cycle Theory, fractional reserve banking, money supply and Bitcoin

The Austrian Business Cycle Theory, "ABCT" was originally developed by Mises (1912) and subsequently treated by other Austrians, for example Rothbard (2004) or de Soto (2009). A simplified interpretation is that the expansion of credit through fractional reserve banking increases the money supply in a way that creates a particular type of price structure disequilibrium. This affects economic calculation, and investments that do not have a real-value profitability would appear to have nominal-value profitability. This causes a misallocation of investment (capital goods), even though nominally, it appears that the economy is booming. Once the disequilibrium effect wears off (as maintaining it requires an exponentially progressing credit expansion), a reallocation of capital goods towards the equilibrium occurs, accompanied by a credit contraction. This is the bust phase. Low interest policies of central banks exacerbate the boom and prolong the bust.

What is interesting is that unlike mainstream economists, who view the boom phase as positive and the bust phase as negative, the Austrians view the boom phase as disequilibrating, while the bust phase as equilibrating. While the mainstream economists argue for the prevention of the bust, the Austrians view the bust as a necessary consequence of the boom, and argue for the prevention of the boom. The tool to prevent the boom is an inelastic money supply. Since the cause of the credit expansion is fractional reserve banking (often abbreviated as "FRB"), the Austrians argue for a suppression of (or at least the absence of support for) fractional reserve banking.

3.7.1 Money supply

Mainstream economists are flexible in the definition of the money supply, Krugman (2010), for example, argues that

> "The truth is that these days — with credit cards, electronic money, repo, and more all serving the purpose of medium of exchange — it's not clear that any single number deserves to be called "the" money supply."

Due to this, Krugman sees the attempts of the Austrians at preventing a (credit) expansion of the money supply as moot. However, the Austrians have a much stricter definition of the money supply. It consists only of money in the narrower sense and money substitutes (minus bank reserves). Financial instruments that are not money substitutes are not a part of the money supply. Salerno (2010) explains:

> "Of primary import, a point that can not be overemphasized, is the requirement that for a thing to be money *it must serve as the final means of payment in all transactions*. In other words, it must be the thing that fully extinguishes the debt incurred in a transaction." [emphasis added]

Rothbard (2011) explains that acceptance in exchange can affect whether a financial instrument is or is not a part of the money supply:

> "And so long as demand deposits are accepted as equivalent to standard money, they will function as part of the money supply. It is important to recognize that *demand deposits are not automatically part of the money supply* by virtue of their very existence; they continue as equivalent to money *only so long as* the subjective estimates of the sellers of goods on the market think that they are so *equivalent* and *accept them as such in exchange*." [emphasis added]

Unfortunately, Rothbard then continues and counts even instruments which are redeemable on demand (zero maturity), but not used as a medium of exchange, as a part of the money supply, for example savings deposits, creating confusion in the Austrian position. Fortunately, Salerno (2010) clarifies the Austrian approach with respect to zero-maturity instruments that are not a medium of exchange:

> "The *essential, economic point* is that some or all of the dollars accumulated in, e.g., passbook savings accounts are effectively withdrawable on demand by depositors in the form of cash. In addition, *savings deposits are at all times transferrable, dollar for dollar, into "transactions" accounts* such as demand deposits or NOW accounts." [emphasis added]

In other words, even though at the precise moment of their existence, savings deposits are not usable as a medium of exchange, they can be at practically any time used to create one, i.e. to increase the money supply. A withdrawal from a savings account either decreases the bank's reserves, thereby increasing the amount of cash in circulation, or it increases the balance on a current account, thereby increasing the amount of transferable bank balances (which are a money substitute). However, one aspect that is missing from Salerno's analysis is that this only works if there already are other money substitutes. If there are no money substitutes, a withdrawal from the savings deposit cannot increase the amount of money supply beyond the reserves of the bank. In other words, zero-maturity instruments that are not money substitutes themselves can only increase the money supply beyond the amount of reserves of the issuer if there is a different instrument that acts as a money substitute.

Therefore, in the Austrian perspective, credit expansion requires money substitutes. Mises (1999) affirms this claim (although with a different terminology, but the essence of his argument is identical to mine):

> "The term credit expansion has often been misinterpreted. It is important to realize that commodity credit cannot be expanded. The only vehicle of credit expansion is circulation credit."

3.7.2 Emergence of money substitutes

The emergence of money substitutes is guided by the same rules as other choices of media of exchange. They need to provide a significant comparative advantage over monetary base in order to be accepted as an "improved version", and out-compete it to a significant degree. Since money substitutes require that money in the narrower sense already exists, they cannot out-compete it on either liquidity or the store of value function. They must out-compete it on transaction costs in the narrower sense. This is a very important point, therefore I provide a larger number of references to demonstrate that my argument is consistent with the Austrian School:

Schlichter (2011) explains:

> "Carrying heavy gold or silver coins around is *cumbersome*. It is *therefore* fair to assume that a natural demand for *deposit and safekeeping services* arose and that goldsmiths were natural providers of these services." [emphasis added]

de Soto (2009) writes:

> "Clients made deposits for reasons of safety and expected bankers to provide *custody and safekeeping*, along with the additional benefits of *easily-documented cashier services and payments to third parties*." [emphasis added]
>
> ...
>
> "All of these sources show how frequently individuals used the bank for making deposits as well as payments. In addition, due to their highly-developed accounting system, *paying debts through banks became extremely convenient*, as there was an official record of transactions—an important piece of evidence in case of litigation." [emphasis added]

Hoppe (1994) writes:

> "On the other hand, to *economize on the cost of storing* (safekeeping) *and transacting* (clearing) money, in a development similar to that of transferable property titles - including stock and bond certificates - as means of facilitating the spatial and temporal exchange of non-money goods, side by side with money proper also gold certificates - property titles (claims) to specified amounts of gold deposited at specified institutions (banks) - served as a medium of exchange." [emphasis added]

White (1984) writes:

> "Money users find each form of redeemable claim to bank specie *more economical to use* for many purposes *than actual specie*."

While Salerno (2010) does not explicitly mention the causal relationship between transaction costs and the emergence of money substitutes, he recognises that they coincide:

> "With the use of clearing systems, money substitutes are virtually costless to transfer."

If, therefore, financial instruments and other goods cannot out-compete the monetary base on the narrower sense, they cannot evolve into money substitutes, and the money supply will be equal to the monetary base. In order to reach a particular goal with respect to the money supply, this can be achieved not only by regulating the interface between the monetary base and money substitutes, but can also be achieved by eliminating one of them altogether. Yeager (2001) realises this when he writes:

> "The very existence of base money distinct from other kinds of money poses problems."

Since Yeager does not subscribe to the gold standard branch of the Austrian School, from his perspective, the elimination of the monetary base is the preferred course of action. For the gold standard branch though, the elimination of money substitutes is preferred.

3.7.3 Money supply of Bitcoin

Bitcoin already has very low transaction costs (in the narrower sense). I explained earlier how difficult other system have it to compete with Bitcoin on transaction costs. The likelihood that "Bitcoin-substitutes" emerge is very low. Even though such as system hasn't existed prior to Bitcoin, it could be argued that White (1984) realised that it is hypothetically possible, i.e. predicted this feature of Bitcoin:

> "Coinage reduces transaction costs compared to simple exchange, because of authentication and weighing. Bank liabilities also reduce transaction costs. *But these are empirical factors, and not something inherent in all possible monetary systems.*" [emphasis added]

The economists analysing Bitcoin realise this. Bednár and Karpiš (2011) argue that Bitcoin already provides features that normally require substitutes, which means there is less demand for such substitutes. Schlichter (2012a) comes to the same conclusion:

> "FRB is particularly unlikely to develop in a Bitcoin economy, as there is no need for a depository, for safe-keeping and storage services, and for any services that involve the transfer of the monetary system's raw material (be it gold or state paper tickets) into other, more convenient forms of media of exchange, such as electronic money that can facilitate transactions over great distances. The owner of Bitcoin has an account that is similar to his email account. He manages it himself and he stores his Bitcoin himself. And Bitcoin is money that is already readily usable for any transaction, anywhere in the world, simply via the internet. The bank as intermediary is being bypassed. The Bitcoin user takes direct control of his money. He can access his Bitcoins everywhere, simply via the SIM card in his smartphone."

In addition to that, a substitute introduces new risks that negatively impact transaction costs. Various (2012) writes about the emergence of counter-party risk associated with redeemable codes (which are an example of Bitcoin-denominated financial instruments):

> "Essentially, a redeemable code obtained not directly from the issuer but instead from an intermediary *should be considered as something having no value until it is successfully redeemed.*"

and regulatory risk:

> "Unlike how the Bitcoin digital currency employs a decentralized architecture, the Bitcoin exchanges are entities that can essentially be shut down with a single phone call."

Gothill (2011), however, argues that service providers could provide services that Bitcoin itself doesn't and therefore cause a Bitcoin substitute to emerge. He lists the following possibilities: enhanced security, faster transactions, and interest payments. On the other hand, as I argued earlier, Bitcoin is form-invariant and can be used in almost any way. Even if these features might not be available natively in Bitcoin now, they could become available in the future. Indeed, already multi-key signatures allow for enhanced security. Faster transactions are already provided by green addresses[54], and an potential alternative ZipConf[55] claimed to use the properties of the Bitcoin protocol in such a way that it can ensure a faster clearing (seconds instead of minutes), for a fee. Last but not least, Bitcoinica, while it was still operating, provided interest payments on deposits without providing the ability to use them as a medium of exchange directly (Bitcoinica used a form of liquidity arbitrage to generate revenue).

A more complex topic is interventionism. There are at least two ways interventionism can create a demand for substitute media of exchange: fixed exchange rates (Gresham's Law, i.e. "bad money drives out good if their exchange rate is set by law"), or, as argued by Suede (2012), directly seizing control of the banks and confiscating the reserves. Unless Bitcoin is either legal tender or the dominant medium of exchange, it is unclear how much effect Gresham's Law would have. Furthermore, if the technological transaction costs of Bitcoin remain significantly lower, it is also debatable if interventionism can lead to emergence of Bitcoin substitutes out of Bitcoin-denominated financial instruments. This also assumes that the intervention can be effectively enforced.

Altogether, the evolution of Bitcoin-denominated financial instruments into Bitcoin-substitutes appears to be unlikely. Technological progress can also, hypothetically, reduce the transaction costs of future versions of Bitcoin to such an extent that this becomes entirely impossible. Bitcoin, therefore, if it evolves into money, would most likely feature an inelastic supply.

3.7.4 Alternative methods for avoidance of credit expansion

So far, the Austrian solution for preventing credit expansion has been the prohibition of fractional reserve banking. However, this would face significant practical and legislative obstacles. The attempt to implement a ban on the fractional reserve banking is bound to cause problems in its implementation. First of all, in order for the ban to work, it needs

[54] Green addresses work by using a reputable middleman for transaction. The middleman is a known person and promises not to perform double-spends. This reduces the time for the transaction to be considered "safe". An analogy would be a prepaid card, i.e. the user would need to pay the middleman in advance of making actual payments. However, it is implemented natively with Bitcoin protocol.

[55] ZipConf publicity and the corresponding website, http://www.zipconf.com, appears to have vanished before it was officially launched, so it never actually provided services. However, on theoretical level, the properties of such a service sound plausible. See Buterin (2012c).

to be implemented worldwide. If not, people can use instruments issued by fractional reserve banks in a different country. Anything less than a worldwide ban on fractional reserve banking would fail to achieve the goal. Yeager (2001) appears to agree:

> "Efforts to monitor and stamp out all institutions and practices that would have the effect of fractional-reserve transactions accounts, including efforts to keep the law abreast of innovations, would require a hyperactive and practically totalitarian state and would probably prove futile after all."

Another problem is that whether a financial instrument is, or is not, a money substitute, is ultimately determined by the payee, not the payer or the issuer. Attempts to place restrictions on the issuer for the actions of a payee (in particular when the issuance comes chronologically before the payment, and therefore the payee cannot cause the issuance) contradict the libertarian theory of justice (see Kinsella and Tinsley (2004)). This is further exacerbated with money substitutes that do not have any reserves at all (i.e. are not based on the concept of demand deposits).

A second issue was mentioned by Suede (2011b):

> "Another problem with paper representing gold is that paper is easily destroyed while gold is not. This represents an accounting problem for banks issuing the paper. *If paper is destroyed, the gold that is represented by that paper still exists, but now that gold is in a state of limbo.* There is simply no way for the bank to know with any certainty that the paper was really destroyed. Every bill that is lost puts the gold behind that bill permanently out of circulation (assuming the bank abides by standard accounting rules). In a large banking system, this dilemma represents a real problem." [emphasis added]

Even a fully voluntary solution, as proposed by Mises (1912) (and repeated by Hoppe et al. (1998)) of an increased use of gold coins as a method to counter the pressure to increase the money supply:

> "Gold must be in the cash holdings of everyone. Everybody must see gold coins changing hands, must be used to having gold coins in his pockets, to receiving gold coins when he cashes his paycheck, and to spending gold coins when he buys in a store."

would not work, as long as money substitutes decreased transaction costs of gold. And indeed, this is inevitable. Selgin (1988) realises that when he writes:

> "In a mature free banking system, commodity money does not circulate, its place being taken entirely by inside money."[56]

Similarly, Brito (2012) writes as well:

> "It's almost inevitable that digital money will soon replace not just the penny, but all physical money — in the U.S., Canada and elsewhere. Moving away from paper notes and coins and toward a digital currency is a no-brainer, at least when it comes to *cost and efficiency*." [emphasis added]

[56] Based on my debate with George Selgin on http://www.freebanking.org, it appears though that he thinks that this is due to the interest being paid on holding bank liabilities even in the absence of an improvement in transaction costs, but unfortunately it is not entirely clear from his response.

In other words, a prohibition of fractional reserve banking would *increase* the transaction costs of exchange. Therefore, market participants would not voluntarily choose it and ultimately it would fail. As a method for a prevention of the business cycle, Bitcoin is superiour to gold (and, obviously, fiat money, since fiat money is elastic in the first place).

3.8 Conclusion

As I have shown, transaction costs (in the broader sense) are the reason for the choice of a medium of exchange, and their reduction is the consequence of the choice. Normally, the determining factor of (broader) transaction costs is liquidity. However, a significant comparative advantage in (narrower) transaction costs can overcome this obstacle. This can result in a shift. The question of the ability of Bitcoin to store value is controversial. There are no fundamental obstacles, but sufficient liquidity presents a practical obstacle.

As a result of the comparative advantage in transaction costs, Bitcoin can be expected to be used in those markets where the improvement in transaction costs is significant, or markets which are highly sensitive to transaction costs. The activities of the regulatory and legislative bodies may affect this process, however they can be counterproductive (i.e. an increase in regulation can result in a shift towards, instead of away from, Bitcoin).

Bitcoin adheres to the Austrian theory of the catallactic origin of money. It is not (yet) money, merely a medium of exchange. However it already passed the thresholds that must praxeologically precede the function of medium of exchange: the emergence of price (which was originally based on production costs), and the emergence of liquidity (which was probably motivated by "rational expectations" and libertarian bias of its early adopters). Arguably, it also passed a third threshold, the critical mass of the network effect, where the demand for Bitcoin generated only through its liquidity is self-sustaining.

Due to its extremely low transaction costs, a monetary system based on Bitcoin is expected to have a money supply identical to the monetary base, i.e. inelastic. This is an important goal of the proponents of the Austrian Business Cycle Theory. Bitcoin provides a historically first opportunity to achieve a switch and a maintenance of an inelastic money supply without legal reform, and without having to address fractional reserve banking. In this respect, it is superiour to both gold and fiat money.

While some of the aspects of Bitcoin are unusual and unforeseen by the Austrians, in retrospect it is consistent with the fundamentals of the Austrian theory. Even though reveals imprecisions in some of the definitions used by the Austrian writers, there are several suggestions about how to "fix" these imprecisions.

Chapter 4

Empirical analysis of Bitcoin

4.1 Price and visibility

4.1.1 Price

The data for the price of Bitcoin was taken from the historical trade data on Mt.Gox exchange. Mt.Gox trade history is available in JSON[57] form to download from Mt.Gox website. The data is provided in chunks of 100 entries. A PHP[58] script was written to regularly download the new trade data and import it into a MySQL[59] database. The time frame is July 18$^{\text{th}}$ 2010 until November 18$^{\text{th}}$ 2012.

The results used in empirical analysis were calculated as weighted average (formula (4.1), where μ is the weighted average, w is the amount traded and x is the USD price per Bitcoin). Charts of the price are shown at Figure 4.1 on page 51 through Figure 4.3 on page 52.[60]

$$\mu = \frac{\sum wx}{\sum w} \tag{4.1}$$

4.1.2 Visibility

I use the term visibility (of Bitcoin) to denote the intensity of the interest of general public (in Bitcoin). The empirical data used for visibility was obtained through Google Trends[61]. Google Trends is a metric provided by Google denoting how many times people used the Google search engine to search for a particular term. In this case, the term was "bitcoin". Google provides the data with a weekly granularity (one data point per week), and is normalised so that the peak value is always 100. The output of Google Trends was downloaded as a CSV file and imported into a MySQL database. The time frame is since the launch of Bitcoin, January 3$^{\text{rd}}$ 2009 until November 4$^{\text{th}}$ 2012.

[57] JavaScript Object Notation, a standard for storing data objects.
[58] PHP is a scripting language.
[59] MySQL is a relational database system.
[60] Similar charts are available at http://www.bitcoincharts.com, see e.g. The Economist (2012).
[61] Google Trends is available at http://www.google.com/trends/

Figure 4.1: Price of Bitcoin (in USD), daily granularity

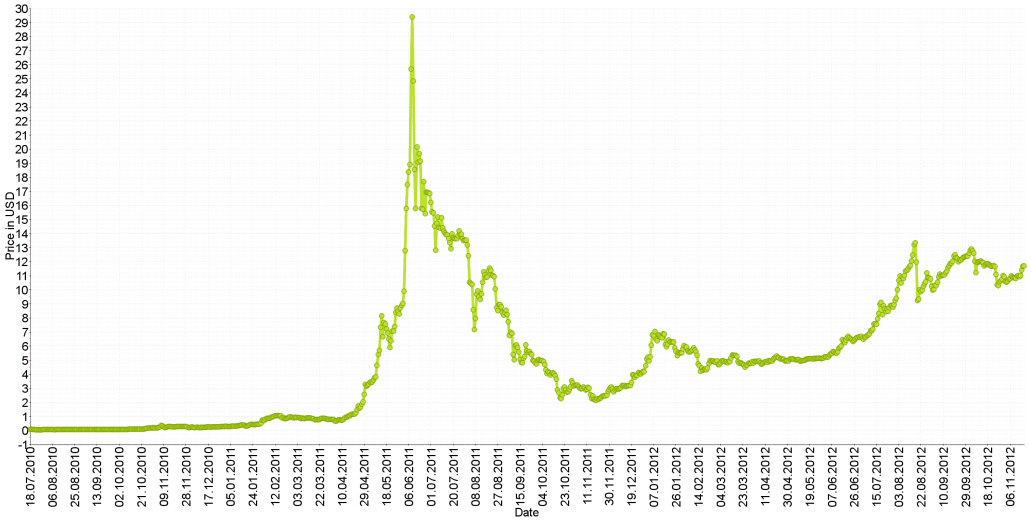


Figure 4.2: Price of Bitcoin (in USD), weekly granularity

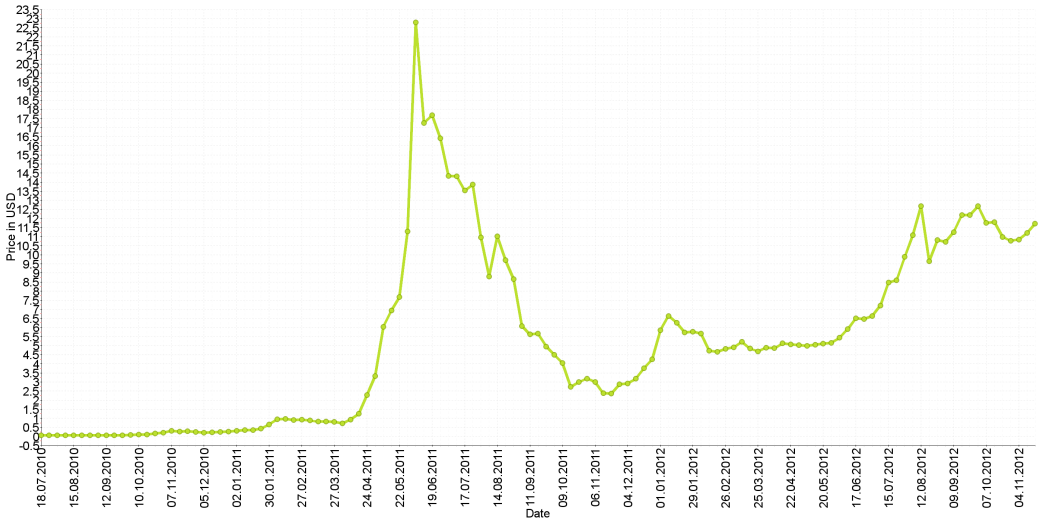


Figure 4.3: Price of Bitcoin (in USD), monthly granularity

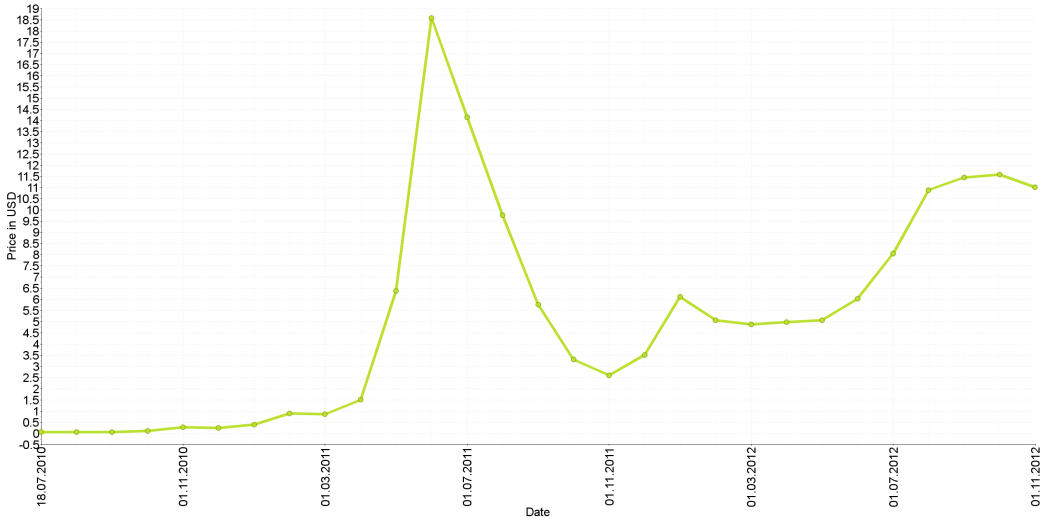


Table 4.1: Correlation coefficient between price and visibility

granularity	correlation coefficient
day	0.77
week	0.81
month	0.85

4.1.3 Correlation between price and visibility

The formula used for calculation of correlations (both in this section as well as in Section 4.2.4) is the Pearson product-moment correlation coefficient, as seen in formula (4.2), where $r_{x,y}$ is the correlation coefficient, n the number of elements in the sample, x_i the i-th element of the variable x and y_i the i-th element of the variable y.

$$r_{x,y} = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}} \tag{4.2}$$

The scope variable, granularity, has three possible values, three correlation coefficients were calculated. The result is presented in Table 4.1 on page 52. In addition to calculating correlations, scatter plot diagrams including a best-fit line are presented.

Interpretation

The correlation of price in USD with visibility (measured in terms of number of Bitcoin searches in Google) increases as granularity decreases. This indicates that short-term fluctuations in Bitcoin price and/or visibility are influenced by other factors. It should also be noted that data for visibility is not actually available with daily granularity, therefore daily granularity correlation calculation is less accurate.

Figure 4.4: Scatter plot diagram of price and visibility, daily granularity

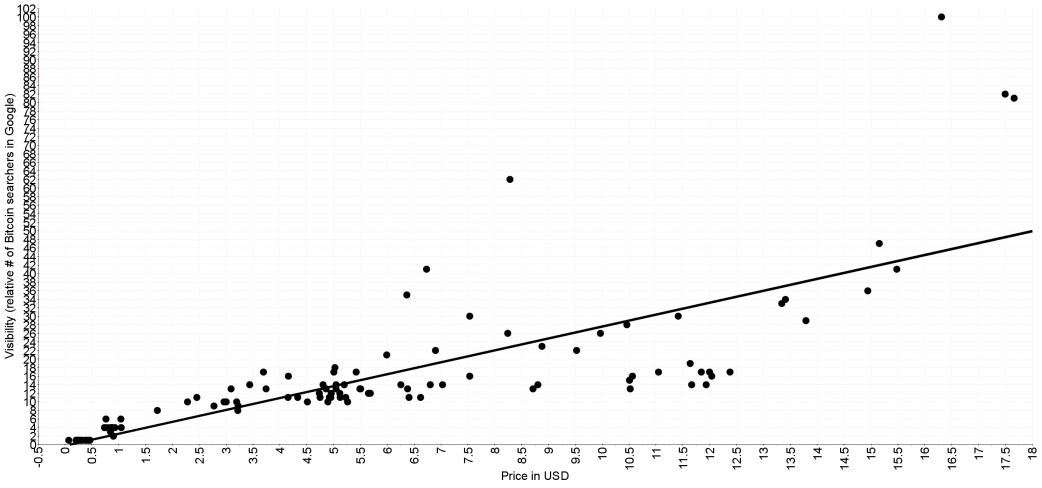


Figure 4.5: Scatter plot diagram of price and visibility, weekly granularity

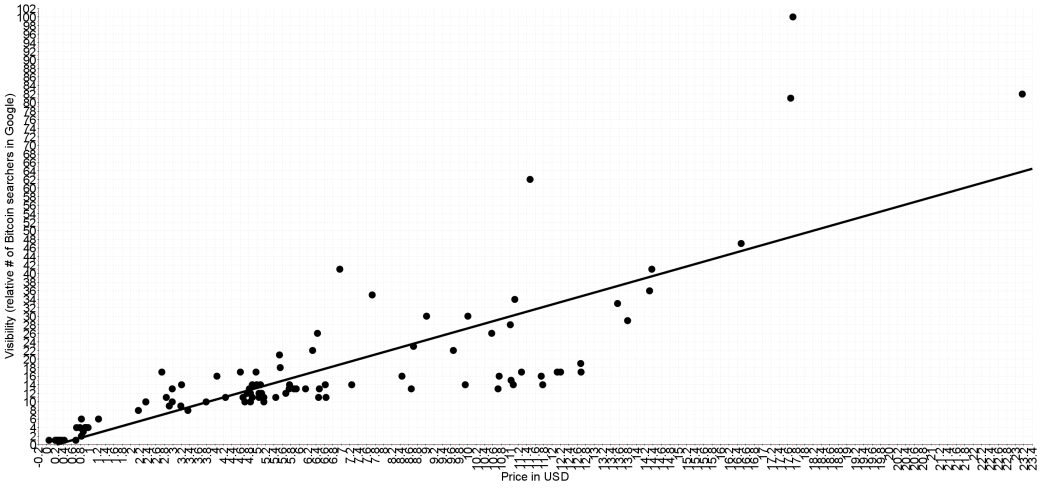
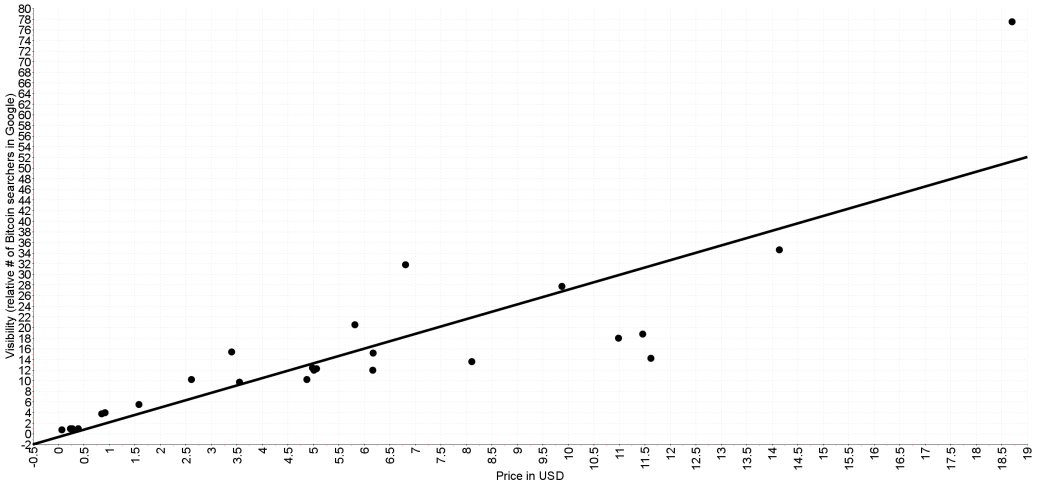


Figure 4.6: Scatter plot diagram of price and visibility, monthly granularity



Regression analysis shows a strong positive correlation between Bitcoin price in USD and visibility (measured in terms of number of Bitcoin searches in Google). In other words, the price of Bitcoin correlates with the public interest in Bitcoin. I present these possible reasons for this correlation:

- A rising price price creates hype and motivates people's interest in Bitcoin
- Rising interest in Bitcoin results in excessive buying of Bitcoin, driving the price up
- Rising interest and rising price mutually influence each other
- Other factors (e.g. the demand, since the supply is inelastic) influence both people's interest in Bitcoin as well as cause excessive buying

4.2 Liquidity and price volatility

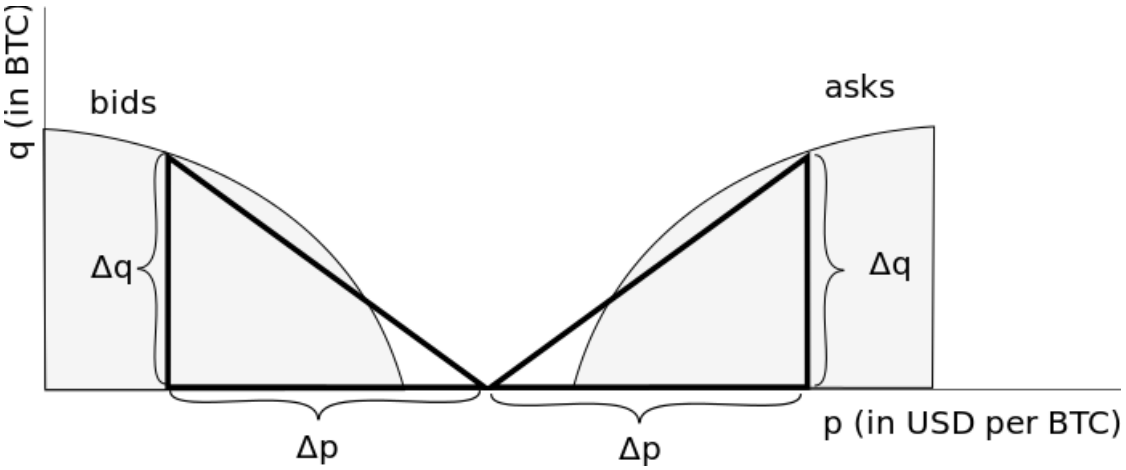
4.2.1 Liquidity

The data from liquidity calculation was taken from Mt.Gox order book. Since Mt.Gox only provides the current snapshot of the order book, the data had to be gathered over a longer period of time.[62] The available time frame is December 19$^{\text{th}}$ 2011 until October 4$^{\text{th}}$ 2012.

The approach I used for calculating liquidity is based on elasticity, or slope, of a function. It is the change in quantity divided by change in price, as per (4.3), where l_i is the liquidity at promille i, Δq the cumulative order amount (separately for the bid side and ask side), and Δp the price change. The order amount used in calculations is based on a fixed proportion of the total Bitcoin supply (21 million), 1‰ (21,000) and

[62] Most of the data was provided by Felix Tendler, who has been gathering it longer than me.

Figure 4.7: Graphical representation of liquidity used in calculations. Chart for illustrative purposes, does not represent actual data.



5‰ (105,000). Even though not all Bitcoins have been produced, the total future supply is known in advance.

$$l_i = \frac{\Delta q}{\Delta p} \tag{4.3}$$

In order to account for the effect of the bid-ask spread on liquidity, the starting price (for the Δp) isn't the maximum (bid) or minimum (ask) price, but the average of these two. The result is thus smaller when the bid-ask spread is higher. A graphical representation of this is visible in Figure 4.7 on page 55.

The liquidity calculation was done separately on the bid side and ask side, and the average of these two was calculated and used in further calculations (e.g. regression analysis).

Analysis

Higher liquidity at 1‰ than at 5‰ is a suggestion of a concave liquidity function. A concave liquidity function can be interpreted as more trades occurring closer to the market price, i.e. a healthy market. A convex liquidity function, on the other hand, would indicate a higher chance of a rapid price increase (on the ask side) or decrease (on the bid side). However, two points are insufficient to conclude whether the function is concave or convex and a more complex calculation of slopes is outside of the scope of this thesis.

4.2.2 Evolution of liquidity over time

For an evaluation of a medium of exchange, the evolution of the liquidity over time is the most important factor. In addition to a line chart, a scatter plot diagram and a correlation coefficient between those two variables (liquidity and time) was calculated.

The correlation of liquidity (measured in terms of daily, weekly or monthly slope of the cumulative bids and asks on Mt.Gox) with time is very weak, positive in case of 1‰ and

Figure 4.8: Liquidity at 1‰, daily granularity

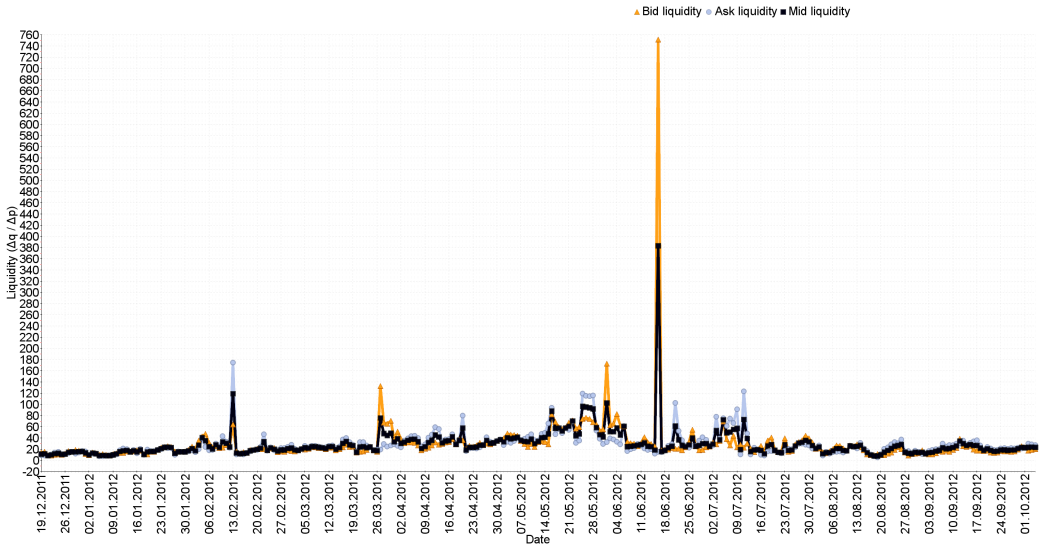


Figure 4.9: Liquidity at 1‰, weekly granularity

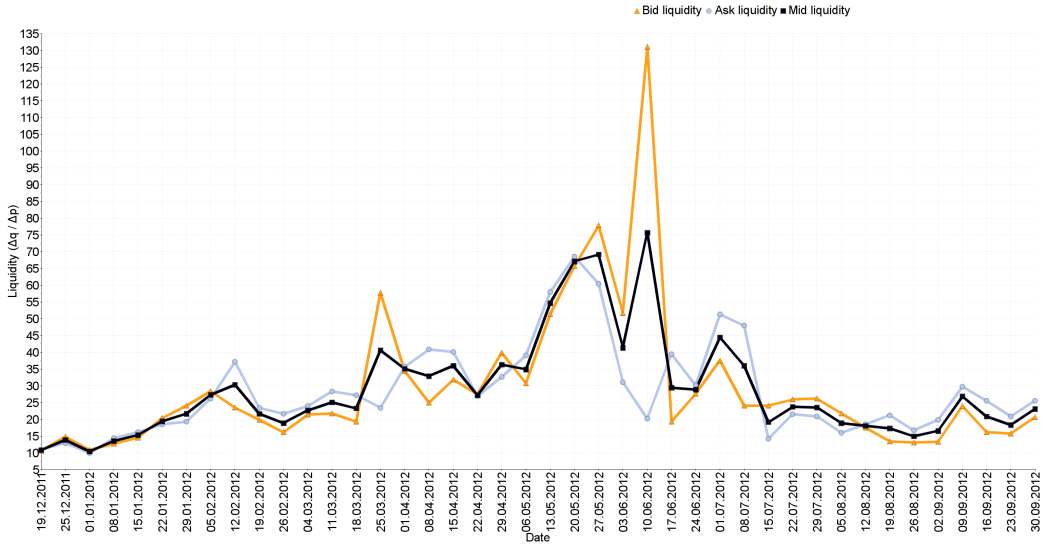


Table 4.2: Correlation coefficient between liquidity and time

granularity	1‰ liquidity	5‰ liquidity
day	0.07	-0.19
week	0.12	-0.21
month	0.17	-0.23

Figure 4.10: Liquidity at 1‰, monthly granularity

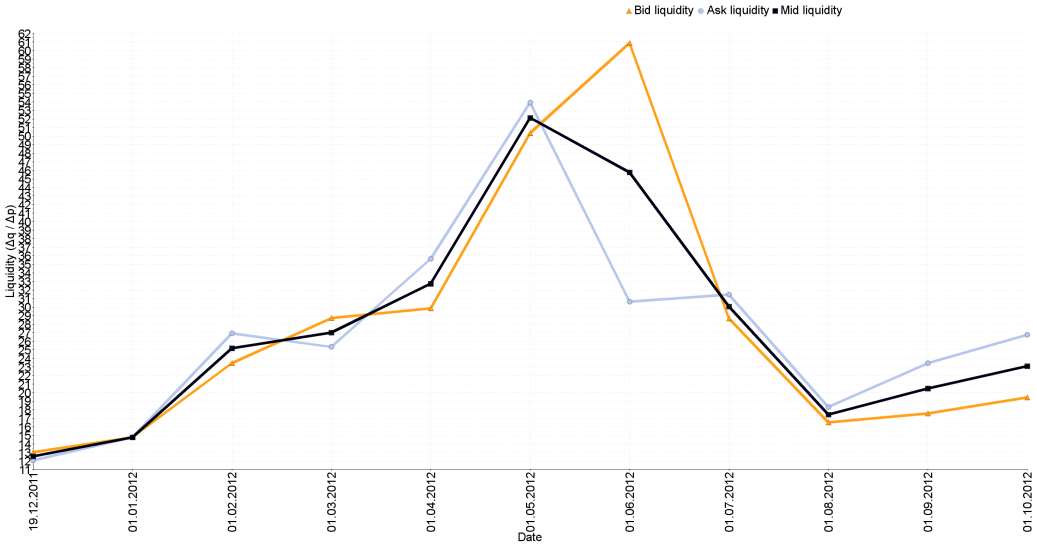


Figure 4.11: Liquidity at 5‰, daily granularity

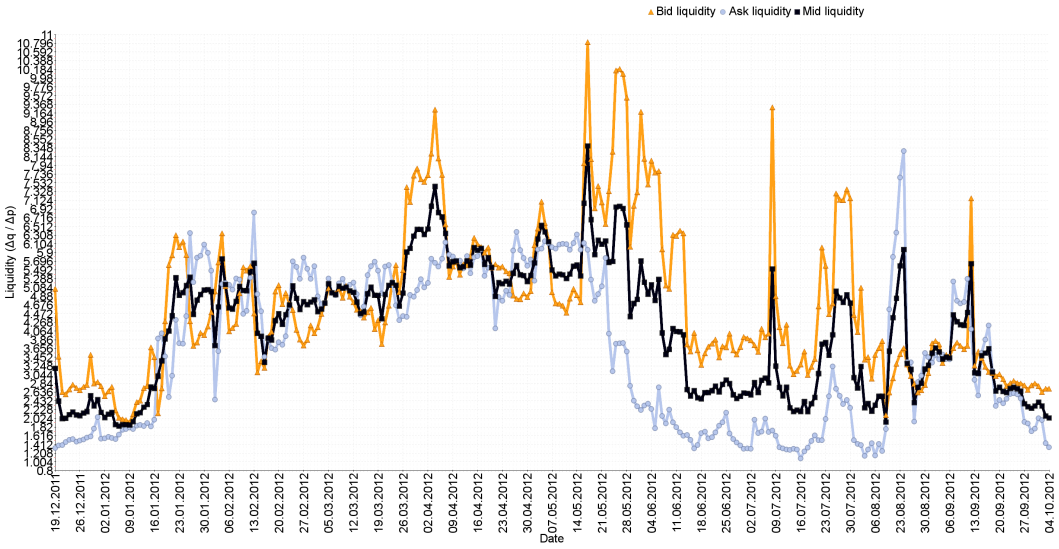


Figure 4.12: Liquidity at 5‰, weekly granularity

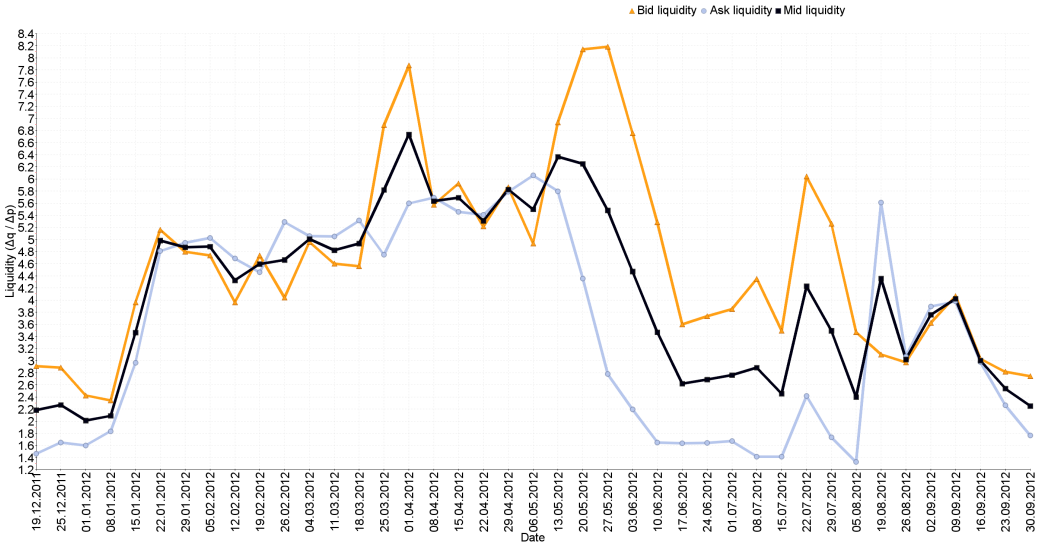


Figure 4.13: Liquidity at 5‰, monthly granularity

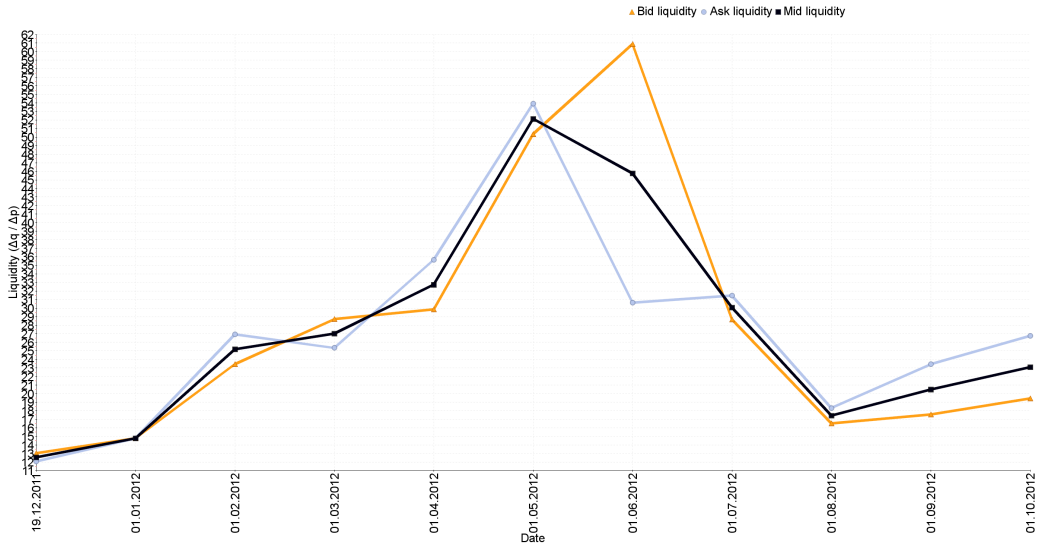


Figure 4.14: Liquidity/Time at 1‰, daily granularity

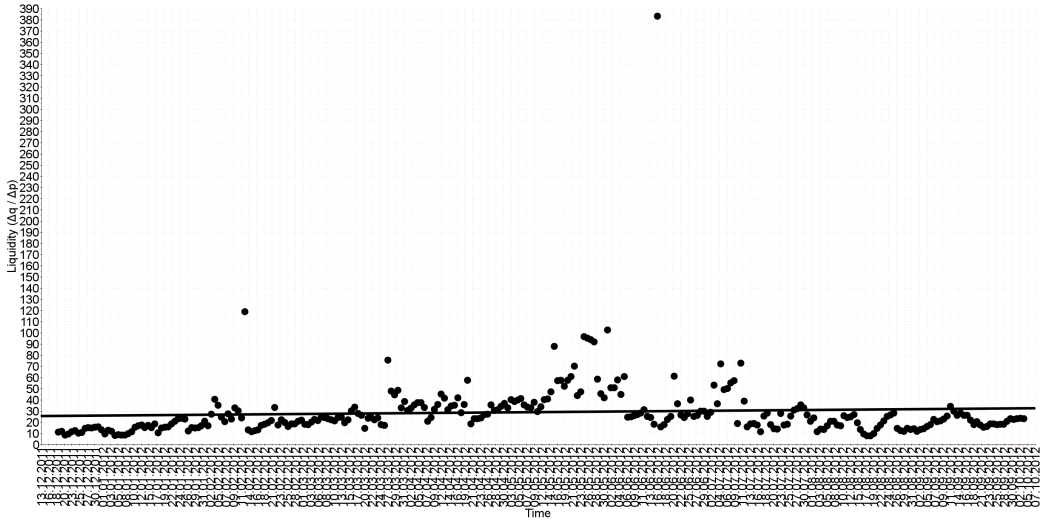


Figure 4.15: Liquidity/Time at 1‰, weekly granularity

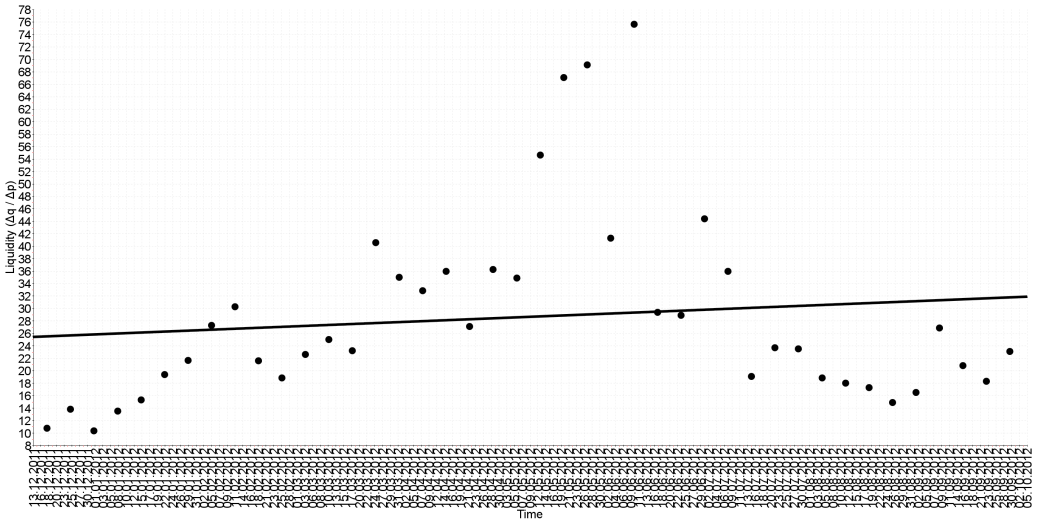


Figure 4.16: Liquidity/Time at 1‰, monthly granularity

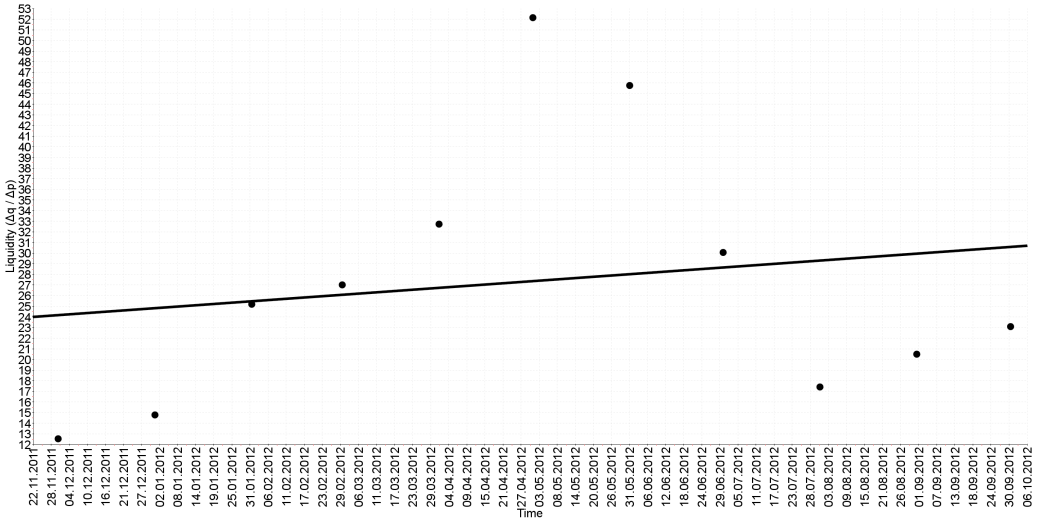


Figure 4.17: Liquidity/Time at 5‰, daily granularity

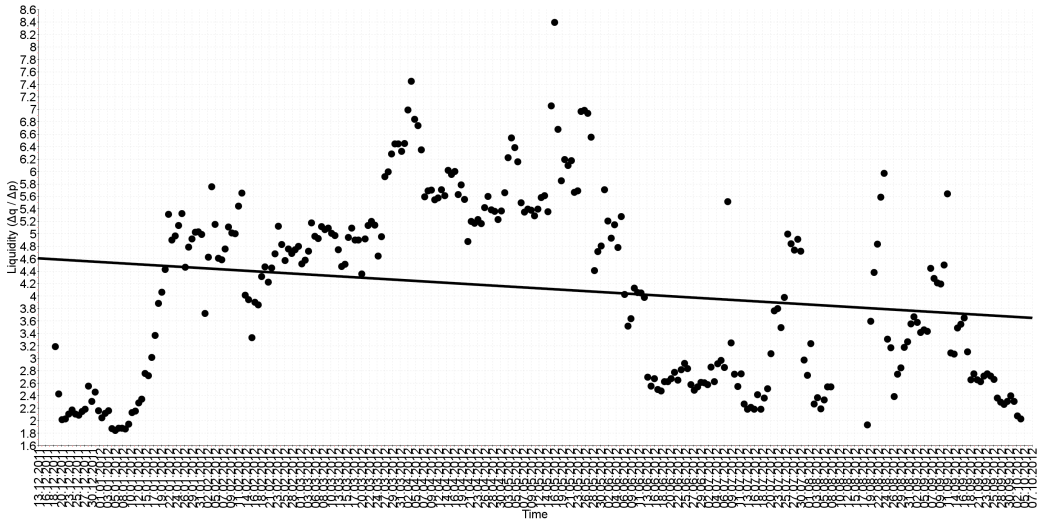


Figure 4.18: Liquidity/Time at 5‰, weekly granularity

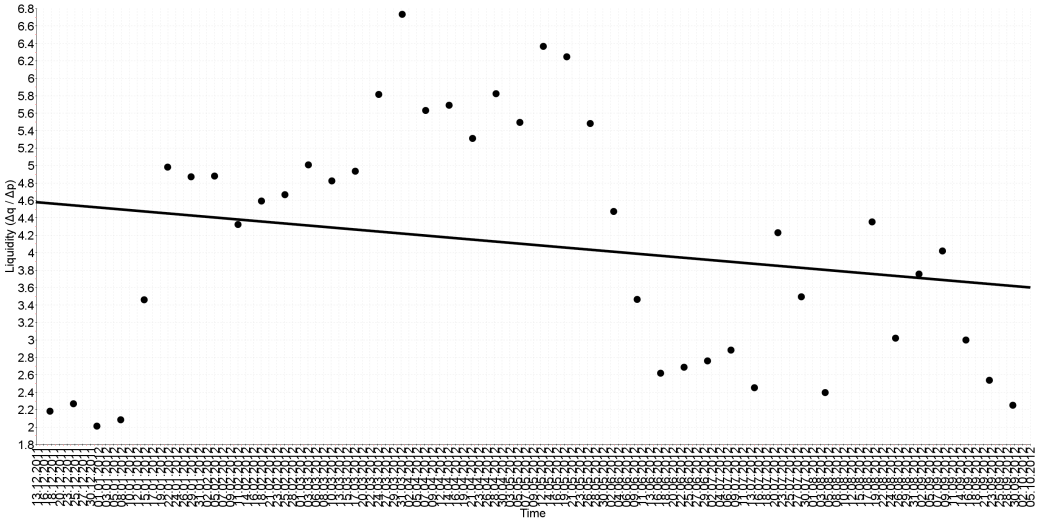


Figure 4.19: Liquidity/Time at 5‰, monthly granularity

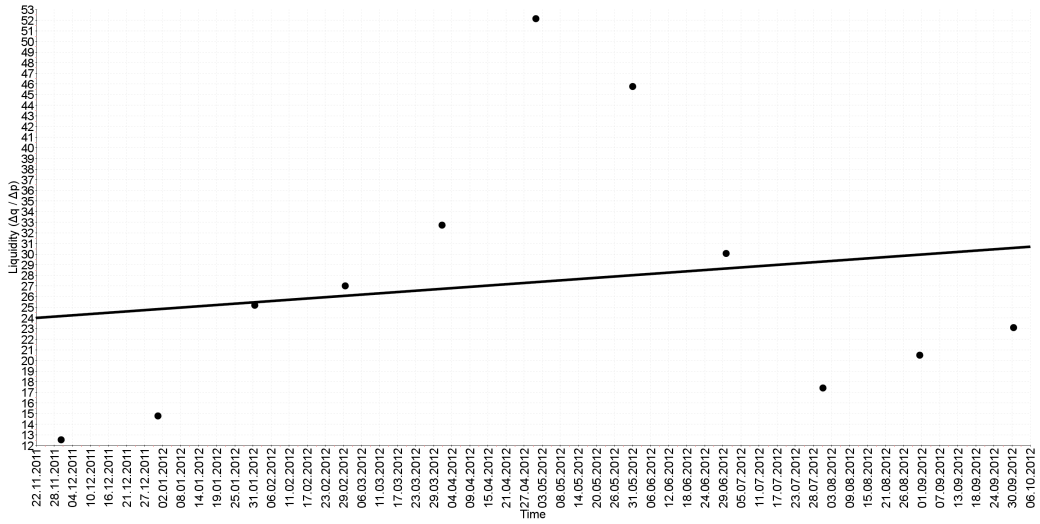
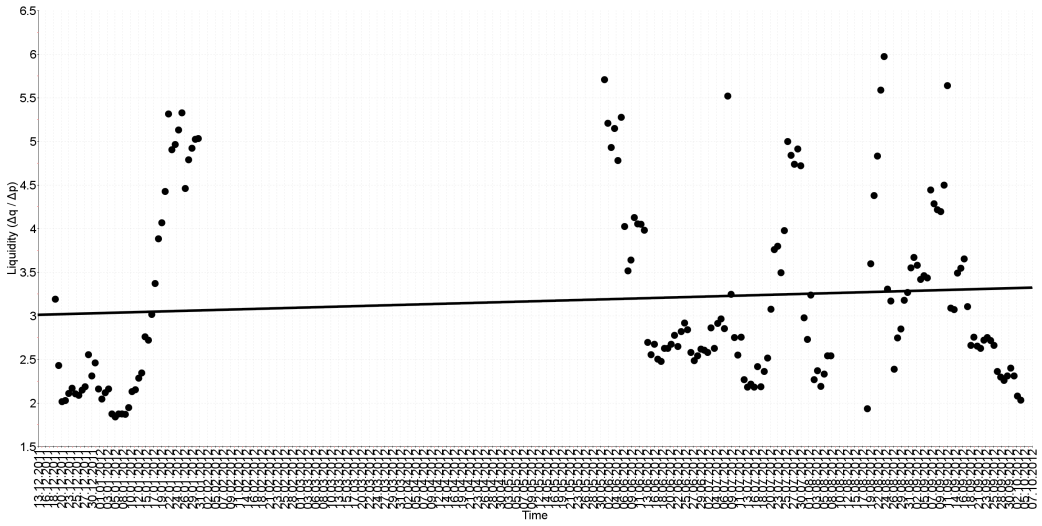


Table 4.3: Correlation coefficient between liquidity and time, excluding February-May 2012

granularity	5‰ liquidity
day	0.10
week	0.06
month	0.14

Figure 4.20: Liquidity/Time at 5‰, excluding February-May 2012, daily granularity



negative in case of 5‰ liquidity. A closer look reveals that during the period between February and May 2012, 5‰ liquidity was on average higher than during the rest of the analysed time period. If we eliminate this time period from the analysis, the correlation turns weakly positive instead of weakly negative:

Analysis

Several sources, for example GoWest (2012) and Buterin (2012a), suggest that the reason for the higher liquidity during this time is due to liquidity arbitrage activities of Bitcoinica and BTCST. Both companies stopped operating in the meantime (as of November 2012, Bitcoinica is in liquidation, and BTCST vanished and is being investigated by the US Securities and Exchange Commission). I was unable to verify the claim that these two companies were conducting liquidity arbitrage, as Mt.Gox, the only independent party who has access to the data, declined to provide the necessary information due to privacy policies. However, anecdotal evidence suggests that this is a plausible explanation. Bitcoinica source code was leaked and analysed, and it reveals a hedging algorithm consistent with liquidity arbitrage activities. The person behind BTCST, "pirateat40" (whose real name has since been revealed to be Trendon Shavers), has, according ongoing investigations [63], a long history of allegations of fraud or outright theft. While it thus appears

[63] According to a private convesation with BrightAnarchist (2012)

Figure 4.21: Liquidity/Time at 5‰,excluding February-May 2012, weekly granularity

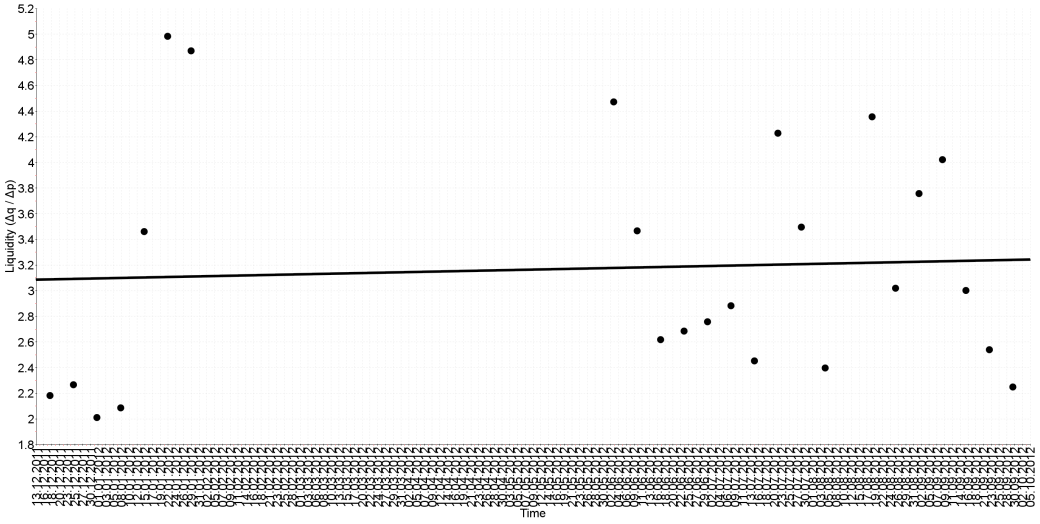


Figure 4.22: Liquidity/Time at 5‰, excluding February-May 2012, monthly granularity

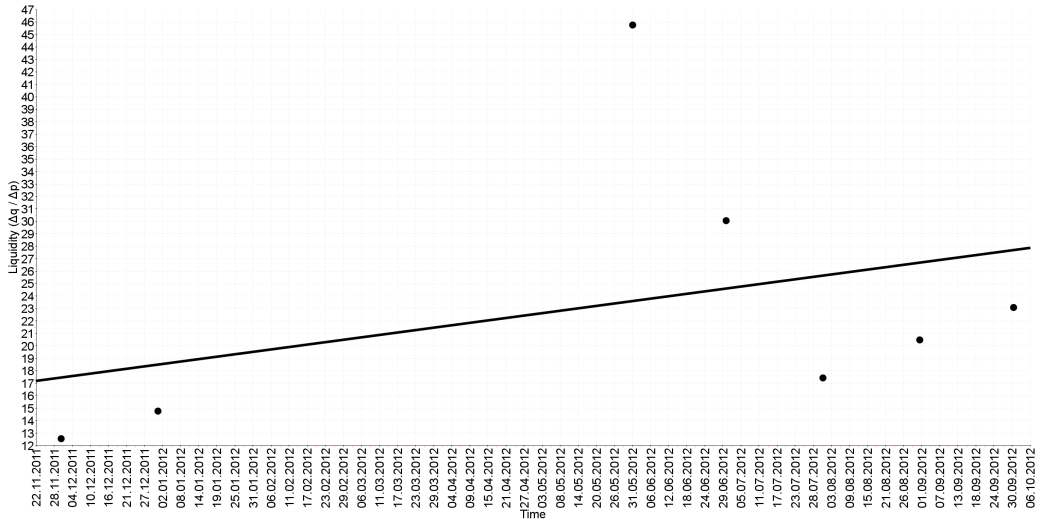
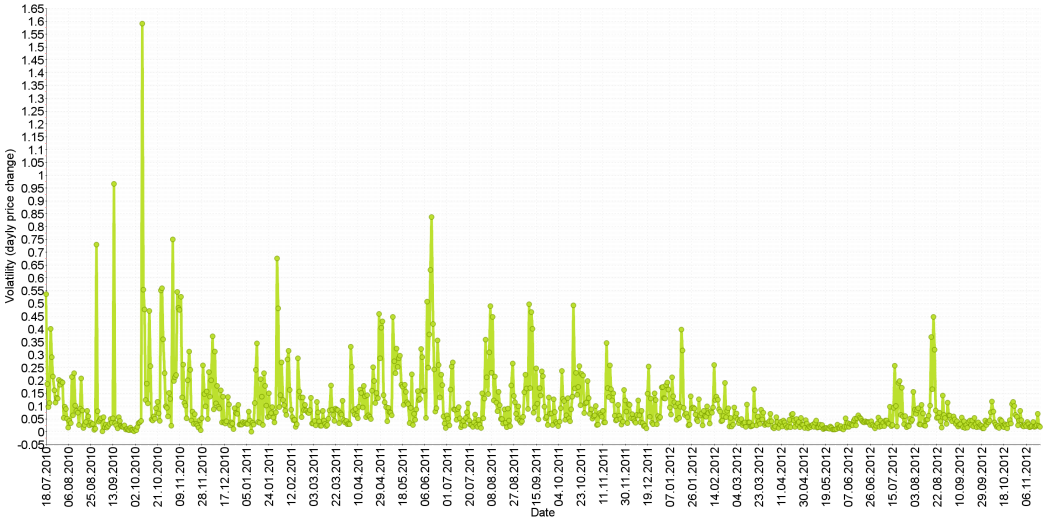


Figure 4.23: Price volatility, daily granularity



unlikely that Shavers did actually conduct liquidity arbitrage, or any trading strategy for that matter (and more likely was running a plain Ponzi scheme), after he stopped paying out, this created collapses on derivative and loan markets (for example BTCST pass-through bonds floated on GLBSE, people who borrowed money to invest into BTCST or BTCST-derivatives), as documented by BCB (2012). These collapses could have affected liquidity of Bitcoin, however only after August 2012, when BTCST closed down. So BTCST probably did not affect the liquidity during the February-May period.

A regression analysis of the evolution of liquidity of Bitcoin over time is, overall, inconclusive. Based on the available data, we cannot make predictions for future liquidity. Either we would need to obtain other data sources, or wait for data over a longer period.

4.2.3 Price volatility

Price volatility is another important aspect of money. I calculated the price volatility as the relative change of the price during the granularity interval (e.g. one day). The available time frame is the same as for price itself. The formula is (4.4), where $vol_{i,j}$ is the volatility between the first price in the interval, p_i, and the last price in the interval, p_j.

$$vol_{i,j} = \frac{max\left(p_i, \ldots, p_j\right) - min\left(p_i, \ldots, p_j\right)}{\frac{max(p_i,\ldots,p_j)+min(p_i,\ldots,p_j)}{2}} \tag{4.4}$$

4.2.4 Correlation between liquidity and price volatility

In addition to granularity, there is a second scope variable, liquidity, and has two possible values, 1‰ and 5‰. Therefore, six correlation coefficients were calculated. The result is presented in Table 4.4 on page 65.

Figure 4.24: Price volatility, weekly granularity

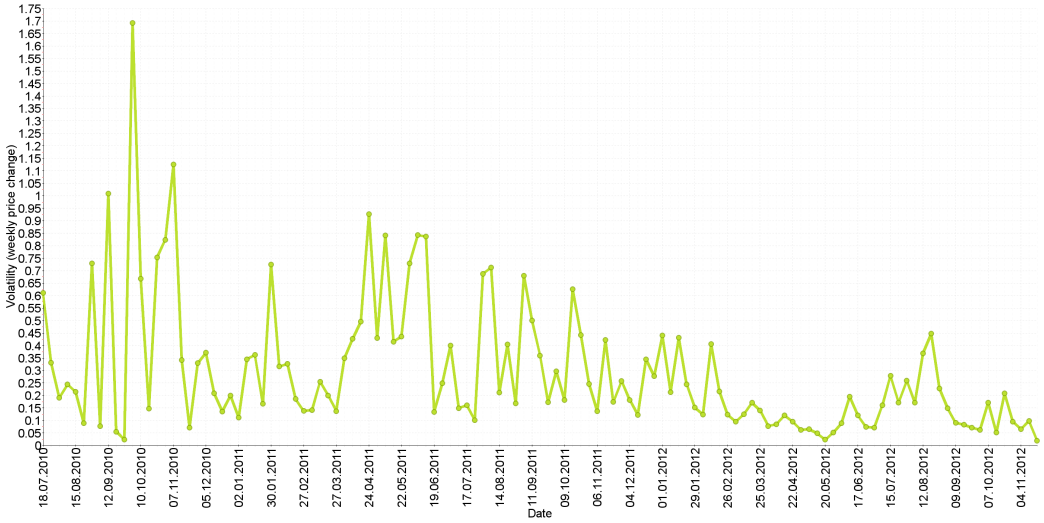


Figure 4.25: Price volatility, monthly granularity

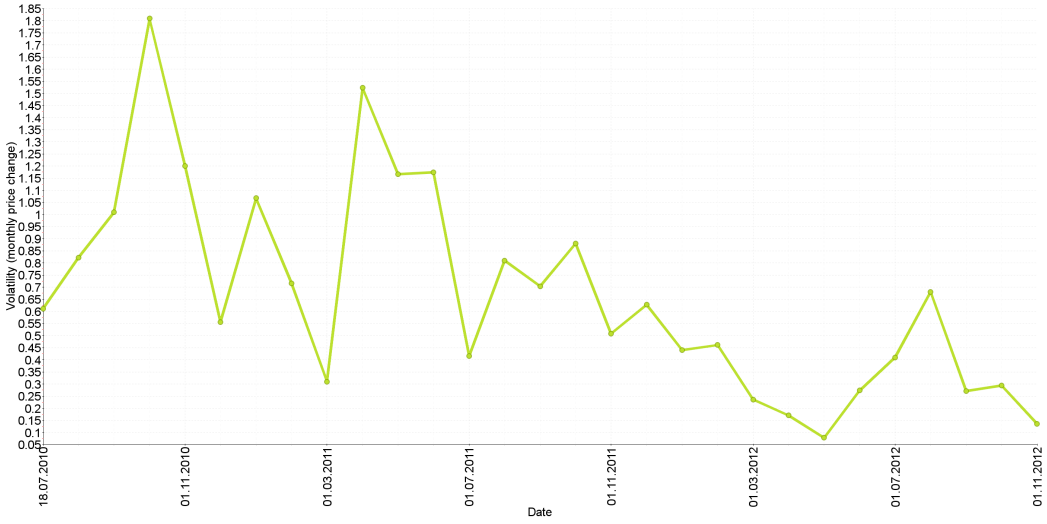


Table 4.4: Correlation coefficient between liquidity and price volatility

granularity	1‰ liquidity	5‰ liquidity
day	-0.24	-0.33
week	-0.50	-0.40
month	-0.74	-0.63

Figure 4.26: Liquidity / price volatility at 1‰, daily granularity

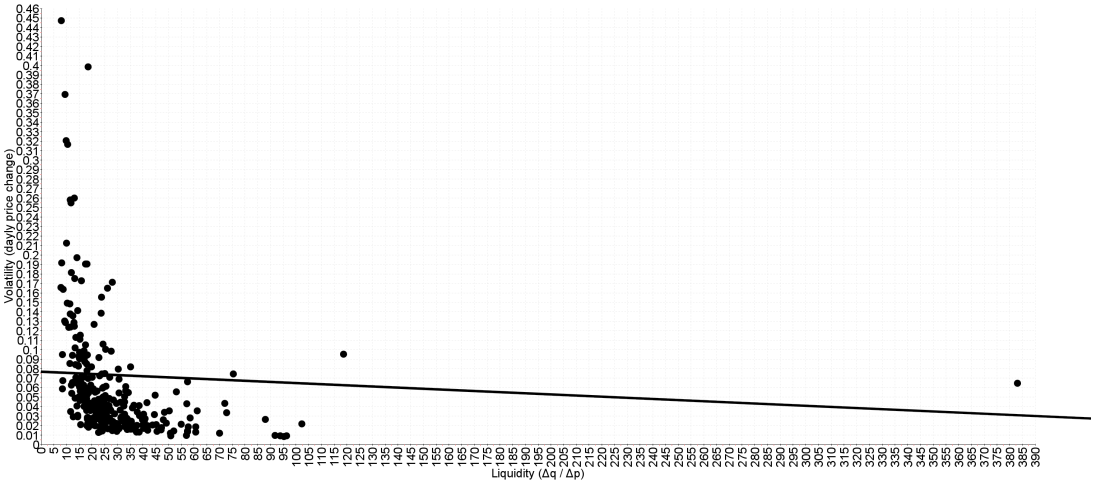


Figure 4.27: Liquidity / price volatility at 1‰, weekly granularity

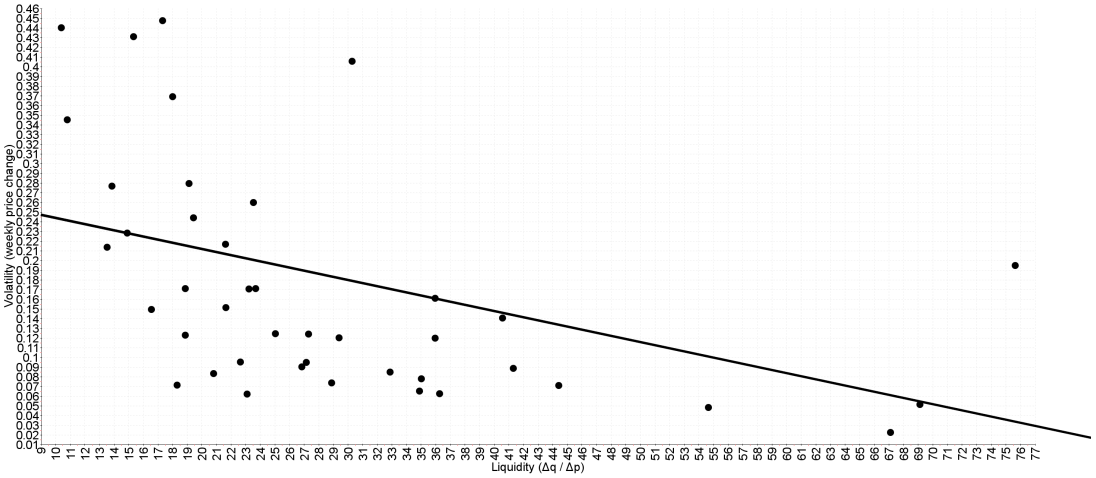


Figure 4.28: Liquidity / price volatility at 1‰, monthly granularity

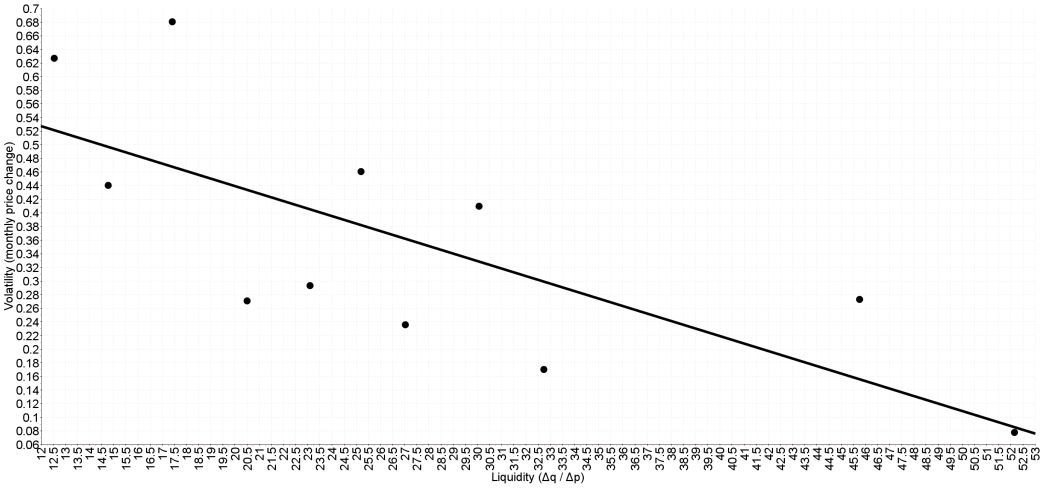


Figure 4.29: Liquidity / price volatility at 5‰, daily granularity

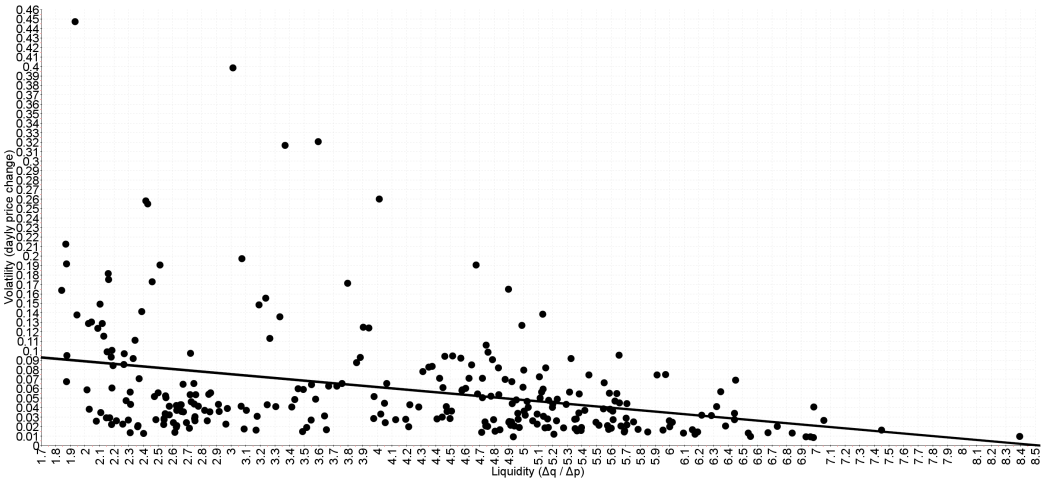


Figure 4.30: Liquidity / price volatility at 5‰, weekly granularity

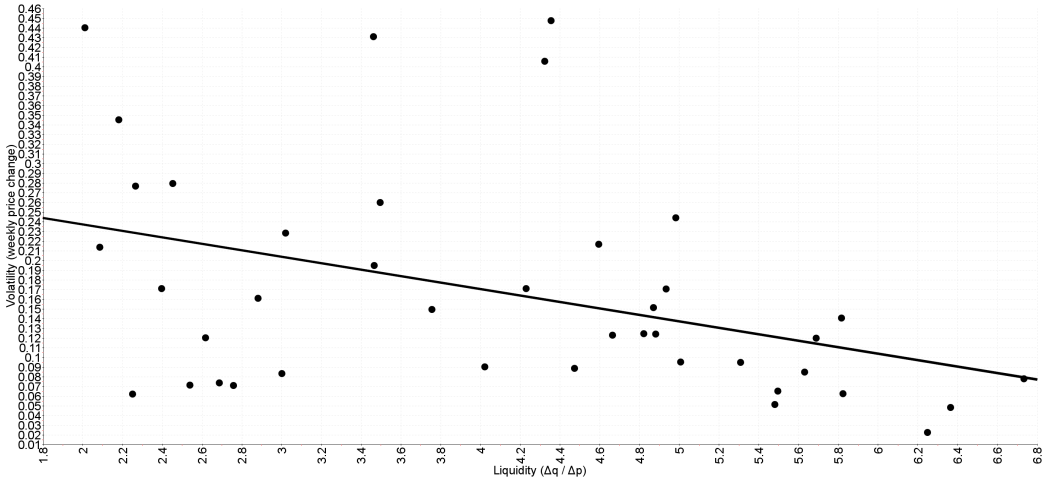


Figure 4.31: Liquidity / price volatility at 5‰, monthly granularity

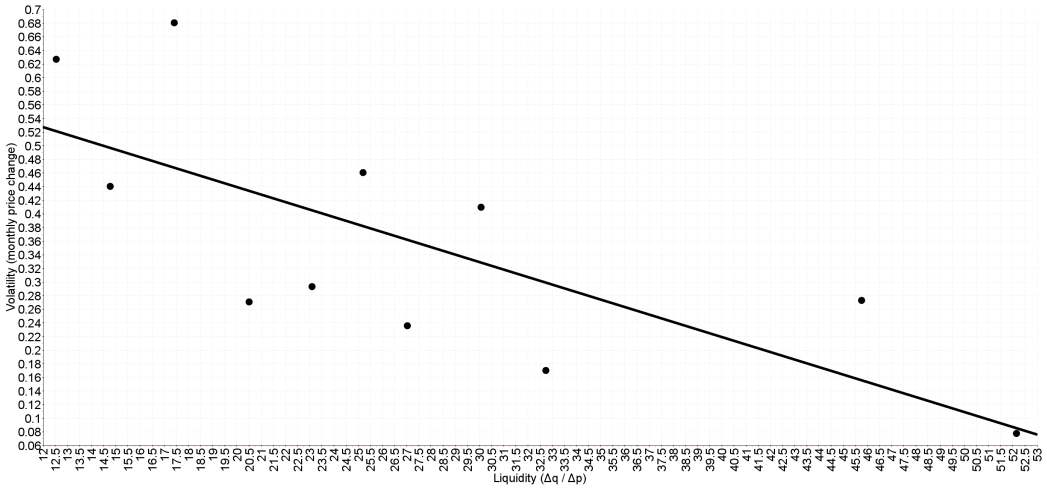
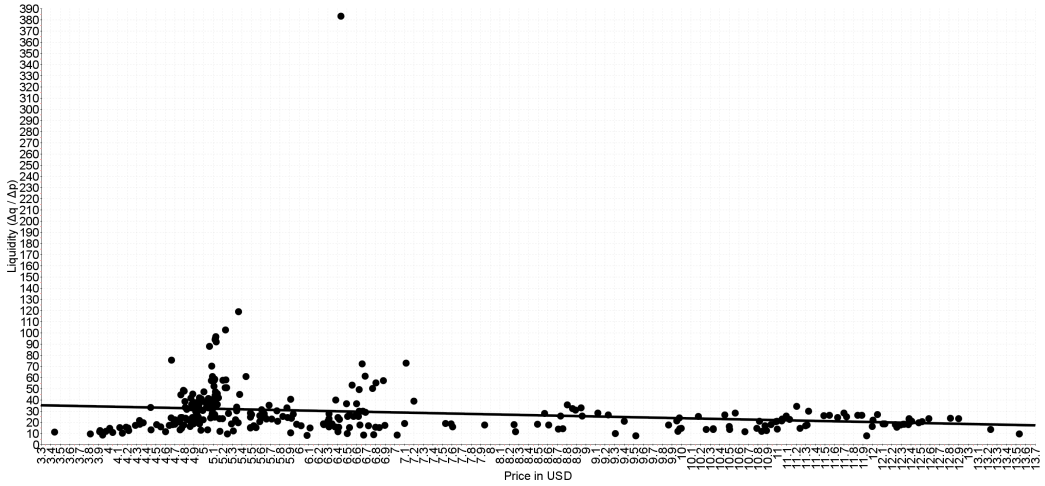


Table 4.5: Correlation coefficient between price and liquidity

granularity	1‰ liquidity	5‰ liquidity
day	-0.17	-0.45
week	-0.32	-0.49
month	-0.26	-0.48

Figure 4.32: Price / Liquidity at 1‰, daily granularity



Analysis

Regression analysis between Bitcoin price volatility (measured in terms of daily, weekly or monthly USD price change) and liquidity (measured in terms of daily, weekly or monthly slope of the cumulative bids and asks on Mt.Gox) reveals a medium to strong negative correlation. This is consistent with a medium of exchange with an inelastic supply, as well as the economic features of competition between media of exchange: liquidity plays a significant role in the choice. I would however advice caution in interpreting these results as a proof of Bitcoin becoming money. Liquidity arbitrage could also have the same effect, even though without depending on the medium of exchange functionality.

4.2.5 Correlation between price and liquidity

The regression analysis of the relationship between price and liquidity is based on the variables presented earlier in this chapter, therefore only results are presented. The correlation coefficient table is in 4.5, scatter plot diagrams at Figure 4.32 on page 69 through Figure 4.37 on page 72.

Figure 4.33: Price / Liquidity at 1‰, weekly granularity

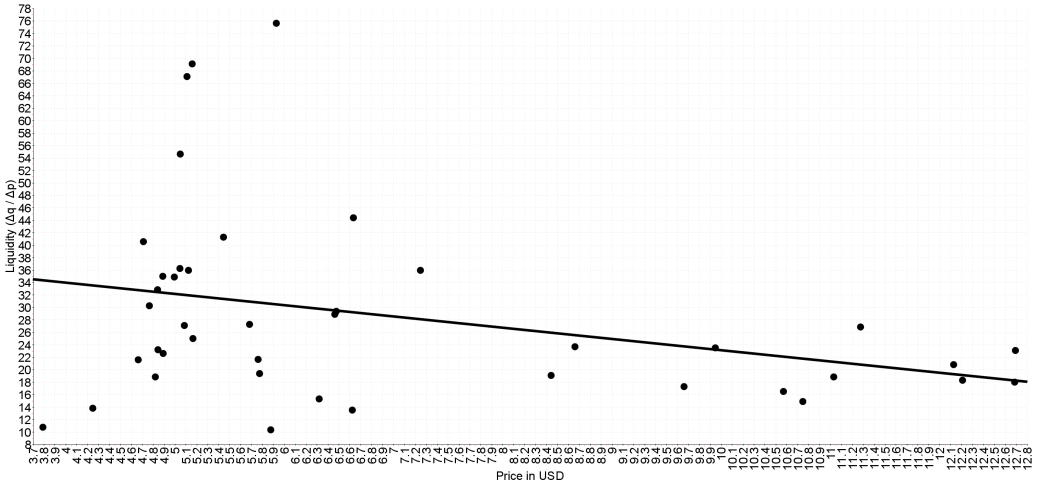


Figure 4.34: Price / Liquidity at 1‰, monthly granularity

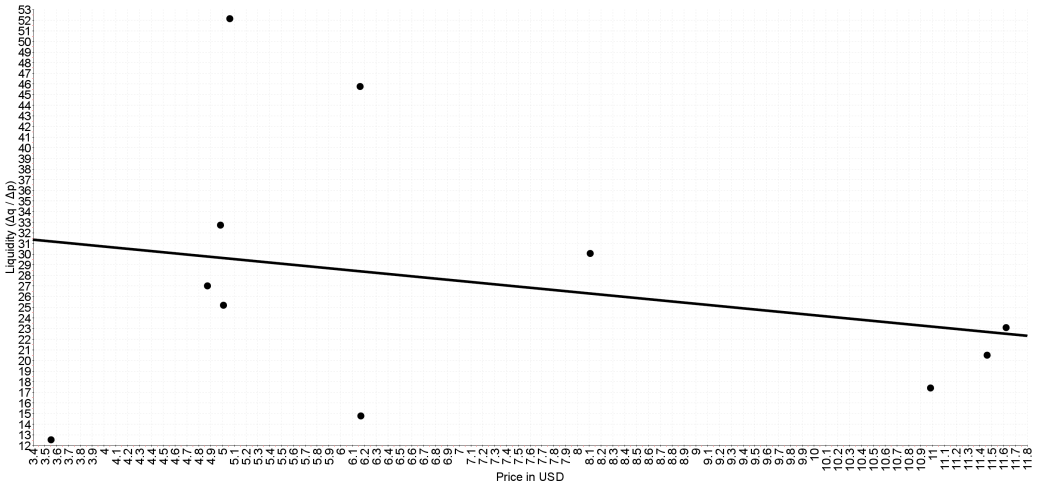


Figure 4.35: Price / Liquidity at 5‰, daily granularity

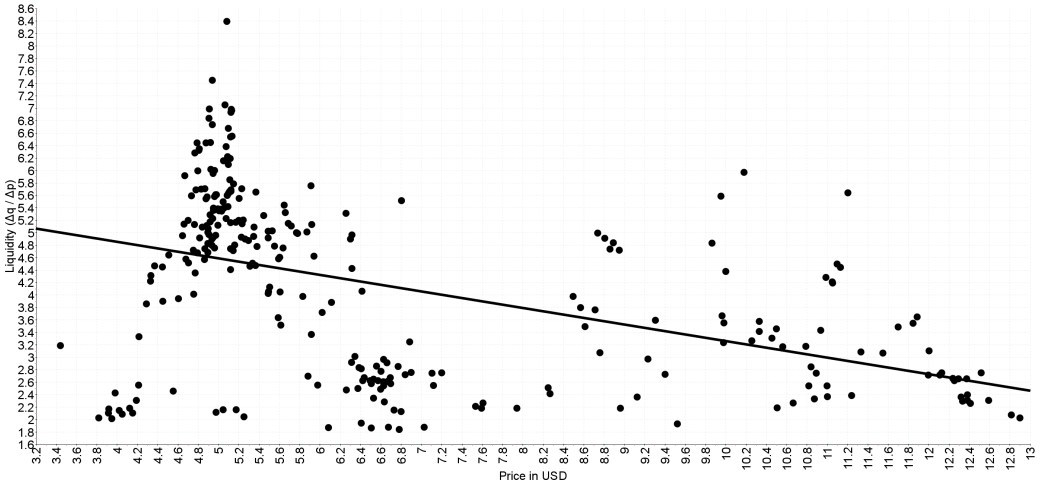


Figure 4.36: Price / Liquidity at 5‰, weekly granularity

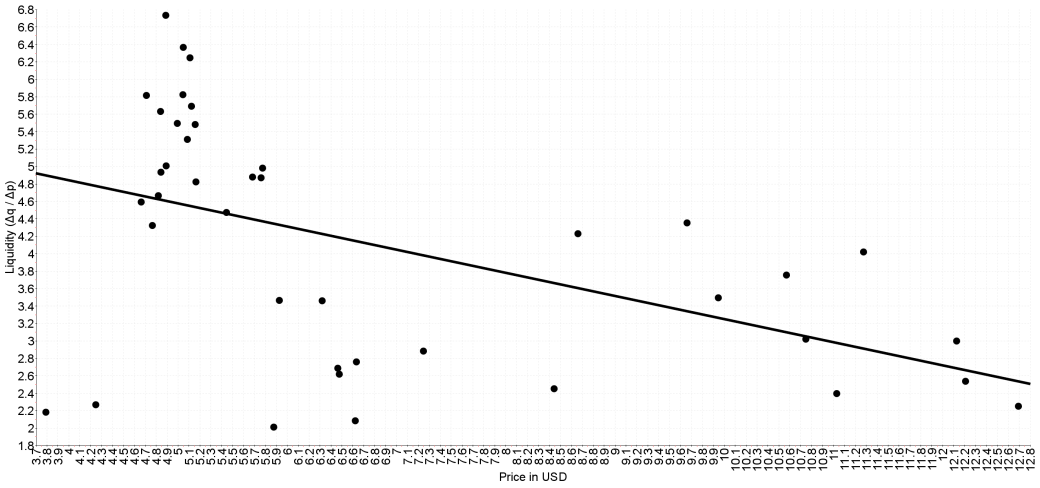
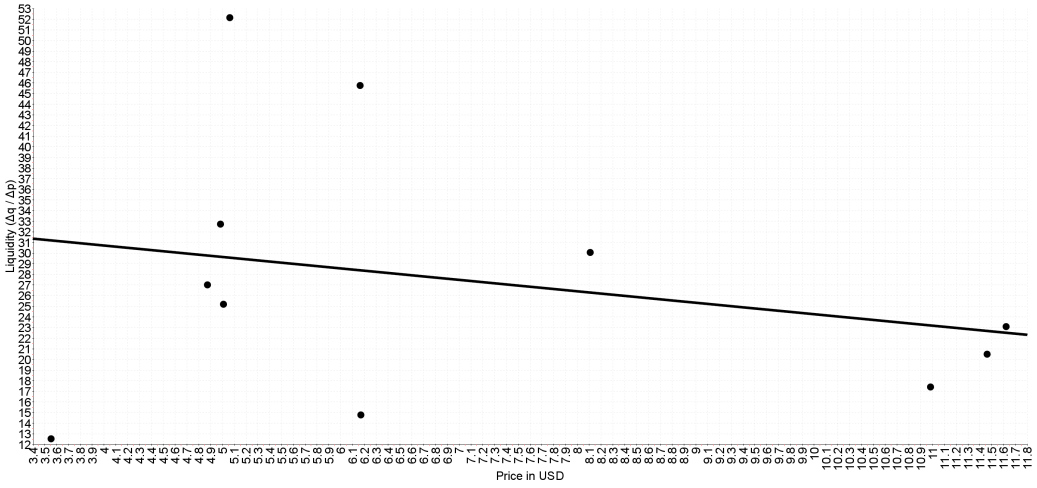


Figure 4.37: Price / Liquidity at 5‰, monthly granularity



Analysis

The correlation coefficient between Bitcoin price in USD and liquidity (measured in terms of daily, weekly or monthly slope of the cumulative bids and asks on Mt.Gox) is weak to medium negative. It is weaker than between price volatility and liquidity. High price is accompanied with low liquidity, which can be interpreted as high prices being bubble behaviour. On the other hand, low price being accompanied by high liquidity could be interpreted as a solid economic foundation of Bitcoin, i.e. an economic resistance to a total collapse.

4.3 Velocity of circulation

Since the transactions in the blockchain are publicly accessible, this can be used for calculating the velocity of circulation. A collective effort of Bitcoin enthusiasts brought up a proposal for a measure of velocity called Bitcoin Days Destroyed (BDD). John Tobey made a first implementation in his project Bitcoin-Abe[64]. A related measure is Cumulative Bitcoin Days Destroyed (CBDD) was built on top of BDD. While BDD can be seen as a sequence, CBDD can be seen as a (normalised) series based on the sequence.

Bitcoin Blockchain is distributed and available by using a Bitcoin client (for example the reference client originally written by Nakamoto and further developed in open source manner). The data is stored in Berkeley-DB format, however the aforementioned Bitcoin-Abe can convert it into MySQL. This is how the blockchain data was obtained. The time frame analysed is since the launch of the blockchain, January 3rd 2009 until November 18th 2012.

In order to use a velocity for economic purposes, CBDD had to be adjusted. First of

[64] Bitcoin-Abe can be downloaded from https://github.com/jtobey/bitcoin-abe

Table 4.6: Transaction fee comparison for selected Bitcoin payment processors and exchanges

Service provider	Basic fee
WalletBit (see WalletBit (2012))	0.89%
BitPay (see BitPay (2012))	0.99%
Mt.Gox (see Mt.Gox (2011))	2*0.6% = 1.2%

all, CBDD is normalised based on the maximum supply of Bitcoins (21 million). I re-normalised it to fit the number of Bitcoins existing at time of transaction. Furthermore, CBDD is based on days, while economics typically uses velocity over a year. So the result was multiplied by 365[65]. Last but not least, velocity of circulation is only calculated from value the transaction *added* to the economy, not from total volume (in other words, only the value of the *final* goods and services)[66]. This datum is not available for Bitcoin. However, the fees of the Bitcoin payment processors and exchanges involved in Bitcoin are publicly available. Since these companies operate on a free market, they need to price competitively, so their fees are expected to be close to their value added. The result is presented in Table 4.6 on page 73. Based on the results, I use a value added ratio, V_A, of 1%.

The resulting formula is presented as formula (4.5), where vel_i is the average cumulated velocity of blocks 0 through i, B_i is the number of Bitcoins created until block i, V_A, as mentioned above, is the average value-added ratio of a Bitcoin transaction, S_{d_i} is the "satoshi seconds destroyed" (i.e. Bitcoin days destroyed but using different units, satoshis instead of bitcoins, and seconds instead of days) until block i, and s_{t_i} "total satoshi seconds", i.e. nominal total transaction volume until block i.

$$vel_i = 365 \times V_A \times \frac{1 - \frac{S_{d_i}}{S_{t_i}}}{B_i} \tag{4.5}$$

In addition to the problem with estimating V_A, the velocity calculation also does not capture ToK transactions (which need to be included), but it correctly ignores the forex transactions occurring on the exchange (trade of Bitcoin against fiat currencies).

4.3.1 Velocity of other currencies

Federal Reserve Bank of St. Louis (2012) provides velocity data for the US dollar. A summary is presented in Table 4.7 on page 74. Depending on the monetary aggregate and time period, the velocity of the USD is between 1.568 and 10.367.

Godschalk (2006) provides information about velocity of various complementary currencies, as well as for the USD and the Euro:

> "Thus the velocity of the Bethel-money used in the v. Bodelschwingh Foundation Bethel in Bielefeld-Bethel is approximately 14 p.a. The velocity of M1

[65] I used 365 instead of 365.25 or separate 365/366 depending on leap year. There are several reasons for this. The first one is that we do not know the cyclical behaviour of Bitcoin users. For example, agricultural processes or taxation are more dependant on the season or a particular date, so an adjustment in such a case might be helpful. On the other hand, digital goods usually do not depend on a particular date, so an adjustment for the leap year might make the result less accurate. Last but not least, an adjustment is algorithmically more complicated, and would require de-cumulation of the data first. When I combined the two factors, I opted for a simpler solution.

[66] I would like to thank John Barrdear for this point.

Figure 4.38: Velocity of Bitcoin, daily granularity

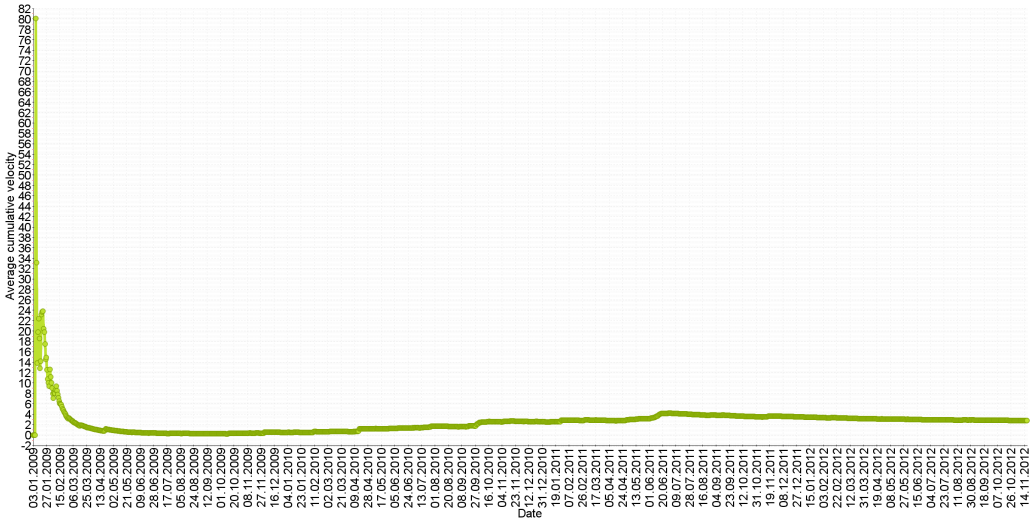


Figure 4.39: Velocity of Bitcoin, weekly granularity

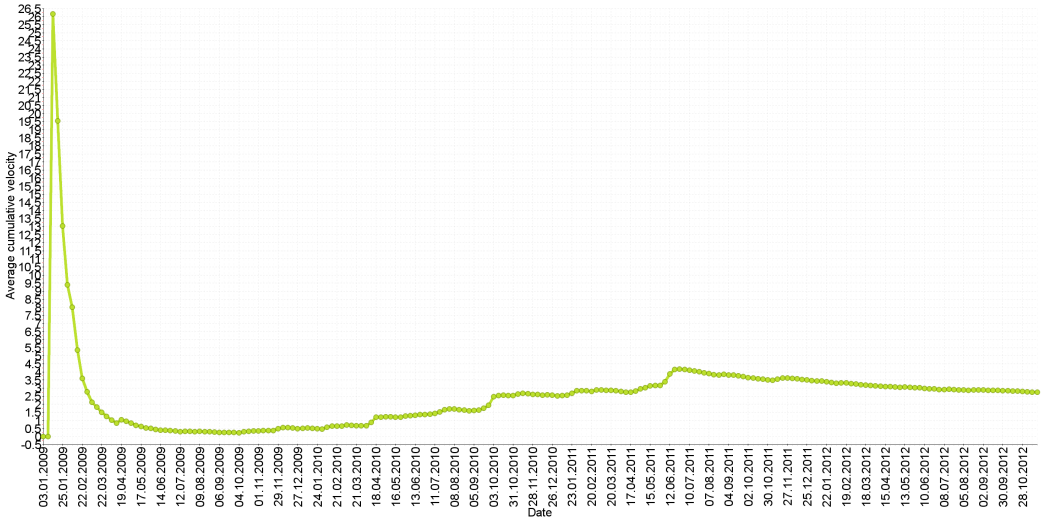
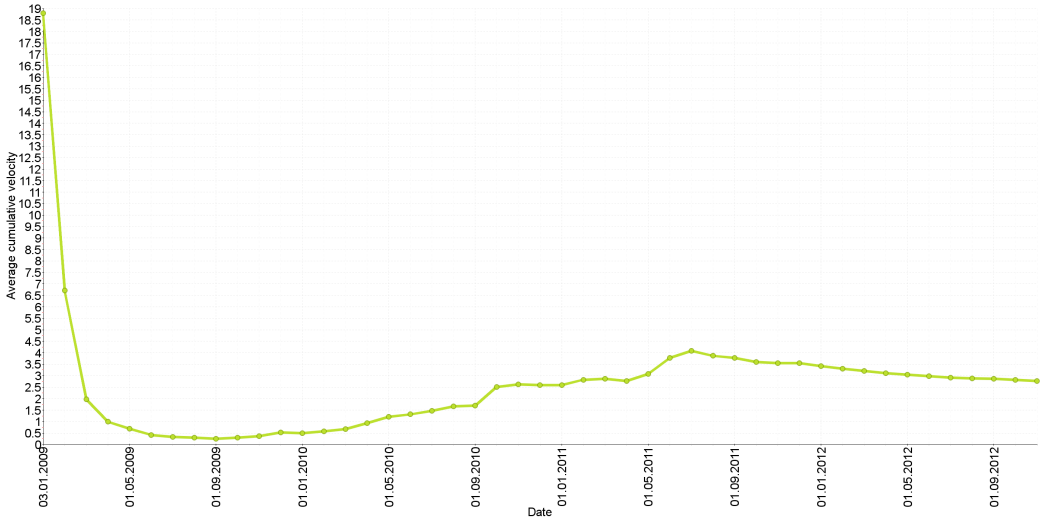


Table 4.7: Velocity of USD, 1959:Q1 to 2012:Q3

Monetary aggregate	Minimum	Maximum
M1	3.556	10.367
MZM	1.418	3.458
M2	1.568	2.135

Figure 4.40: Velocity of Bitcoin, monthly granularity



(cash and demand deposits) in Germany is approximately 3.5 p.a. For certain types of complementary currencies, records exist for the date of issue, date of redemption, as well as every transaction. Therefore the velocity can be calculated exactly. The velocity of the local currency in the city of Santa Cruz (California) was approximately 48 p.a., while the Dollar (M1) was only used between 2.2 and 2.3 on average during this period.[67]

The commentary provided by Godschalk however indicates that the complementary currency velocity was calculated from total sales volume, rather than only the value added. Therefore, the data from complementary currencies would need to be adjusted for value added, similarly as I do with my calculations of the velocity of Bitcoin. The argument of Godschalk that complementary currencies have a higher velocity than national money should therefore be treated cautiously (indeed, if I did not attempt an adjustment, I would conclude that the velocity of Bitcoin is 10-20 times that of complementary currencies and 100 times that of national currencies).

4.3.2 Analysis

The velocity shows a peak around June 2011, coinciding with the price peak in price. Over longer term, the velocity appears to be stabilising, however strictly speaking the data presents an *average cumulated* velocity rather than only the immediate one, so the magnitude of the stabilisation as seen in the chart might be misleading.

[67] Translated from "So beträgt die Umlaufgeschwindigkeit des innerhalb der Bodelschwinghschen Anstalten in Bielefeld-Bethel verwendeten Bethel-Geldes ca. 14 p.a. Die Umlaufgeschwindigkeit von M1 (Bargeld und Sichteinlagen) beträgt in Deutschland ca. 3,5 p.a. Bei bestimmten Arten dieses Nebengeldes wurden Ausgabedatum, Einlösedatum und jede Transaktion festgehalten, so dass die Umlaufgeschwindigkeit exakt ermittelt werden konnte. Die Geschwindigkeit betrug z. B. bei dem Regionalgeld in der Stadt Santa Cruz (Kalifornien) ca. 48 p.a., während der Dollar (M1) in dieser Periode im Durchschnitt nur 2,2 bis 2,4 mal eingesetzt wurde."

Bitcoin appears to have a similar velocity to other currencies (in particular when considering broader monetary aggregates and taking into account intermediate goods), however significant approximations were made, so a direct comparison should be treated cautiously.

4.4 Conclusion of empirical analysis

Regression analysis reveals several relationships. Bitcoin price correlates with visibility, which could be interpreted in multiple ways. The one I consider most likely is that the two variables mutually influence each other.

The correlation between liquidity and price volatility is consistent with a medium of exchange, but liquidity arbitrage could have affected the correlation. Liquidity also weakly correlates with price, which I interpret as an indication of a strong support from the bottom, yet proneness to bubbles.

On the other hand, the data is insufficient to conclude how liquidity of Bitcoin evolves over time. Based on this, we cannot conclude whether Bitcoin is evolving as a medium of exchange.

The velocity of Bitcoin appears to be similar to other currencies, but significant approximations were made and the result could be significantly under- or overestimated.

Chapter 5

Conclusion

This thesis is about the analysis of Bitcoin as money, whether it poses a serious alternative to fiat currencies or gold. In the theoretical part, I tie together academic research and views from within the Bitcoin community, based on a libertarian point of view. The results are that Bitcoin conforms to the Austrian theory of the catallactic origin of money. It already crossed the obstacles that are the praxeological preconditions for the function of a medium of exchange (the emergence of price, and the emergence of liquidity), as described in the Mises' regression theorem. It is at a very early stage of evolution, users and service providers facing a high level of uncertainty, however, the ecosystem already shows a high level of specialisation, and the services are maturing.

Bitcoin can, hypothetically, eventually evolve into money through the behaviour of market actors. It can also, hypothetically, gain the functions of store of value and unit of account (assuming it does not have them already). Currently, there are areas where Bitcoin has a comparative advantage over other media of exchange, mainly through the reduction of transaction costs in the narrower sense. The existence of this comparative advantage probably means that the critical mass for the network effect has been reached and at this level, the Bitcoin ecosystem is self-sustaining.

If this comparative advantage persists, network effect can increase the adoption of Bitcoin, and thus make the evolution into money more likely. Whether, or to what extent, this comparative advantage persist, depends on the strength and flexibility of the Bitcoin ecosystem, the level of regulation, the emergence of new competitors (e.g. new cryptocurrencies) and the stability of the fiat money.

If Bitcoin becomes money, it would most likely present a system with an inelastic supply and thus conform to the ideal money as viewed by the gold standard branch of the Austrian School. This would be achieved without a legislative reform and irrespective of the existence of fractional reserve banking. In this respect, it is superiour both to fiat money and gold.

In the empirical part, I use data to depict economic features of Bitcoin development: price (June 2010 - November 2012), price volatility (June 2010 - November 2012), liquidity (December 2011 - October 2012), visibility (January 2009 - November 2012) and velocity (January 2009 - November 2012).

Liquidity of Bitcoin appears to correlate negatively with price volatility. This is consistent with a behaviour of a medium of exchange (but not necessarily a proof thereof). Price and visibility of Bitcoin appear to correlate too. The interpretation that I find most

likely is that they are both a consequence of demand for Bitcoin. Price and liquidity correlate weakly. It can be interpreted as certain level of stability of its foundation, but being prone to bubbles. The evolution of liquidity over time does not follow any particular direction. Factors other than those measured (for example, qualitative factors or fraud) have the potential to influence liquidity to a significant extent. The velocity of Bitcoin appears to be similar to other currencies, however due to significant approximations a direct comparison should be treated cautiously.

List of Tables

List of Figures

Index and Abbreviations

Bibliography

Andresen, Trond (2012): What if the Greeks, Portuguese, Irish, Baltics, Spaniards, and Italians did this: high-tech parallel monetary systems for the underdogs? *Real-World Economics Review*, 59(3):105–112. http://www.paecon.net/PAEReview/issue59/whole59.pdf.

Babaioff, Moshe; Shahar Dobzinsky; Sigal Oren; and Aviv Zohar (2012): On Bitcoin and Red Balloons. In: *Proceedings of the 13th ACM Conference on Electronic Commerce*. ACM New York, NY, USA, pp. 56–73. https://research.microsoft.com/pubs/156072/bitcoin.pdf.

BCB (2012): Trendon Shavers - Pirate Pass Through - Crowdsource list. *Bitcoin Forum*. https://bitcointalk.org/index.php?topic=120880.0, datum per se 27. Oct. 2012.

Becker, Jörg; Dominic Breuker; Tobias Heide; Justus Holler; Hans Peter Rauer; and Rainer Böhme (2012): Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency. *SSRN eLibrary*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2041492, datum per se 24. Feb. 2012.

Bednár, Juraj and Juraj Karpiš (2011): Bitcoin - Progressbar Hackerspace. http://video.progressbar.sk/pgb_20110323_bitcoin_sk.mp4, datum per se 23. Mar. 2011.

BitPay (2012): Bit-Pay expands Direct Deposit to CANADA and MEXICO. *BitPay website*. https://bitpay.com/press/2012-03-14-01, datum per se 13. Mar. 2012.

BrightAnarchist (2012): Re: Pirate ponzi investigation. *Private correspondence*, datum per se 25. Oct. 2012.

Brito, Jerry (2012): A Shift Toward Digital Currency. *Room for Debate (New York Times Blog)*. http://www.nytimes.com/roomfordebate/2012/04/04/bringing-dollars-and-cents-into-this-century/a-shift-toward-digital-currency, datum per se 4. Apr. 2012.

Buterin, Vitalik (2012a): Bitcoinica: An Obituary. *Bitcoin Magazine (Blog)*. http://bitcoinmagazine.net/Bitcoinica_An_Obituary/, datum per se 14. May. 2012.

Buterin, Vitalik (2012b): Brain Wallets: The What and the How. *Bitcoin Magazine (Blog)*. http://bitcoinmagazine.net/brain-wallets-the-what-and-the-how/, datum per se 7. Apr. 2012.

Buterin, Vitalik (2012c): Zipconf: The Other Side Of Instant. *Bitcoin Magazine (Blog)*. http://bitcoinmagazine.net/zipconf-the-other-side-of-instant/, datum per se 2. May. 2012.

Catao, Luis and Marco Terrones (2000): Determinants of Dollarization: The Banking Side. *International Monetary Fund Working Paper*, 00(146). http://www.imf.org/external/pubs/ft/wp/2000/wp00146.pdf.

Christin, Nicolas and Jerry Brito (2012): Nicolas Christin on anonymous online market Silk Road. *Surprisingly Free (Podcast)*. http://surprisinglyfree.com/2012/08/28/nicolas-christin/, datum per se 28. Aug. 2012.

de Soto, Jesús Huerta (2009): *Money, Bank Credit, and Economic Cycles*. Mises Institute, 2nd edn. http://mises.org/document/2745/Money-Bank-Credit-and-Economic-Cycles.

deepceleron (2012): Faraday Cage / Cold Storage. *Bitcoin Forum*. https://bitcointalk.org/index.php?topic=60903.msg710662#msg710662, datum per se 24. Jan. 2012.

Dellingshausen, Christoph N. (2011): BVDW warnt Verbraucher und Händler vor Bitcoins als Zahlungsmittel. *Bundesverband Digitale Wirtschaft*. http://www.bvdw.org/medien/bvdw-warnt-verbraucher-und-haendler-vor-bitcoins-als-zahlungsmittel?media=3006, datum per se 1. Jun. 2011.

Elias, Matthew (2011): Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy. *SSRN eLibrary*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1937769, datum per se 3. Oct. 2011.

European Central Bank (2012): Virtual Currency Schemes. http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, datum per se 29. Oct. 2012.

Federal Reserve Bank of St. Louis (2012): Money Velocity. *FRED Economic Data*. http://research.stlouisfed.org/fred2/categories/32242.

Gesell, Silvio (1936): *The Natural Economic Order*. Free-Economy Publishing Company. http://www-tracey.archive.org/details/TheNaturalEconomicOrder.

Godschalk, Hugo (2006): Streitfall Regionalwährungen. *Zeitschrift für Sozialökonomie*, 43(149):26–28. http://www.sozialoekonomie-online.de/ZfSO-149_Godschalk-Streitfall.pdf.

Goldman, David (2012): Google's Schmidt: Tech is widening gap between rich and poor. *CNN Money*. http://money.cnn.com/2012/02/28/technology/google_future_of_internet/index.htm, datum per se 28. Feb. 2012.

Gothill, Eli (2011): Bitcoin and Fractional Reserve Banking. *Webisteme - Thoughts on the Future of Money*. http://www.webisteme.com/blog/?p=192, datum per se 2. Apr. 2011.

GoWest (2011): GoldMoney is No Longer... Money. *The Bitcoin Trader*. http://www.thebitcointrader.com/2011/12/goldmoney-is-no-longer-money.html, datum per se 20. Dec. 2011.

GoWest (2012): Bitcoin's Liquidity: A Third Look. *The Bitcoin Trader*. http://www.thebitcointrader.com/2012/05/bitcoins-liquidity-third-look.html, datum per se 26. May. 2012.

Greco, Thomas (2001): *Money: Understanding and Creating Alternatives to Legal Tender*. Chelsea Green.

Güring, Philipp and Ian Grigg (2011): Bitcoin & Gresham's Law - the economic inevitability of Collapse. http://iang.org/papers/BitcoinBreachesGreshamsLaw.pdf.

Hamacher, Kay and Stefan Katzenbeisser (2011): Bitcoin - An Analysis [28C3]. *YouTube*. http://www.youtube.com/watch?v=-FaQNPCqG58, datum per se 29. Dec. 2011.

Hearn, Mike (2012): The future of Bitcoin and rebuilding the financial system. http://www.youtube.com/watch?v=CUP38679mxY&feature=youtube_gdata_player. *Bitcoin Conference 2012 London*, datum per se 15. Sep. 2012.

Hoppe, Hans-Hermann (1994): How Is Fiat Money Possible?–or, the Devolution of Money and Credit. *The Review of Austrian Economics*, 7(2):49–74. http://mises.org/journals/rae/pdf/rae7_2_3.pdf.

Hoppe, Hans-Hermann (1996): Banking, Nation States, and International Politics: A Sociological Reconstruction of the Present Order. *Review of Austrian Economics*, Vol 4(No 1):p. 55–87. http://mises.org/journals/rae/pdf/RAE4_1_3.pdf.

Hoppe, Hans-Hermann; Walter E. Block; and Jörg Guido Hülsmann (1998): Against Fiduciary Media. *Quarterly Journal of Austrian Economics*, 1(1):19–50. https://mises.org/journals/qjae/pdf/Qjae1_1_2.PDF.

jahabdank (2011): BitCoin and Silver: silver is store of value, BitCoin is 21st century medium of exchange. http://www.youtube.com/watch?v=E_4wqNLE5TY&feature=youtube_gdata_player, datum per se 12. Jun. 2011.

Karame, Ghassan O.; Elli Androulaki; and Srdjan Capkun (2012): *Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin*. Tech. Rep. 248. http://eprint.iacr.org/2012/248.

Kinsella, N. Stephan and Patrick Tinsley (2004): Causation and Aggression. *Quarterly Journal of Austrian Economics*, 7(4):7. http://mises.org/journals/qjae/pdf/qjae7_4_7.pdf.

Krugman, Paul (2010): What Is Money? *Paul Krugman Blog*. http://krugman.blogs.nytimes.com/2010/12/15/what-is-money/, datum per se 15. Dec. 2010.

Krugman, Paul R. (1980): Vehicle Currencies And the Structure Of International Exchange. *Journal of Money, Credit and Banking*, 12(3):513–526. http://www.nber.org/papers/w0333.

Krugman, Paul R. (1984): *The International Role of the Dollar: Theory and Prospect*. NBER chapters, National Bureau of Economic Research, Inc. http://ideas.repec.org/h/nbr/nberch/6838.html.

Krüger, Malte (2001): Offshore E-Money Issuers and Monetary Policy. *First Monday*, 6(10). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/894/803, datum per se 1. Oct. 2001.

Krüger, Malte and Hugo Godschalk (1998): Herausforderung des bestehenden Geldsystems im Zuge seiner Digitalisierung - Chancen für Innovationen? *TA-Datenbank-Nachrichten*, 7. Jahrgang(Nr. 2):8–14. http://www.itas.fzk.de/deu/tadn/tadn298/krgo298a.htm.

Ladd, Watson (2012): Blind Signatures for Bitcoin Transaction Anonymity. http://wbl.github.com/bitcoinanon.pdf, datum per se 4. Mar. 2012.

Levy-Yeyati, Eduardo (2004): *Financial Dollarization: Evaluating the consequences*. Econometric Society 2004 Latin American Meetings 184, Econometric Society. http://ideas.repec.org/p/ecm/latm04/184.html.

Matonis, Jon (2011): Why Are Libertarians Against Bitcoin? *The Monetary Future*. http://themonetaryfuture.blogspot.ie/2011/06/why-are-libertarians-against-bitcoin.html, datum per se 26. Jun. 2011.

Matonis, Jon (2012a): Bitcoin Prevents Monetary Tyranny. *Forbes (Blog)*. http://www.forbes.com/sites/jonmatonis/2012/10/04/bitcoin-prevents-monetary-tyranny/, datum per se 4. Oct. 2012.

Matonis, Jon (2012b): Brainwallet: The Ultimate in Mobile Money. *Forbes (Blog)*. http://www.forbes.com/sites/jonmatonis/2012/03/12/brainwallet-the-ultimate-in-mobile-money/, datum per se 12. Mar. 2012.

Menger, Carl (1871): *Principles of Economics*. Ludwig von Mises Institute, online [2004] edn. http://mises.org/etexts/menger/principles.asp.

Menger, Carl (1892): *On the Origins of Money*. Ludwig von Mises Institute, online [2009] edn. http://mises.org/resources/4984.

Mises, Ludwig von (1912): *The Theory of Money and Credit*. Ludwig von Mises Institute, online edition [2010] corresponding to 1953 yale university press edn. http://mises.org/resources/194.

Mises, Ludwig von (1999): *Human Action*. Ludwig von Mises Institute, online [1999] edn. http://mises.org/document/3250/Human-Action.

mndrix (2011): Bitcoin: Gold of the Future. *Mndrix (Blog)*. http://mndrix.blogspot.ie/2011/11/bitcoin-gold-of-future.html, datum per se 8. Nov. 2011.

Mt.Gox (2011): Fee schedule. https://mtgox.com/fee-schedule. *Mt.Gox website*, datum per se 1. Dec. 2011.

Murphy, Robert P. (2012): Robert Murphy Responds to Reddit Ask Me Anything. http://www.youtube.com/watch?v=wyUNdzLwte4&feature=youtube_gdata_player, datum per se 18. Feb. 2012.

NewLibertyStandard (2009): 2009 Exchange Rate. *NewLibertyStandard*. http://newlibertystandard.wetpaint.com/page/2009+Exchange+Rate.

North, Gary (2011): *Mises on Money*. Ludwig von Mises Institute, epub edn. http://mises.org/resources/6772.

Pattison, Melissa L. (2011): Buying into Bitcoin: An Austrian Analysis of the Virtual Currency's Sustainability. http://www2.gcc.edu/dept/econ/ASSC/Papers%202012/Buying%20into%20Bitcoin.pdf, datum per se 14. Dec. 2011.

Reid, Fergal and Martin Harrigan (2011): An Analysis of Anonymity in the Bitcoin System. *arXiv:1107.4524*. http://arxiv.org/abs/1107.4524, datum per se 22. Jul. 2011.

Rosenfeld, Meni (2011): Analysis of Bitcoin Pooled Mining Reward Systems. *arXiv:1112.4980*. http://arxiv.org/abs/1112.4980, datum per se 21. Dec. 2011.

Rothbard, Murray N. (2004): *Man, Economy, and State (with Power and Market)*. Ludwig von Mises Institute, online edn. http://mises.org/rothbard/mes.asp.

Rothbard, Murray N. (2005): *The Case for a 100 Percent Gold Dollar - Murray N. Rothbard - Mises Daily*. Ludwig von Mises Institute. http://mises.org/daily/1829.

Rothbard, Murray N. (2011): *Economic Controversies*. Ludwig von Mises Institute, online edn. http://mises.org/resources/6301.

RowIT Ltd (2012): Bitcoin Peer to Peer Network Status. http://bitcoinstatus.rowit.co.uk/, datum per se 7. Nov. 2012.

Salerno, Joseph T. (2010): *Money, Sound and Unsound*. Ludwig von Mises Institute, online edn. http://mises.org/document/5827.

Schlichter, Detlev S. (2011): *Paper Money Collapse: The Folly of Elastic Money and the Coming Monetary Breakdown*. Wiley, 1st edn.

Schlichter, Detlev S. (2012a): The death of banks – and the future of money. *Paper Money Collapse*. http://papermoneycollapse.com/2012/06/the-death-of-banks-and-the-future-of-money/, datum per se 20. Jun. 2012.

Schlichter, Detlev S. (2012b): What gives money value, and is fractional-reserve banking fraud? *Paper Money Collapse*. http://papermoneycollapse.com/2012/03/what-gives-money-value-and-is-fractional-reserve-banking-fraud/, datum per se 19. Mar. 2012.

Selgin, George A. (1988): *The Theory of Free Banking: Money Supply under Competitive Note Issue*. Lanham, MD.: Rowman & Littlefield. http://oll.libertyfund.org/?option=com_staticxt&staticfile=show.php%3Ftitle=2307.

Selgin, George A. (1997): *Less than Zero: The Case for a Falling Price Level in a Growing Economy*. Institute of Economic Affairs. http://mises.org/document/5301/Less-than-Zero-The-Case-for-a-Falling-Price-Level-in-a-Growing-Economy.

Selgin, George A. (2012): Quasi-Commodity Money. http://ssrn.com/abstract=2000118. *SSRN eLibrary*.

Smiling Dave (2012): Bitcoin and the Numbers Game, Part 2, in Which we Shew that Bitcoin has Never, Not even Once, been used as a Medium of Exchange. *Smiling Dave's Blog of Psychology, Economics, and Gentle Sarcasm*. http://smilingdavesblog.wordpress.com/2012/10/07/bitcoin-and-the-numbers-game-part-2-in-which-we-shew-that-bitcoin-has-never-not-even-onc datum per se 7. Oct. 2012.

Spekulatius (2012): New Indicator: Number of sites accepting bitcoin. *Bitcoin Forum*. https://bitcointalk.org/index.php?topic=35083.0, datum per se 18. Jun. 2012.

Suede, Michael (2011a): Could The State Exist If Property Rights Were Impossible To Violate? *Libertarian News*. http://www.libertariannews.org/2011/07/01/could-the-state-exist-if-property-rights-were-impossible-to-violate/, datum per se 1. Jul. 2011.

Suede, Michael (2011b): Why Do People Want A Gold Standard When History Shows Us It Does Not Last? *Libertarian News*. http://www.libertariannews.org/2011/12/01/why-do-people-want-a-gold-standard-when-history-shows-us-it-does-not-last/, datum per se 1. Dec. 2011.

Suede, Michael (2012): Fractional Reserve Banking With Bitcoins. *Libertarian News*. http://www.libertariannews.org/2012/03/09/fractional-reserve-banking-with-bitcoins/, datum per se 9. Mar. 2012.

Taaki, Amir (2012): Sex and the Bitcoin | Bitcoin Media. *Bitcoin Media*. http://bitcoinmedia.com/sex-and-the-bitcoin/, datum per se 29. Apr. 2012.

Tanaka, Tatsuo (1996): Possible Economic Consqeuences of Digital Cash. *First Monday*, 1(2). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/474/830, datum per se 5. Aug. 1996.

The Economist (2012): Bitcoin: Monetarists Anonymous. *The Economist*, p. 73. http://www.economist.com/node/21563752, datum per se 29. Sep. 2012.

The Publications Office of the European Union (2000): Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions. *EUR-Lex*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046%:EN:HTML, datum per se 18. Sep. 2000.

Thornton, Mark (1991): *The Economics of Prohibition*. Univ of Utah Pr (T). http://mises.org/resources/913/Economics-of-Prohibition-The.

Unknown (2012): History - Bitcoin. *Bitcoin Wiki*. https://en.bitcoin.it/wiki/History, datum per se 31. Oct. 2012.

Various (2012): Redeemable Codes Bypass International Banking System. *Bitcoin Money*. http://www.bitcoinmoney.com/post/18506669111/redeemable-code-bypass, datum per se 29. Feb. 2012.

Vernengo, Matias (2012): Hyperinflation in Bitcoinland. *Naked Keynesianism*. http://nakedkeynesianism.blogspot.ie/2012/01/hyperinflation-in-bitcoinland.html, datum per se 1. Jan. 2012.

WalletBit (2012): Pricing and Fees. *WalletBit website*. https://walletbit.com/pricing, datum per se 21. Oct. 2012.

Wehinger, Gert D. (1997): Bargeldinnovationen und ihre geldpolitieschen Konsequenzen. *Berichte und Studien*, 1:p. 60–76.

White, Lawrence H. (1984): Competitive Payments Systems and the Unit of Account. *The American Economic Review*, 74(4):699–712. http://www.jstor.org/stable/1805134.

Woodford, Michael (2000): Monetary Policy in a World Without Money. *National Bureau of Economic Research Working Paper Series*, No. 7853. http://www.nber.org/papers/w7853.

Yeager, Leland B. (2001): The Perils of Base Money. *The Review of Austrian Economics*, 14(4):251–266. http://www.gmu.edu/depts/rae/archives/VOL14_4_2001/2_yeager.pdf.