Why Bitcoins Have Value, and Why Governments Are Sceptical

Torbjørn Bull Jenssen

Master's thesis

Economic Theory and Econometrics

Department of Economics

University of Oslo

May 14th 2014

Why Bitcoins Have Value, and Why Governments Are Sceptical

A Master's thesis by Torbjørn Bull Jenssen

-Economic Theory and Econometrics-

Department of Economics, University of Oslo

May 14th 2014

2014

Why Bitcoin Have Value and Why Governments are Sceptical

Torbjørn Bull Jenssen

http://www.duo.uio.no/

Trykk: Reprosentralen, Universitetet i Oslo

Abstract

The aim of this thesis is to provide a holistic analysis and an economic understanding of Bitcoin, answering two key questions:

(i) *Why do bitcoins have value?*
(ii) *Why and how will governments seek to regulate the use of bitcoin?*

To answer these questions, the thesis begins with a discussion of money itself, developing a framework of different types of monies in terms of their uses and properties that will form the basis of the analysis. Based on the technical properties of Bitcoin the framework developed above is then applied to identify bitcoin as a digital commodity money. Following this identification, potential uses of bitcoin supporting its value will be discussed, drawing particular attention to Bitcoin's resilience to regulation. In addition, real world examples of other commodity monies will be used to support the claim that bitcoin may circulate without use value and state backing. Governments tend to seek economic control through controlling money, and it will be argued that there are good reasons to expect governments to be hostile towards widespread use of bitcoin. This is to be expected, as use of bitcoin undermines governments' capacity to control money.

Acknowledgements

Without the assistance and support from all the people around me, writing this thesis would have been very tough. I would especially like to thank my supervisor Nina Larsson Midthjell and prof. Costas Lapavitsas for valuable feedback and guidance. I am also grateful for the help from my good friend Oisin J. Zimmermann, and for the scholarship granted by "Professorship in Macro and Monetary Policy Issues". Finally, I would like to thank my family and fellow students for general backing and for being patient listeners.

Table of contents

1 Introduction 1
1.1 Investigating Bitcoin from an economic perspective 2
1.2 The aims of this thesis 3
2 What is money? 4
2.1 Moneyness 5
2.2 The importance of transaction costs 6
2.3 Different relations, different monies 8
2.3.1 Commodity money 8
2.3.2 Fiat money 9
2.3.3 Credit money 10
2.3.4 Electronic money – the realm of Bitcoin 11
2.4 The institutional underpinning of different money forms. 13
2.4.1 The importance of trust 14
3 What is Bitcoin? 16
3.1 How to transfer bitcoins? 16
3.1.1 The transaction chain 18
3.1.2 Double spending 19
3.1.3 The block chain 19
3.2 The bitcoin supply 21
3.3 Pseudonymity and user defined anonymity 21
3.4 Colouring; non-monetary use of bitcoins 22
3.5 Bitcoin; a digital commodity money 23
3.5.1 Moneyness of bitcoin 24
4 Real world examples of commodity money 26
4.1 The stones of Yap 26
4.2 Somali Shilling 27
4.3 Iraqi-Swiss Dinar 29
5 Solving real world problems; Bitcoin and current transaction costs 31
6 What is a bitcoin worth? 35
6.1 Bitcoin as a flow 35
6.2 Bitcoin as a stock 37

7 Bitcoin and the government 41
7.1 Current regulation 41
7.2 Neo-classical market failures 44
7.3 The realpolitik of money and Bitcoin 46
7.3.1 Demonetisation of gold 46
7.3.2 The desire to regulate Bitcoin 48
8 Concluding remarks 51
Bibliography 53
Appendix A 60

1 Introduction

"*Our own money, the money we have grown up with, the system under which it is controlled, these appear "real and "rational" to us. The money of other countries often seems to us like paper or worthless metal, even when the purchasing power of individual units is high*."

(Friedman, 1991, p. 5)

In October 2008, a research paper by Nakamoto (2008)[1] was spread through a cryptography mailing list,[2] describing a new kind of payments system, with a unit called bitcoin at its core. What happened next was nothing short of astounding.

In less than a year the Internet community, working essentially pro bono and cooperating across multiple jurisdictions, took the protocol outlined in the paper and created what we know today as the Bitcoin network. Starting from these very humble beginnings, essentially creating something out of nothing, the Bitcoin network grew at an exponential rate to gain a present day market capitalization between six and five billion USD,[3] consisting of more than two and a half million unique users,[4] and attracting almost 100 million USD in venture capital investments (CoinDesk, 2014).

The emergence of this new payments system has sparked a slew of negative reaction from prominent economists, governments and central banks. Allan Greenspan, Paul Krugman, and Nouriel Roubini have argued respectively that bitcoin is a bubble, evil, and a Ponzi scheme. [5] ECB,[6] Banque de France,[7] Peoples bank of China,[8] and even the U.S. SEC[9] have issued warnings to their citizens, outlining the dangers of getting involved in the system. Some countries like Russia[10] and Thailand[11] have also almost banned it.

---

[1] Nakamoto has remained anonymous to date, and there could be a group behind the pseudonym.
[2] http://www.metzdowd.com/
[3] Accessed May 8th, 2014: https://blockchain.info/charts/market-cap
[4] Estimated March 2012 by Adi & Dorit (2013)
[5] Kearns (2013), Krugman (2013), Holm (2014)
[6] (European Central Bank, 2012)
[7] http://www.telegraph.co.uk/finance/currency/10497427/French-central-bank-warns-against-using-bitcoin.html
[8] http://online.wsj.com/news/articles/SB10001424052702304655304579547251552490962?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052702304655304579547251552490962.html
[9] http://investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments#.U23gJfmSy3T
[10] http://www.reuters.com/article/2014/02/09/us-russia-bitcoin-idUSBREA1806620140209
[11] http://www.telegraph.co.uk/finance/currency/10210022/Bitcoins-banned-in-Thailand.html

The lady doth protest too much, methinks.[12]

At the same time, Larry Summers thinks: "*Bitcoin has the potential to be a very, very important development",* [13] and Ben Bernanke said in a letter to congress: "*that there are areas in which digital currencies may hold long-term promise*".[14]

How did this happen? Why is the reaction from government authorities predominantly vitriolic, while still largely lacking consensus? Indeed, how can something created out of nothing have or obtain such value? These are the central questions of this thesis, questions which strike at the heart of what money is, how we value it, and what it means.

1.1 Investigating Bitcoin from an economic perspective

In order to analyse Bitcoin as an economist, it is of paramount importance to follow Mises (1935 [1881]) in the sense that Bitcoin should be investigated in terms of what it does and what it can do as an economic phenomenon, not as defined by lawmakers or computer scientists.

In general, economic theory can be understood as the study of resource allocation, and a substantial part of the academic work has been devoted to the study of "the efficient allocation", as in Koopmans (1951). Transactions, on the other hand, have received less focus from many dominant schools of thought, potentially explaining why complex institutions like money have received so little attention from many academics. To understand Bitcoin as an economic phenomenon it is therefore necessary to draw on a variety of theories emphasising the importance of transactions and payment.

"*Payment is more than a mechanical act. It is, in a sense, the quintessential economic activity, the "glue" that binds together the gains from trade*" (Kahn & Roberds, 2009).

[12] A quote from Shakespeare's play, Hamlet, used as a figure of speech to capture the ironic situation when a person's intense attempts to convince others about something ends up convincing them that the opposite is true, as the person looks insincere and defensive. Source: Wikipedia: http://en.wikipedia.org/wiki/The_lady_doth_protest_too_much,_methinks. Accessed May 13th 2014.
[13] Davidson & Lee (2014)
[14] U.S. Department of Homeland Security (2013)

1.2 The aims of this thesis

This thesis will provide a holistic analysis of Bitcoin, taking into account multiple schools of economic thought, historical facts, and political and social relations. The motivating questions of this thesis are:

(i) *Why do bitcoins have value*?
(ii) *Why and how will governments seek to regulate the use of bitcoin?*

With a comprehensive analytical framework in place, the thesis seeks to answer these questions, providing not only an economic understanding of Bitcoin, but also offering compelling insight into that fascinating and often neglected social construct: money.

The remaining sections of the thesis are organised as follows. Section 2 presents a theoretical framework apt to categorise and analyse different forms of money. Section 3 involves a discussion of what Bitcoin actually is, describing the underlying technology to clarify its essential properties. Applying this to the theoretical framework outlined above, bitcoin becomes identified as a digital commodity money. Section 4 lays out three cases in which an object without use value, or state backing, served historically as money. Section 5 highlights some real world applications of bitcoin. Section 4 and 5 work together to emphasise a fundamental contention of this thesis; there is no reason why bitcoin should not be seen as money. Accepting this contention, the determination of demand, and thereby prices, is addressed in section 6, before section 7 rounds off by analysing why governments might seek to regulate the use of bitcoin. Section 8 summarises the analysis and contains some concluding remarks on the subject as a whole.

2 What is money?

Economists tend to identify money by its three key functions: store of value, medium of exchange and unit of account (Mishkin, 1993). While this identification provides a clear definition of what money does, the question of what actually makes something money is rarely addressed in a satisfactory manner by mainstream economics. The framework of neo-classical theory is based on the frictionless world of Arrow-Debreu, where complete contracts can be written at no cost. Within such a framework, money is redundant, as anything could serve as money, and money's role is reduced to that of a numéraire. Furthermore, the New-Keynesian models, applied to model monetary economics without money, clearly illustrates that it is insufficient to tweak the neo-classical framework by adding some frictions to capture the nature of money. Payments are ubiquitous and obviously essential to real-world economics (Kahn & Roberds, 2009, p. 2). Therefore, in many situations, transactions ought to be made the basic unit of analysis, as advocated by Williamson (1985).

While mainstream economics today is very light on the analysis of money, alternative schools of thought and great thinkers throughout history have sought to uncover the origin and nature of money; a study that may result in "Babylonian Madness".[15] This has led to the development of an enormously rich and diverse literature on the subject.[16] Nevertheless, there seems to be no broad consensus surrounding the role of money in the economy. This shall come as no surprise, as "*Money is privately possessed but socially consumed*" (Lapavitsas, 2003, p. 49), making money reflect the complexity and dynamics of human relations.

The theoretical framework suggested in this thesis which follows below is a synthesis of several distinct approaches, and seeks to highlight some of the social aspects of money. To this end, the characteristics of transaction costs, giving rise to different types of money, intermediating different kinds of relationships, will be investigated.

[15] In the 1920's, Keynes spent five or six years studying metrology and numismatics in search for the historical and logical origins of money. The search absorbed him to the point of frenzy, and he himself refers to this as his "Babylonian Madness" (Ingham, 2000, p. 16).

[16] "*Of all branches of economic science, that part which relates to money and credit has probably the longest history and the most extensive literature*" (Robbins, 1953, p. 11)

2.1 Moneyness

In monetary economics, assets are normally divided into money (if money is included at all) and non-money. While this dichotomous way to analyse monetary phenomena is rigid and has some advantages, the sharp division between money and non-money obscures the economic processes at work, thus making it difficult to capture how market forces actually react to financial constraints. For money to be money, it must be the most sought after asset, i.e. the most liquid asset available. In other words, merchants absorbed with self-gain, must find it desirable to sell their product for the money-asset (Lapavitsas, 2003).

The tacit consent from market participants, that others will exchange the current form of money for actual goods in the future, effectively renders money a general claim on production. The self-reinforcing network effects underpinning such a consent has a monopolising effect, making money the only asset with the ability to buy (Lapavitsas, 2003). All assets may be used for exchange. However, when using a non-monetary asset, one will have to discount its (market) value to enable such exchange. All assets therefore possess a degree of moneyness, measured as the inverse of the discount necessary to get it to facilitate exchange. [17] The moneyness of an asset clearly depends on what market one operates in and from whom one is trying to buy. As a result, the moneyness of different assets is determined in a simultaneous fashion by supply and demand, and will react endogenously to changing market conditions.

Once it is understood that money is not an *either or* concept, it becomes clear that one must investigate the processes through which assets acquire moneyness to uncover the dynamics of money in the economy. For that reason, different approaches to analyse money effectively seek to answer the question of what it is that makes certain assets liquid.

In Chartalist theory, the focal point of analysis is on money as a unit of account. As the unit of account, money is used to establish *nonreciprocal obligations* in the form of debt and taxes. When all money is identified as a form of debt, the Chartalist conclusion that the obligation underpins the moneyness of a given asset naturally follow. In theoretical Metallism on the other hand, the main focus is on money as a store of value. For an object to store value, it must hold value in itself. With a commodity standard, this value is seen as derived from the

[17] In finance, moneyness is used as a measure of the price of an underlying asset relative to the strike price of a derivative contract written over said asset. This interpretation of the term should not be confused with its use in this thesis.

value of the money as a commodity. Thus, the moneyness of a given commodity is primarily assumed to be determined by its ability to store value, in a *non-social* manner, by being useful in itself. In the Austrian approach associated with Carl Menger and Ludwig von Mises, money as the medium of exchange is analysed as the characteristic from which money's other capabilities are derived. As a medium of exchange, established by network effects and learning, money is practically viewed as a form of delayed *reciprocity*.

The different approaches to money analysis may seem contradictory and mutually exclusive. However, it is my contention that the theories are more complementary than contradictory. They identify different social relations; non-reciprocal, non-social, and reciprocal, related to the functions of money as the exclusive drivers of moneyness. Yet, they fail to appreciate the simultaneity of these relations. By taking the arguments to the extreme, the theories end up analysing particular structures of economic organisation intermediated by particular forms of money. The theories gain clarity and precision by restricting the system under investigation, but by doing so lose generality. Therefore, a more general analysis of money, drawing on insights from the different theories, is presented below to provide a framework for the identification of Bitcoin.

2.2 The importance of transaction costs

Consider an economy populated with agents seeking to maximise their utility given their individual preferences, resource endowment and production technology. With a weighting of all agents, society's welfare level can be calculated as a weighted sum of all individuals' utilities. Since any particular allocation will correspond to particular utility levels, allocations may be ordered hierarchical, following the Pareto Principle.

Transaction costs affect interaction between agents, and the higher the cost the lower the welfare level. When transaction costs are so high that no exchange take place, agents live in autarky and society is at its lowest welfare level. Transaction costs drive a wedge between individuals' marginal rates of substitution (MRS), and potential welfare gains from reducing this wedge may be substantial. Hence, when transaction costs are high, [18] the willingness to pay for a workaround will be correspondingly high. This willingness to pay manifests itself as

[18] Transaction costs could e.g. be measured indirectly as the wedge between MRSs.

a rent available to any organisation or participants of an institutional arrangement overcoming the transaction costs.

In a broad sense, transaction costs are the costs of running the economic system (Arrow, 1969), and more precisely, the costs of enforcing and operating property rights. In a game theoretic framework, transaction costs can be identified as the *cost of coordination*, the *cost of containing free riding*, and the *cost of conflict and distribution*. By assuming that preferences are independent of transaction costs, all allocation effects of the existence of money may in theory be analysed, using the lens of transaction cost economics.

Transaction costs are the result of both physical and social barriers. Although physical barriers may have effects on social organisation and visa verse, it seems plausible to assume that technology is mostly developed to overcome physical barriers, while institutions[19] develop to reduce social barriers. If better infrastructure (in this context understood as technology) was built, agents may be enabled to meet and engage in direct barter. The reduced transaction costs will expand the set of possible allocations, and an economy with direct barter will Pareto-dominate an economy in autarky. Nevertheless, there will still be substantial transaction costs due to incomplete contracting. Barter does not scale[20] and the problem of "double coincidence of wants" will keep the economy from reaching potential welfare maximum.

The three functionalistic characteristics of money may be linked to the three aforementioned categories of transaction costs. First, as a general medium of exchange, money lowers the cost of coordination by eliminating the problem of double coincidence of wants. Second, as a store of value, money only provides purchasing power to its holder and thereby reduces the cost of containing free riding. Third, money as a unit of account (and universal measure of value), reduce the difficulty of agreeing to a certain distributional outcome, and thereby lowers the cost of conflict.

To investigate how different forms of money may develop and affect transaction costs, it would be fruitful to analyse a hypothetical scenario in which welfare maximum is achieved. To this end, one can think of the economy as provided with a perfect public record, or as in

[19] Institutions can be defined as *"humanly devised constraints that structure political, economic and social interaction"* (North, 1991, p. 97).
[20] Without a numéraire, the number of prices/exchange ratios at a market grows exponentially with the number of goods for sale.

Kocherlakota (1998) "memory". If all agents could keep a true record of what all other agents had done, the set of incentive feasible allocations would Pareto-dominate any other set (ibid.). The organisation of market production could be modelled as a game of iterated prisoner's dilemma, and optimising agents would follow a tit-for-tat strategy. Production would be "given" to the market, and agents would only take back something worth the same as what they "gave". Furthermore, if an agent brings something back before he has contributed, society will hold a record of that, and demand that the agent bring something of equal value to the market at a later point in time. Agents defecting, taking more than what they give, will be identified and punished (e.g. excluded from further participation, as in Diamond (1990)). This ensures that cooperation remains the dominant strategy.

In reality, however, no flawless public record exist. Agents defecting cannot be identified (at no cost) and excluded. Thus, the game of iterated prisoner's dilemma will collapse into a succession of static games. The dominant strategy will be for everyone to defect in each period, since one cannot know whether an agent was cooperating or not. Therefore, without a public record, the economy falls back into direct barter.

To move on from direct barter, institutions substituting for a perfect public record must be developed. Money can be analysed as such an institution, operating indirectly as a record, acquiring credibility by being a "Proof of Work" (POW). Not necessarily because agents care about the sunk cost of work from the past, but because the required work makes it costly to alter "the record".

2.3 Different relations, different monies

2.3.1 Commodity money

In a commodity monetary system (CMS), a good that is costly (as in not free) to produce, may serve as a POW. As an example, one can think of gold. There are only two ways to acquire gold: (i) Working in the mines, or (ii) working somewhere else and take your product to market to be paid in gold. In a capitalist economy with gold as money, the price of goods must equal the ratio of the work required in goods production to that of gold production (on

average over time). [21] Otherwise, the return to investment would not be equal in all industries, and no profit-seeking agents would invest in the lower-yielding industry. This relationship is structural and simultaneous, so that no one-way causality can be inferred. In other words, the value of a commodity money is equal to its production cost (over time), but the cost and the value are variables that are normally codetermined. One does not determine the other. In theory, with relative stable production costs in the economy, this link will keep prices stable and ensure that gold is credible as an indirect public record.

The adoption of any particular commodity as money will hinge on characteristics of the commodity, such as how easy it is to identify, divide and store. Agents' ability to identify a commodity should be increasing in its use as medium of exchange. When more agents become familiar with "money", demand will become less sensitive to idiosyncratic shocks. It is important to notice that identification in this context is to be understood as the ability to predict future demand for the money commodity.

Mises' regression theorem assumes backward-looking expectations, and explains very well the network effects that make something money to day, because it was money yesterday. However, unlike the claim in Austrian economics, money does not need to originate in an object with use value, a good that enters agent's utility functions or can be used as an input in production. Instead, a leap of faith (trigger strategy), initiated by agents with forward-looking expectations, could serve as well as any use value, as an endpoint to the Misesian regression. As an example of this, Duffy and Ochs (2002) showed that in experiments simulating the economic environment of Kiyotaki & Wright (1989) a good with sufficiently low storage cost might emerge as the general medium of exchange, without use value and state backing. It is the work required in the production of the money commodity that makes it valuable and a trustworthy record of the past. Any additional use value will only serve as a hedge against situations where the recording capacity of the commodity money is lost, i.e. when the tit-for-tat strategy is abounded.

2.3.2 Fiat money

A CMS expands the incentive-feasible allocation set and Pareto-dominates direct barer. Still, using commodity money is an expensive way to produce money because of the associated

[21] Assuming perfect competition or monopoly modelled with price considerations and non-diversifiable risk as a part of the cost structure.

resource cost. If "the social planner" could step down and provide creditable POWs to those taking their goods to market, there would be no need to waist resources in the gold mines. The only way to obtain money, and thereby the cheapest way to obtain other goods, would be to bring one's production to the social planner. As under a CMS, the work required to obtain money is what makes it credible as a record keeping device. The resource cost under a CMS signifies a rent, stimulating the emergence of institutions that can provide trust at a lower cost, and thereby make a profit from tapping down this rent through seignorage. Hence, without a trusted social planner, a credible state, could serve as a fictitious "gold mine" by requiring work in exchange for a money token. Prices denominated in state money would, as under a CMS, be determined by the ratio of required work in production to the work required to obtain the money from the state. When a state issuing money also accepts the same money in discharge of taxes, the states flexibility in spending is increased. The state may to a greater extent change the difficulty to obtain money, without degrading the money's purchasing power.

Although new fiat money in theory could enter the economy through government spending, it is worth bearing in mind that most countries operate under an institutional structure where money issuance goes through the central bank (CB). Hence, fiat money is created in a credit way, through an expansion of the CB's balance sheet. Even so, fiat money is not proper credit money, as it is a claim on nothing, but itself, and the stylised analysis of fiat money above, should still hold.

2.3.3 Credit money

In a system with fiat money, the resource cost of a CMS is overcome, and accrues to the money issuing authority in the form of seignorage. Still, to cover the full set of incentive-feasible allocations in the economy with a perfect record, it must be possible to take something back from market before you produce. Not only governments, but also private agents, must be enabled to undertake autonomous spending. If the social planner could know the future with certainty, he could let agents issue private debt without any risk. Debt, a promise to work, would then be equivalent to a POW from the future. Furthermore, as debt creation always is a two-sided balance sheet operation, a risk-free IOU would be a promise to work for the creditor, and POW to the debtor. The only way to obtain another agent's IOU would be by working. As with commodity and fiat money, the value of an IOU would be

regulated by the work required to obtain it. Hence, truly risk free IOUs will circulate as money; an observation found in much of the literature on money and credit (e.g. as in Shubik (2004)), but following a slightly different line of argument.

In reality, however, promises to work are not generally risk free. Incomplete contracting makes IOUs circulate at a discount due to the cost of obtaining private information from the issuer (Kiyotaki & Moore, 2000). Private IOUs have some degree of moneyness, but are not money. This difference between the face value and market value of private IOUs creates a rent, incentivising the emergence of institutions capable to extract private information at a lower cost than the market. The key institution emerging to do this has been banks. By exploiting increasing returns to monitoring and diversification, banks are able to issue IOUs circulating with a higher degree of moneyness than the assets they obtain, thus making a profit from the difference. In fact, bank deposits tend to circulate at face value, i.e. as money, letting banks earn a form of seignorage from crating new money through lending. According to standard literature on banking, banks are institutions emerging because they are efficient, acting as maturity transformers and intermediaries between borrowers and lenders (Freixas & Rochet, 2008). Although banks serve these functions, it is essential to understand that they only exist to make a profit, and that the profit is made from the difference in moneyness between assets and liabilities.

2.3.4 Electronic money – the realm of Bitcoin

With the development of personal computers and the Internet, money has immigrated into the digital world. As in the non-digital world, electronic money (e-money) comes in many different forms. Since the Internet only is another medium where human relations can form, principles guiding the emergence of institutions in the non-digital world apply online as well. Hence, money on the Internet follows the same principles as money in the rest of the economy. E-money should therefore not be seen as a generic form of money. In fact, in many cases, e-money is just a digital representation of normal credit or fiat money. However, the emergence of online societies, as within computer games, have resulted in the development of what the ECB calls Virtual Currency Schemes (VCS) (European Central Bank, 2012). VCSs bear some similarities to e-money, but is purely a digital representation of itself, not other monies.

In the report (ibid.), ECB classifies three different categories of VCSs based on how the flows between the currencies and the rest of the economy operates. First, there are closed systems such as those that can be found in computer games like World of Warcraft. Second, there are systems with unidirectional flows, where "normal" money can be converted into non-redeemable tokens. Third, there are bidirectional flows as associated with the Linden Dollars issued in Second Life. With bidirectional flows, agents are free to trade in and out of their position in the VCS. As a result, effects on the real economy caused by changes in category three VCSs is potentially greater than from changes in category one and two VCSs.

Bitcoin is put in the third category together with Linden Dollars because of the bidirectional flow of funds. Yet, there is a fundamental difference between Bitcoin (and alt-coins[22]) and other VCSs. As will be clear from the analysis of Bitcoin in this thesis, bitcoins are no one's liability and there is no centralised monetary authority in the Bitcoin network. This is a crucial difference, making bitcoins a potential form of electronic cash (e-cash). Anticipating the development of e-cash, as opposed to centralised e-money, the economist Milton Friedman argued in an interview in 1999 that:

"…the internet is going to be one of the major forces for reducing the role of government, and the one thing that is missing, but that will soon be developed, is a reliable e-cash. A method where by, on the internet, you can transfer funds from A to B without A knowing B or B knowing A. The way I can take a 20-dollar bill and hand it over to you…" (NTU/F, 1999).

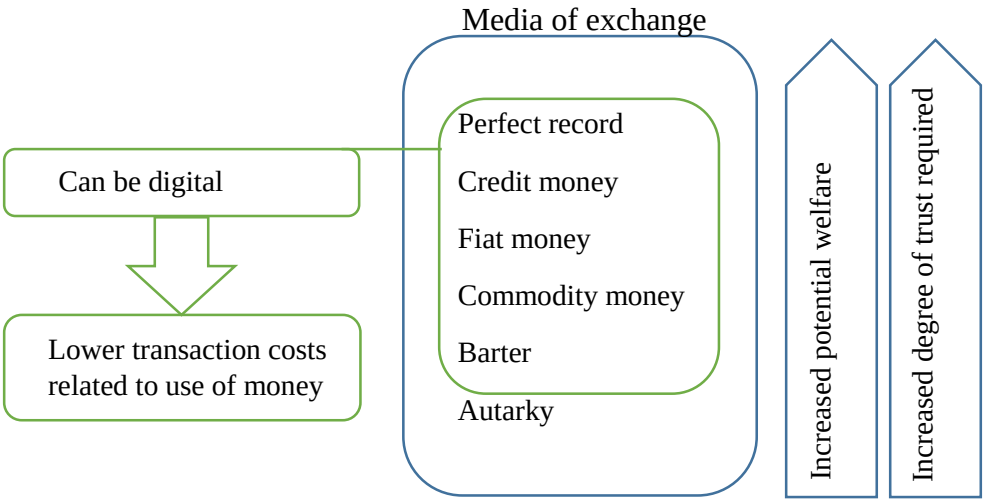
Before Bitcoin, all forms of e-money and VCS were centralised, impeding them from becoming e-cash.

[22] Alt-coin is as a general term capturing all the different "currencies" based on the Bitcoin technology.

2.4 The institutional underpinning of different money forms.

If credit money is more efficient than fiat money, which in turn is more efficient than commodity money, and e-money is just an electronic representation of other forms of money, as highlighted by figure 1 below, the natural question to ask is why all the money forms presented in section 2.3 are in operation. Moreover, why would anyone use assets with moneyness rather than money?[23]

Figure 1 – Hierarchy of money



The figure illustrates a hierarchical ordering of different generic forms of money based on potential welfare and degree of trust required.

When addressing the questions above, it is important to bear in mind that for a single agent, the cost of using a particular money-form is independent of the cost to the society. This claim holds as long as the agent cannot produce the money himself. However, in many situations, agents can in fact create their own money. This is because money is money only relative to a market, and not any market in general.

As argued in Coase (1937), Alchain and Demsetz (1972), and Williamson (1985), firms emerge as organisations economising on different transaction costs. In a market, monetary prices serves as the main organising principle. Within a firm, on the other hand, internal bookkeeping and centralised planning are applied to overcome the transaction costs of using

[23] To answer these questions thoroughly is beyond the scope of this thesis. Consequently, the following paragraphs only provide a simple sketch, indicating some possible elements of what could become a more comprehensive analysis.

money, thus rendering money as a record device superfluous. In other words, a "perfect record" is normally used for intra-firm organisation of production. Furthermore, high frequency of interaction between economic agents tend to lead to the formation of credit relations (Jin & Temzelides, 2004). As a result, trade credit may circulate within a production chain due to mutual dependence and a high level of knowledge about counterparties, which establish trust. This supports the circulation of credit within the chain, making production chains relay on credit money for inter-firm organisation. Yet, trade credit from a particular production chain normally only poses a degree of moneyness, and is not money relative to the rest of the economy.

Within the borders of the nation state, the government tends to be the single most important economic agent, with monopoly of violence and the ability to impose taxes. Fiat money may therefore circulate as money at a national level, supported by trust in the stability of monetary policy, and the compulsion of juridical regulation and taxes.

For international settlements, no national currency was trusted without commodity backing up until 1971. A national fiat currency without commodity backing can be used to manipulate international wealth distribution by inflating away debt, or appreciating claims through deflating the currency. Nevertheless, the US position as the absolute hegemon in the West after the fall of Bretton Woods enabled the USD to fulfil the role as the fiat money of the world.

2.4.1 The importance of trust

As indicated in the examples above, and illustrated by figure 1, the organisation of production and the selection of a particular form of money will hinge on the cost-benefit trade-off of trusting the record keeping capacity of that money. The level of trust will be determined by the cost of defection from implicit or explicit established strategies and the opportunity cost of not trusting. Shubik (2004) uses a game theoretic approach, highlighting the relationships between money and trust to argue that an ideal money would serve a perfect substitute for trust. Yet, in reality, the more efficient a money is, the more trust it requires, and the use of an ideal money would be a manifestation of trust rather than a substitute within the framework of this thesis.

Both in autarky and with direct barter, no trust is required. In a CMS, one has to trust that the market as a whole will continue to accept the money commodity as payment in the future, and that the cost of production keeps inflation stable. As long as the cost of trusting the CMS is less than the benefit of participation, in expectation, agents will find it beneficial to cooperate within the framework of a monetary economy. In addition, positive network effects will increase the benefit and reduce the cost as the network expands.

In a fiat monetary system, the credibility of CB monetary policy combined with the compulsion of tax generates trust in the government issued money enabling it to substitute for commodity money. To establish trust in monetary policy is much harder than establishing trust in the cost of e.g. gold production. Governments have incentives, and political considerations may lead to manipulation of fiat money through changing the difficulty to obtain money. A gold mine, on the other hand, does not poses the ability to manipulate the cost of gold production at will. Nonetheless, the increased power of the state, achieved through the control of money, may reinforce its general capacities, including money creation.

With the use of credit money, trust is shifted from the network as a whole to trust in individual debtors. Hence, to enable trust in a single agent, the anonymity inherent to other money forms must be sacrificed. Relying on credit relations consequently impose higher informational and enforcement costs (Kahn & Roberds, 2009, p. 19), and credit money can only function in a market where it is expensive to default and agents are willing to give up privacy.

3 What is Bitcoin?

Before setting out to analyse Bitcoin as an economic phenomenon, it is important to possess a comprehensive understanding of the technology.[24] At is core, Bitcoin is just a digital public ledger used to enforce and operate private property rights of the virtual unit bitcoin.[25] To operate entries in the ledger, one must use software scripted to work with the Bitcoin protocol. The Bitcoin protocol, like HTML for webpages, regulates how peers in the network can interact. In other words, the protocol function as an ineluctable law book governing the network. The Bitcoin protocol is open source and freely available to everyone with access to the Internet. The main purpose of the protocol is to enable people to transfer electronic cash directly between each other in a decentralised peer-to-peer (P2P) network. Traditionally, trusted third parties, such as banks, have operated most payment systems, enabling complete strangers to interact economically through the exchange of IOU's, with claims on assets or national fiat currencies. The Bitcoin protocol, on the other hand, is designed so that no trusted third party is needed to secure and verify transactions of the virtual unit known as bitcoin. Solving this well known "Byzantine Generals' Problem" is seen as the protocol's crowning achievement. As will be argued later, decentralised clearing is what makes Bitcoin as a digital payment scheme unique and interesting.

3.1 How to transfer bitcoins?

If Alice (a peer in the network) wants to transfer some bitcoins to Bob (another peer in the network), all she has to do is to broadcast a message like "send 10 bitcoins from Alice to Bob", to the network. The nodes[26] receiving the message will update their copy of the ledger and pass along the transaction message. To make sure the request of sending 10 bitcoins from Alice to Bob is authentic; a "Digital Signing Scheme" is used. To spend money belonging to an account, a pair of keys, one private and one public, is needed. Actually, in the Bitcoin

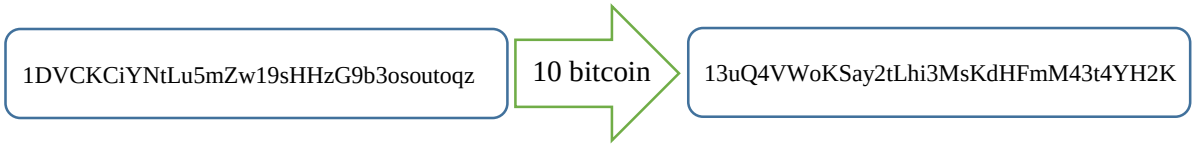
[24] This technical overview is based on knowledge acquired through reading about Bitcoin online on forums and in blogs. Consequently, it is difficult to reference this section properly. For a comprehensive explanation of Bitcoin, see Ramzan (2013).

[25] Bitcoin (upper case B) defines the technology and the network, while bitcoin (lower case b) defines the virtual units transferred within the network.

[26] A node is any computer participating in the work of maintaining the ledger. Every node is also a peer, but not every peer is a node.

Network the public keys are the “accounts” so a transaction from Alice to Bob would look more like:

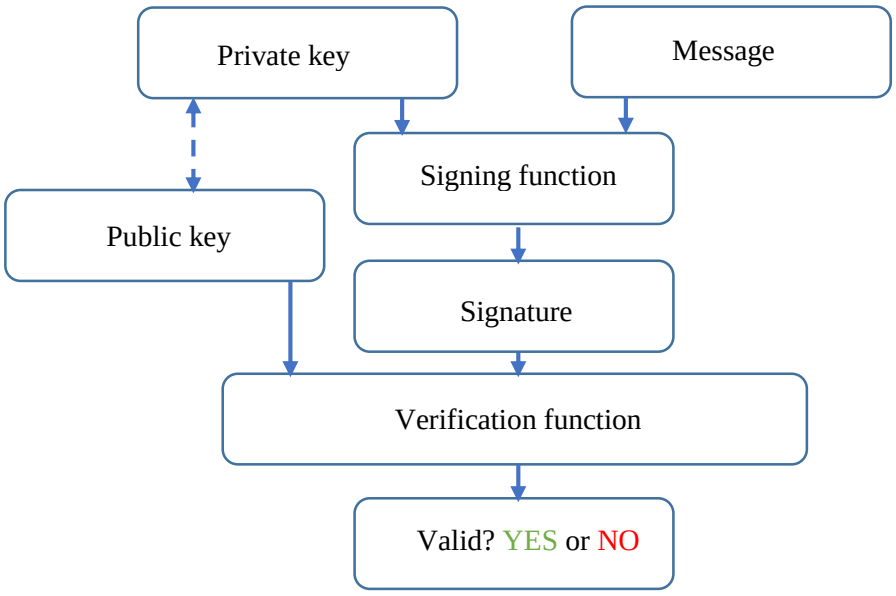
Figure 2 – Bitcoin transaction



An example of real addresses/keys that is used when transferring bitcoins.

The pair of keys associated with an “account” are obviously different, but generated in a way so they are mathematically related. When the private key and the transaction message are combined in some mathematical function, a unique signature is generated. To verify this signature, and thereby the validity of the transaction request from Alice to Bob, the signature is put into a verification function together with the message and Alice’s public key. The relationship between the private and the public key makes it possible to conclude whether Alice’s private key was used to generate the signature or not, without ever knowing Alice’s private key, as illustrated in figure 3 below.

Figure 3 – Digital Signature Scheme



Simplified illustration of how a Digital Signature Scheme works.

Since verification of transactions requires verification of signatures, the uniqueness of signatures is an important feature in the Bitcoin protocol, making sure that signatures cannot

be copied and reused by others. Moreover, as a result of the fact that the message is tied to the signature, past transactions cannot be changed without invalidating the signature.

Hence, when sending bitcoins to someone's address/public key, it is like using a drop-safe that only a person holding the right private key can open. While it normally is the case that only one signature/key is needed to unlock the funds, arrangements that are more complex, are possible. As an example, two out of three signatures could be required for an escrow-based transaction.

3.1.1 The transaction chain

As described above, digital signatures are used to verify transactions. Although this is true, the presentation was over-simplified, as there are no records of accounts and balances in the network. Instead, the network stores the transaction history of all bitcoins ever created. The ownership of funds is therefore validated through the verification of links to previous transactions. Hence, to own bitcoins constitutes a situation in which bitcoins are directed towards you, without you redirecting them towards someone else. When Alice wants to send 10 bitcoins to Bob, she has to reference both transactions where she received at least 10 bitcoins, and the new recipients of those funds, when generating the signature.

The incoming transactions to Alice are called "inputs", while the new transactions are called "outputs". Unless the referenced inputs sum exactly to 10 bitcoins, Alice will have to send the rest of the funds back to herself as change (assuming no transaction fee). To verify these new transactions, nodes will have to check that the inputs actually belong to Alice and that they add up to the sum of the outputs. To make the ownership of bitcoins definite, verified transactions are irreversible.

The validity of any transaction of bitcoins always depend on the whole chain of transactions with those bitcoins leading up to the current transaction. To make sure the last transaction is valid, the whole chain needs to be verified. This process of going through all past transactions is both time and energy consuming, but needs to be done only once. The first time you start your Bitcoin wallet software; the whole transaction chain of all bitcoins is downloaded and checked. [27] Thereafter, only new transactions need to be verified.

[27] In many cases, users will use a wallet provider and interact with the network through an app. It is therefore not necessary for users to verify the transaction record themselves.

As mentioned earlier, the Bitcoin protocol is open source, and anyone is free to write their own software and claim conditions compatible with the protocol. However, should you end up doing mistakes when scripting, or lose your private key, your bitcoins may be lost forever. For this reason, it is natural to assume that most users will want to use software and services delivered by third parties to minimise the risk of losses.

3.1.2 Double spending

An input can only be referenced and used once. Had this not been the case, inputs could be double-spent by referencing it in multiple transactions. Therefore, nodes also check that none of the referenced inputs in a transaction has been referenced earlier in some other transaction. This check is made rapidly by the use of an index of unspent transactions. Nevertheless, there is a problem; how can one verify the order of transactions? If the same input is referenced twice, the network must be able to verify which reference was made first. In a centralised system, like PayPal, this is easily done as every transaction is recorded on a centralised server. In the Bitcoin network, however, nodes may receive transactions at different points in time and in different order. This would potentially allow Alice to send bitcoins to Bob, wait for Bob to ship a product, and then send another transaction, referencing the same input. A situation could then emerge where the transaction to Bob was registered after the other transaction, and therefore ended up being deemed invalid. To solve this problem, the Bitcoin protocol uses a "Proof of Work" (POW) scheme to create what is called a "Distributed Timestamp Server" (Nakamoto, 2008).

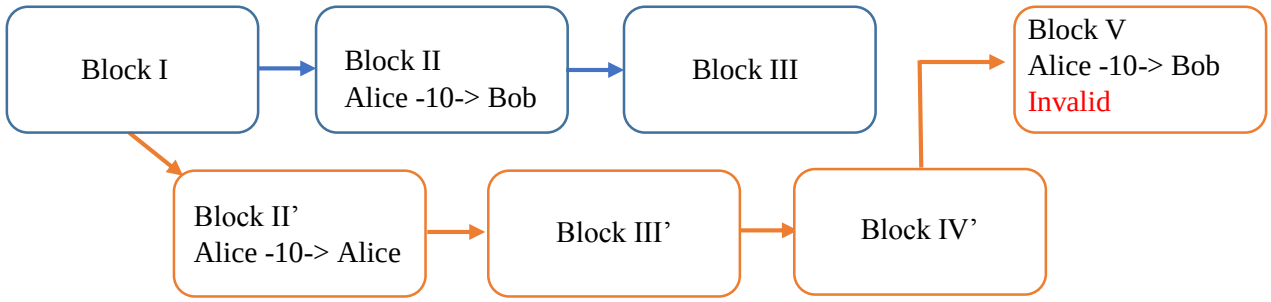
3.1.3 The block chain

When transactions are broadcast to the network, nodes collect unverified transactions and pack them into blocks. Every new block has a reference to the previous block, resulting in an ordered succession of blocks (Nakamoto, 2008). It is important to notice that the block chain is not the same as the transaction chain. The block chain is used to order transactions in time, while the transaction chain is used to keep track of the changes in ownership. All transactions within a block are considered to have happened at the same time, while transactions not yet in a block are unconfirmed. All nodes in the network are free to collect unconfirmed transactions into a block, and suggest to the network what the next block should be. To create a new block, a mathematical problem must be solved by guessing. Hence, the name POW (work as in letting a computer use computing capacity and energy to guess). Although one can be lucky

and guess the solution at the first trial, it will take the network around ten minutes on average to come up with the solution (ibid.). The time it takes to generate a new block is regulated by the protocol, and was chosen arbitrarily. To keep up with the growth of computing power in the network, the system recalibrates the difficulty of the mathematical problem every two weeks. Once a block is created, it is broadcasted to the network, which accepts it and starts working on the next block. However, should two blocks be created and broadcasted simultaneously, the block chain would be divided into two branches. When a bifurcation of the block chain occurs, the nodes keep building atop of the first block they receive. The next block that is solved will make one of the branches longer than the other, and the system switches automatically to build further on the longest branch. Blocks are rarely created at the same time, and more rarely multiple times in a row. As a result, a consensus of the ordering of blocks quickly emerges, and the older the block, the less likely it is to change. The transactions in the blocks that are discarded after a split of the block chain will go back into the pool of unverified transactions and be included in a later block.

A problem with the possibility that the block chain may be divided for some time, is that it opens another opportunity to double-spend, illustrated in figure 4 below. Imagine a situation in which Alice first transfer 10 bitcoins to Bob, and Bob ships the product when he sees that the transaction is verified and included in a block. Then, Alice starts building an alternative chain of blocks in secrecy, including a transaction of the same 10 bitcoins to someone else, instead of Bob. When she broadcasts the alternative chain to the network, it will replace the other chain if it is longer. Bobs payment, that was a part of the other chain, will be thrown back into the pool of unverified transactions. When nodes later try to verify the transaction of 10 bitcoins from Alice to Bob, they will conclude that the transaction is invalid, as Alice has used the referenced inputs already in the other transaction.

Figure 4 – Bifurcated block chain and double spending



The figure illustrates how Alice in theory could double spend bitcoins by generating an alternative block chain.

However, Alice would not be able to pre-generate an alternative block chain as she would need the latest block as reference when generating new blocks. Once she has broadcasted the transaction of 10 bitcoins to Bob, she therefore has to outperform the computing power of the whole network. When Alice commands less than 50% of the total computing power of the system, the probability that she ever catches up with the correct chain drops exponentially with the number of blocks (Nakamoto, 2008), and the longer Bob waits before he ships the product, the more secure the transfer will be. Waiting six blocks (one hour) should be sufficient for most larger transactions. In addition, if Alice were to control too much computing power in the network, using this to game the system, she would undermine the value of her bitcoins, as agents would lose trust in the ledger. Hence, if Alice were a profit maximising agent, she would either reduce her computing capacity voluntarily, or credibly commit to not gaming the system.

3.2 The bitcoin supply

When all new transactions of bitcoins need to reference past transactions, a natural question emerges; where did the bitcoins initially come from? When a new block in the chain is created, an amount of bitcoins is created ex nihilo, and credited to the finder of the block. Nodes use computing hardware and electricity to get these rewards, which is the reason why they often are called miners. Every fourth year the reward is halved, implying that there never will exist more than approximately 21 million bitcoins (Nakamoto, 2008). However, since bitcoins in theory are infinitely divisible (currently down to a satoshi, 10^{-8}-part of a bitcoin), the hard cap of 21 million does not limit the lower value of transfers in the network.

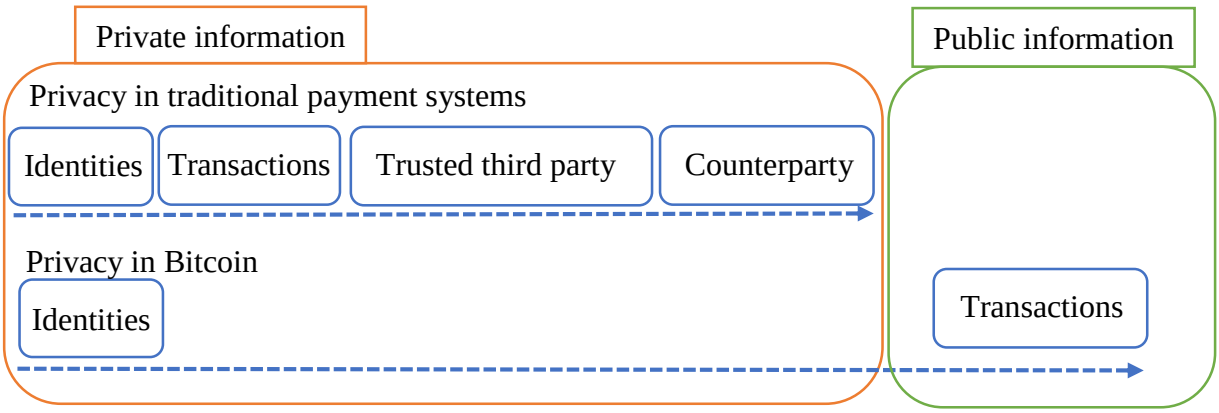
Once the reward from mining is too small to cover the cost, miners will have to be incentivised by transaction fees. Nodes are free to choose which transactions to include in a block, so specifying a fee as a part of your transaction is likely to increase the speed of verification, while competition between nodes is likely to result in fees close to (a very low) marginal cost (of verification).

3.3 Pseudonymity and user defined anonymity

One of the strengths of Bitcoin, highlighted by its proponents, is the way in which privacy is preserved. In many ways bitcoins are like a digital version of cash; bitcoins can be transferred

directly to a receiver who then can verify the validity of the transaction, neither knowing the payer, nor engaging a trusted third party. In other electronic payment systems, privacy has been achieved through keeping information held by financial intermediaries private/unavailable to the public, as showed in figure 5 below. One consequence of this is that it is almost impossible to monitor bank activity properly. Moreover, the centrally stored private information makes a favoured target for hacking, identity theft, and government surveillance. In the Bitcoin network, on the other hand, all information about transactions is public, while privacy is ensured through keeping the identities of the transactors pseudonymous (see figure 5 below).

Figure 5 – Privacy in payment systems



The figure illustrates different ways privacy is ensured in traditional payment systems and in Bitcoin.

Nothing in the protocol requires linking your identity to your public key, and it is up to the user to reveal real information about himself. For those less keen on revealing their identity, different techniques can be applied to make it very difficult to track ownership of bitcoins. As an example, using methods to hide your IP, new addresses/keys for every transaction, and bitcoin tumblers, [28] will make tracking very difficult.

3.4 Colouring; non-monetary use of bitcoins

While most attention surrounding Bitcoin has been on its monetary capacities, a public record can be used for much more than performing payments. By attaching a message to a transaction, not only the transaction, but also the message becomes publicly verifiable. This

[28] Tumblers seek to make tracking of bitcoin ownership as difficult as possible. One can think of it as several users putting bitcoins in a jar, shaking it, and taking out the same amount coins as they putted in.

capacity could for example ease the exchange of legal contracts such as ownership certificates and prevent fraud. By "colouring" a bitcoin with a claim on some asset, the bitcoin will, in addition to be a bitcoin, serve as a representation of the asset on which it has become a claim. Hence, Bitcoin can be used to transfer the ownership of any asset as long as the relevant parties of an exchange recognise claims coloured/written on a bitcoin. In addition, Bitcoin can be used to provide "Proofs of Existence". By hashing[29] a document, e.g. the coding of a new app, and then including the hash in a transaction, it is possible to prove that the code was in the hands of the person performing the transaction, at a given point in time. This could be useful when solving disputes related to the ownership of intellectual property.

This section has outlined the main technical features of Bitcoin, and there should be no doubt that technically, Bitcoin is an impressive innovation. Being a technically impressive, however, does not imply that Bitcoin will have economic consequences. Therefore, to address the economic side of Bitcoin, an identification of bitcoin as an economic object will be presented in the following section.

3.5 Bitcoin; a digital commodity money

To identify what a bitcoin is as an economic object, it is useful to start by listing what it is not. Bitcoin is neither a consumption good, nor a means of production. Hence, its function must be inherently social. When testing bitcoin against the theoretical framework to analyse money presented earlier in the thesis, it is clear that bitcoin is not; a perfect public record, a form of credit, or a form of fiat money. Bitcoin as a ledger actually does serve as a public record. [30] However, without the colouring of every single bitcoin, the record only keeps track of bitcoin balances, and is therefore only an indirect representation of underlying economic transactions. Moreover, bitcoins can hardly be claimed to be someone's liability or issued and backed by any state. Therefore, if bitcoin is some form of money, it must be a commodity money. To see that it actually is, or at least that it has the potential to become, a digital commodity money, or what Selgin (2013) calls a synthetic commodity money, let us compare bitcoin to commodity money in general.

[29] Hash functions are functions mapping data of arbitrary length to data of fixed length.
[30] Luther and Olson (2013), identify Bitcoin as an imperfect form of "memory" complementing traditional currencies.

As with other commodity monies, there are only two ways to obtain bitcoins; (i) using computing capacity and electricity to "mine", or (ii) produce something else and sell the product for bitcoins/ buy bitcoins using other monies. Since bitcoins do not have any use value, bitcoins have acquired exchange value through the belief that bitcoins would hold value at a point in the future. Without use value as a starting point, which some commodity monies have, forward-looking agents must have followed a trigger strategy when assigning a positive value to bitcoin. This observation clearly falsifies the Misesian regression theorem by being an example of exchange value acquired without an initial anchor in use value. However, not all agents need to be forward-looking. The current positive valuation of bitcoin may serve as a reference point for agents with backward-looking expectation formation, thus intensifying the growth of the network through a feedback loop.

Since the selection of a particular commodity as money by the market hinges on the characteristics of the commodity, it is illuminating to highlight some relevant characteristics of bitcoins. First, since the ledger in Bitcoin is decentralised, it is extremely resilient to interference and outside regulation, be it governments seeking to confiscate bitcoins or agents wanting to change the predetermined bitcoin supply. Second, bitcoins are easy to store. For example, a tiny piece of paper or just a person's memory can store any quantity of bitcoins, without the bitcoins deteriorating over time.[31] This makes bitcoins very easy to keep safe, and as stated earlier: low storage cost together with limited supply can be sufficient to ensure circulation of objects without use value, like bitcoin, as media of exchange (Duffy & Ochs, 2002). Third, to transfer bitcoins is a quick and simple task. A receiver knows exactly what he received, and the irreversibility of transactions makes ownership definite. Fourth, bitcoins are (in theory) perfectly divisible so quantities of any size can be transferred. Fifth, the pseudonymity element of Bitcoin makes surveillance and identity tracking through money flows difficult.

3.5.1 Moneyness of bitcoin

Bitcoins can be traded for other currencies 24/7 on online exchanges, and should be relatively liquid. However, the current exchanges are small and new, and high transaction costs have limited interexchange arbitrage trading (Yermack, 2014). Derivative contracts written over

[31] Remember that to store bitcoins only requires storing the keys.

bitcoins have to date been almost non-existent,[32] and short selling has been almost impossible. The market price of bitcoins have therefore varied substantially between different exchanges (ibid.), and determining a price to use as a reference to measure the moneyness of bitcoins is not trivial. Nevertheless, for the purpose of this thesis it is unnecessary to quantify bitcoins' moneyness. More and more merchants accept bitcoin as a form of payment, either directly or more often indirectly via services such as BitPay and Coinbase. In addition, bitcoin can be used to buy gift cards, expanding the number of products that can be obtained by bitcoins even further. Because of the volatile bitcoin exchange rate against other currencies, prices tend to be denominated in some other unit of account with continuously updating bitcoin prices. Still, when using bitcoins, they are more or less accepted at par. [33] On the one hand, this would suggest that bitcoin is traded at a zero discount, rendering it money. On the other hand, bitcoins are only money amongst the limited amount of agents accepting it as a form of payment. While this number of agents is growing rapidly, most economic agents, like your local super market, would not accept bitcoins at any discount, thus making bitcoin's moneyness for that purpose zero. Over time, the contractual constrains underpinning the high transaction costs of shifting in and out of bitcoin is likely to be reduced as more serious financial actors enter the market. [34] Moreover, as long as intermediation in bitcoin transfers remains cheap, bitcoin even do not have to become the unit of account to acquire moneyness in a greater set of markets. Instead, bitcoin could be used solely as the medium of exchange and a store of value. Agents not wanting to hold bitcoin will then either have the opportunity to liquidate their positions consecutively on exchanges, enter offsetting financial contracts written over bitcoin, or let third parties absorb the exchange risk.

[32] The development of derivative contracts seem to gain traction with actors as Tera setting up standards for bitcoin swaps (Stafford, 2014).
[33] The fee when using services like BitPay and Coinbase is currently between zero and one percent according to the homepages of the companies.
[34] This, of course, only holds if governments do not try to stop the development and use of Bitcoin.

4 Real world examples of commodity money

The aim of this section is to provide examples of commodity monies lending support to the claim that bitcoin may function as a digital commodity money, without use value and state backing. A quick investigation of the price history of gold clearly suggests that changes in the value of gold are relatively independent of consumption and industrial demand. Instead, gold prices seem to have been driven by the sentiments of financial markets and government intervention (Shafiee & Topsal, 2010). Gold is just a:

"..metal dug from deep in the ground, refined at great labour, and transported great distances to be buried again in elaborate vaults deep in the ground." (Friedman, 1991, p. 5).

It is not produced to be consumed. It is produced to be stored as a manifestation of wealth, a POW. This indicates that a commodity actually may obtain exchange value independent of its use value. In fact, gold's long history as a form of money clearly illustrates that when acquiring moneyness, commodities may be traded permanently above use value. Nevertheless, many still argue that the element of use value inherent to gold, often labelled intrinsic value, is important to support its exchange value without state backing. To challenge this statement, three monetary cases will be presented briefly below.

4.1 The stones of Yap

In the South Pacific, a small group of islands called Yap have attracted attention by economists because of their somewhat extraordinary form of money, the rai. Rai are giant stone wheels, used for certain exchanges, representing wealth (Bryan, 2004). Without any other value than the wealth they represent, they are a typical example of a commodity money with value derived from its network. As the material rai are made of cannot be found on Yap, rai are carved out and shipped from other islands. This was a costly process, and estimates suggest that more than 10 percent of the adult male population participated (ibid.). Because of the work required, the rai could serve as an indirect record of ones contribution on the island. The stones were not fungible. Older stones carved out with shell tools and carried by canoes were more valuable than newer stones quarried with iron tools and transported by western ships. This reflects the fact that the population of Yap ascribed primary value to the work

involved in the production of the rai. This made work, rather than the stone itself, the effective unit of account, although prices on the island were normally set in terms of a basket of consumption goods (ibid.).

While the stones had holes in the middle so they could be transported, it was a difficult task to move the bigger stones. Therefore, ownership of a stone was independent of its location, and transfers where done through communication. A famous story demonstrating this is the one presented in Friedman (1991). A particular big stone was once lost to the sea during a storm. However, since it was common knowledge that the stone laid at the bottom of the sea, the wealth it represented remained with the owner. Moreover, in the late nineteenth century when Yap was under German rule, the Germans levied taxes through marking some stones with a black X, claiming ownership over them until the tax was paid through work (ibid.).

The rai were never used for trade outside of Yap. For that, woven mattes and now dollars are the medium of exchange. Despite this, the stones are still used for some exchanges, and have retained purchasing power well relative to many fiat currencies (Bryan, 2004). The fact that the stones have maintained value, even after adoption of the dollar as the official form of money, clearly shows the strength of the network effect. As long as the social relations underpinning the value of rai remain stable, the stones should maintain their value.

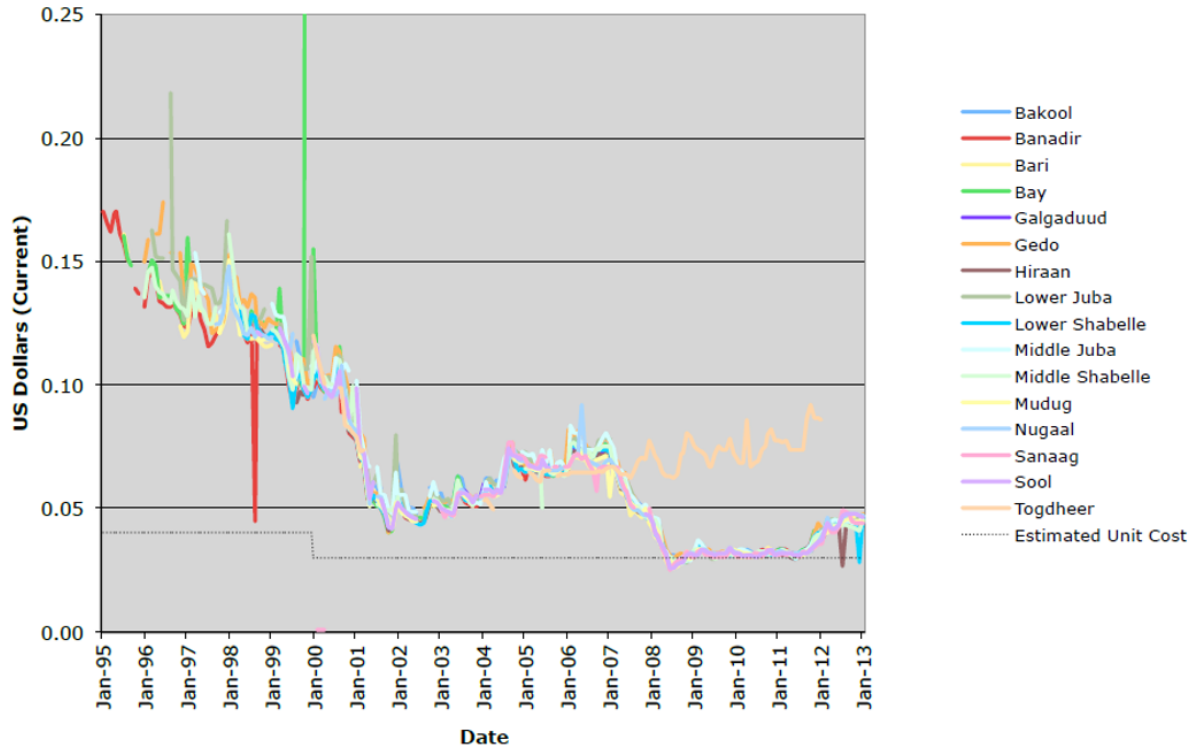
4.2 Somali Shilling

In 1991, the Somalian state collapsed, and with it, the central bank and the entire financial system. Overnight, all deposits were wiped out and money balances shrunk by 54 percent, leaving the economy with a large unsatiated demand for holding monetary balances (Mubarak, 2003). The Somali shilling, previously backed by the state and the central bank, suddenly had no formal backing. Yet, notes issued before the state collapse continued to circulate despite the lack of use value (Luther & White, 2011).

On Yap, the value of a given rai pivoted on the labour that went into producing it. However, had the stones been fungible, such as Somali shilling, it would have been impossible to separate new stones from old ones. The value of all stones would then have been regulated by the marginal cost, not the particular cost to any one stone, which is what happened in Somalia.

Without the legal framework to limit supply, different factions found it profitable to contract with foreign printers, and started to import forgeries (Luther, 2012). However, the public would only accept notes issued by the central bank before the collapse, so production was limited to remakes of the pre collapse 1000 shilling notes. Besides, since the remakes were identifiable, they were normally accepted at a 5 percent discount at infusion (Mubarak, 2003). After some time when the notes were warn, they became indistinguishable from the other notes and circulated at par with the old ones. As long as the new notes circulated above their cost of production, local leaders found it profitable to import more, and the value of the Somali shilling collapsed from 0.30 USD in 1991 to 0.03 USD in 2008 (Luther, 2012). However, as can be seen in figure 6 below, the prices stabilised from 2008, and real money balances even started growing (Luther, 2012).

Figure 6 – Somali shilling exchange rate



The figure shows the exchange rate of 1000 Somali shilling on different markets *Source: (Luther, 2012)*

The Somali shilling transformed from a fiat money to a commodity money valued at its marginal cost of production, circulating without proper state backing for more than 20 years. Somalis would not accept other notes than those pretending to be issued before the collapse. With a fixed marginal cost of production, the value of the Somali shilling became regulated by the printing and transport costs as more zeroes could not be added to the notes.

4.3 Iraqi-Swiss Dinar

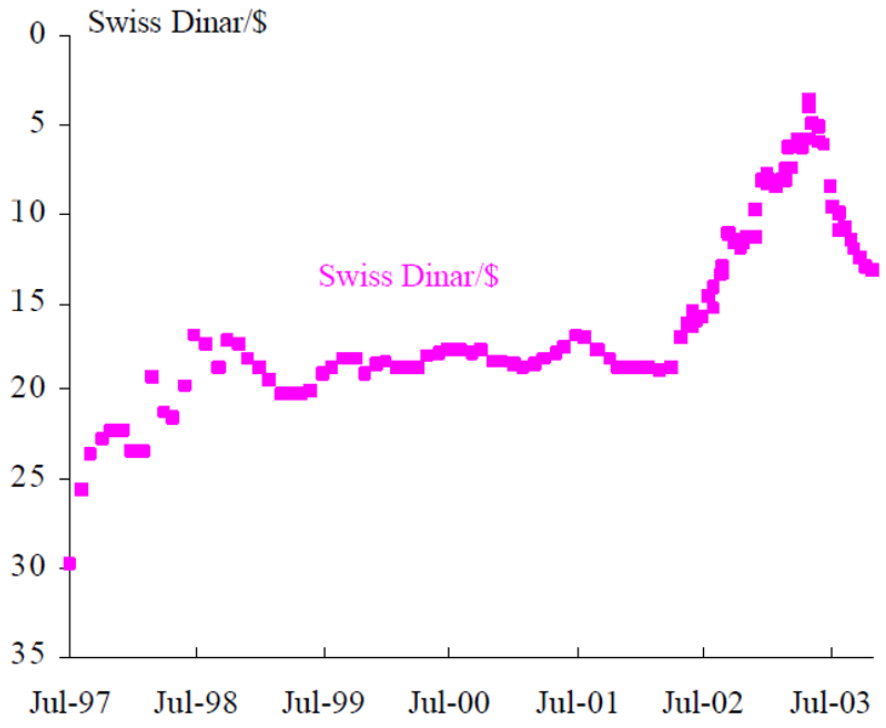
In the early 1990's, the U.S. initiated a trade embargo on Iraq. The government could no longer import foreign printed currency, and in 1993, Saddam withdrew the old 25-dinar notes, called Swiss dinars, from circulation, to replace them with a new locally printed "Saddam" dinar (King, 2004). Residents living in the northern Kurdish controlled part of Iraq were excluded from exchanging their old notes. As a result, Saddam dinars did not circulate in the north, and the Swiss dinar continued to serve as money despite being demonetised by the Iraqi government.

"*Whatever gave the Swiss dinar its value was not the promise of the official Iraqi government, or indeed any other government*" (ibid. p.13).

In both the cases discussed above, the supply of money was elastic and regulated by costs of production, providing an anchor for prices. However, as this example highlights, a completely inelastic money, without use value can also survive without state backing. No Swiss dinars were printed after 1989, implying that the base money supply of Swiss dinars became fixed. [35] While the Saddam dinar was of low quality and depreciated due to forgeries and excessive issuance, the Swiss dinar preserved its purchasing power and even appreciated against the dollar, as can be seen in figure 7 below. The local government in Kurdish Iraq discussed and expressed concerns about having an uncontrolled, hoarded and appreciating currency. Yet, the Swiss dinar maintained its value. This shows how a useless object may continue to circulate and represent value without any formal backing, as long as the implicit backing by the social economic relations constituting its' network endures. [36] Since the Kurdish part of Iraq was almost completely sealed off from the rest of Iraq, the circulation of Swiss dinars did not hinge on acceptability in the southern parts of the country.

[35] Actually with notes deteriorating over time, the nominal money stock was most likely decreasing (King, 2004)
[36] King (2004) argues that the Swiss dinar maintained its value because of the expectation that a central government in the future would back the Swiss dinars in retrospect. Although, the Swiss dinars were recognised after the invasion in 2003, I do not find this argument persuasive, especially when one considers the time horizon.

Figure 7 – Swiss dinar exchange rate



The figure shows the development of the Swiss dinar – USD exchange rate. *Source: (King, 2004)*

The three examples above show that commodity money may circulate without use value and state backing, as long as private agents find it desirable to rely on the money as an indirect record; unbacked commodity money is not only a theoretical possibility, it is also a reality. This observation is essential to answer the question as to why bitcoins have value, and it undermines arguments claiming that bitcoin is a bubble that must burst; that the value of bitcoin has to go to zero. Nevertheless, observing that commodity money may circulate independent of use value and state backing does not necessitate the emergence of bitcoin as a form of money. A new form of money is only adopted by the market if it reduces some transaction costs other monies cannot. Therefore, to answer why bitcoins have value, the next section will highlight some transaction costs that might be overcome by using bitcoin.

5 Solving real world problems; Bitcoin and current transaction costs

Bitcoin as a technology was developed to provide a disruptive form of digital cash, resilient to interference from any central power. Indeed, the discussions and examples above clearly show that Bitcoin has the potential to achieve this goal. Yet, for Bitcoin to have a real and lasting effect on economic affairs, it must engender a permanent and secular shift in certain relevant transaction costs. The success of and demand for bitcoin as a currency will therefore hinge on its ability to make available gains by reducing transaction costs currently resulting in unsatiated demand. To support the contention that Bitcoin could have real economic effects, four major and related transaction costs that could be lowered by Bitcoin will be presented in the following paragraphs. [37]

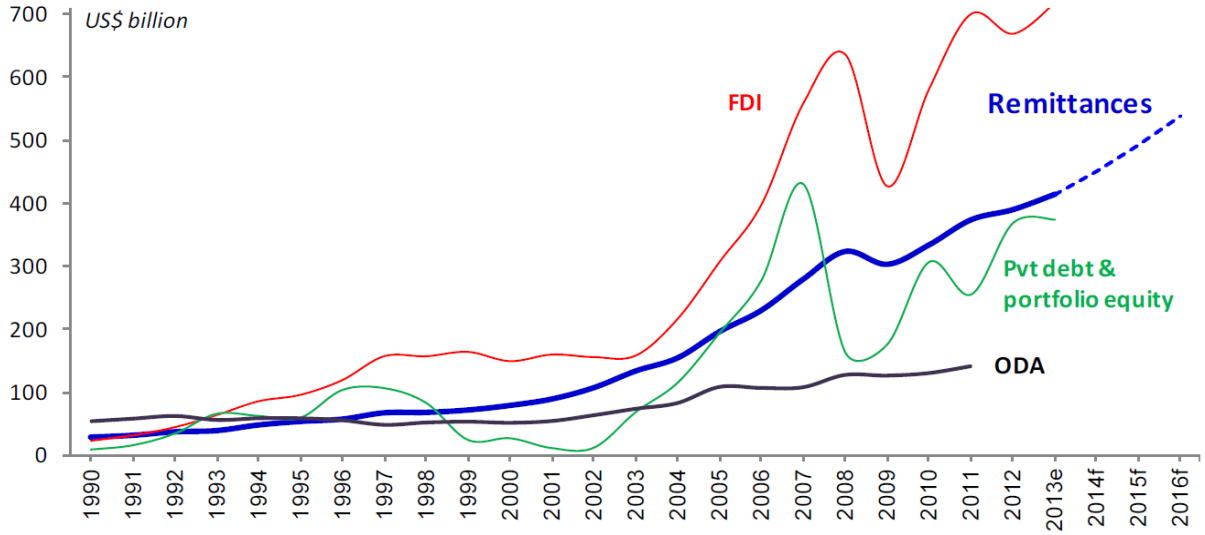
First, the emergence of the Internet has resulted in more and more services being delivered electronically. Since electronic services like programing do not suffer from physical transaction costs, the decision to hire a programmer should be independent of geographical considerations. Yet, for a Chinese programmer to program for an Argentinean firm there must be a medium through which they can facilitate payment. An international currency transfer could serve this purpose. However, it is not given that both parties have a bank account, both China and Argentina regulate flows of capital, and international wire transfers are generally slow and expensive. With an ever-growing amount of people getting access to internet services, the possibility frontier of trade expands. To fully realise the potential gains from trade, however, international money transfers must become as trivial as sending an E-mail. Bitcoins respect neither capital controls, nor monopolistic power in the money transmitting business. With its non-reversible transfers, the benefit from relying on and trusting Bitcoin could therefore potentially outweigh the cost for many agents currently excluded from international trade.

Second, in 2013, officially recorded international remittance flows were estimated to reach around 550 billion USD with an expected annual growth rate of around 8 percent from 2013 to 2016, reaching over 700 billion UDS by 2016 (World Bank, 2013). Most of these funds (estimated 414 billion USD) are flows to developing countries, making the flow of

[37] The relevant transactions identified in this thesis is not meant to be taken as an exhausting list as other transactions may be as important.

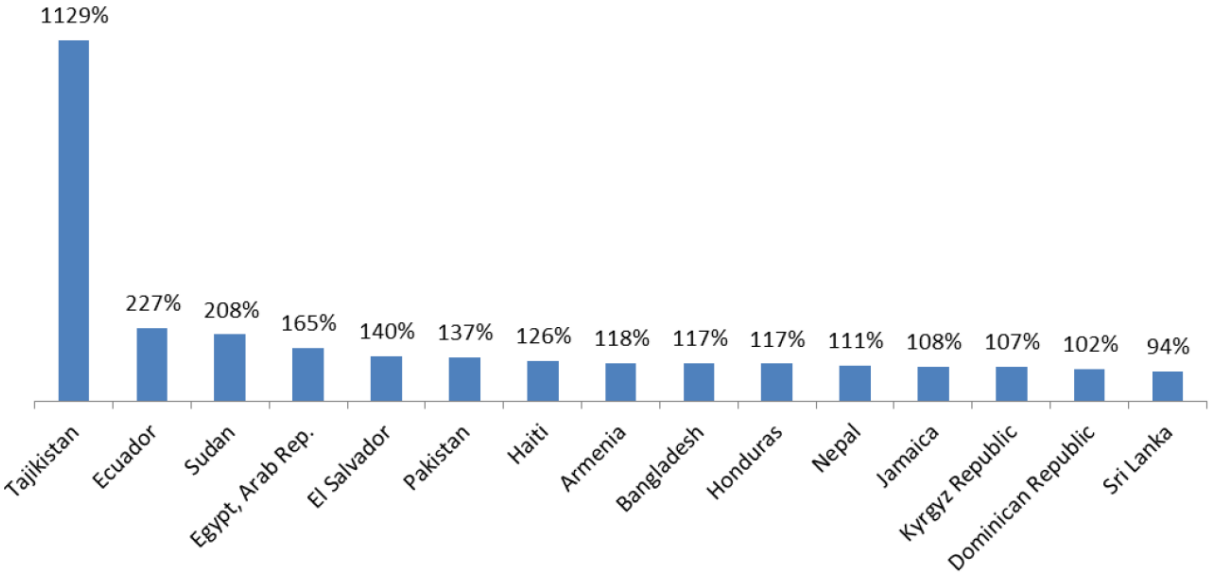
remittances to developing countries larger than both “Official Development Assistance” (ODA) and “private debt and portfolio equity flows”, as showed in the figure 8 below.

Figure 8 – money flows to developing countries.



The flows of remittances to developing countries are large and growing. *Source: (World Bank, 2013)*

Figure 9 – Remittances relative to stock of foreign reserves.



Remittances relative to foreign exchange reserves *Source: (World Bank, 2013)*

These flows are important not only for the welfare of people receiving them, but also for the overall macroeconomic situation in recipient countries. As illustrated by figure 9 above, the annual flow of remittances to several countries exceed their total stock of international reserves. The country with the highest relative inflow of remittances is Tajikistan, which received 48% of GDP in remittances in 2012 (ibid.). This indicates the relative importance of these flows for foreign exchange earnings.

When looking at the total volume of these flows and taking into account that the world average cost of sending remittances is around 9% (ibid.), it becomes clear that Bitcoin could become an important competitor to money transmitters like Western Union. Technological development should have reduced the cost of international money transfers. Yet, international banks are pulling out of developing countries, terminating the accounts of hundreds of money transmitters, because of the high costs associated with strict anti-money laundering laws and combating the financing of terrorism regulation (AML/CFT) (ibid.; Jenkins (2013)). Without the presence of international banks, it becomes almost impossible to send money through formal channels to countries like Somalia, where Barclays are pulling out as the last major bank (Goff, et al., 2013). Since the Bitcoin network is decentralised, it cannot be forced to comply with AML/CFT regulation, although intermediaries using bitcoin can. With fees close to zero for sending bitcoins, agents remitting money could benefit massively from using Bitcoin as a remittances platform. A company called Kipoch has launched an M-Pesa[38] integrated bitcoin wallet, bridging mobile phone money and bitcoins, and another company using Bitcoin, BitPesa, provides intermediated transfers charging only a 3 percent fee. Kenya is a major recipient of remittances, and with Bitcoin bridged with M-Pesa, around 17 million Kenyans[39] and around five million Tanzanians[40] suddenly received access to cheap and quick international money transfers.

Third, there is no need to look to developing countries to find transaction and entry costs leading to financially underserved people. In the U.S nearly 70 million Americans are cut off from the mainstream financial system in some way, and 8 percent are unbanked (United States Postal Service, 2014). Without being a part of the formal financial system, one has to rely on cash only. One becomes excluded from online retailing which requires digital settlement, both as a buyer and as a seller. In several U.S states, it is now legal to sell

[38] M-Pesa is the major mobile-phone money in East Africa.
[39] (Communications Comission of Kenya, 2012)
[40] (TeleGeography, 2013)

marijuana. However, the stores selling marijuana are unable to get a bank account, as the drug remains illegal by federal law, regulating the banks (Kovaleski, 2014). As a result, these stores have to deal with large amounts of cash holdings, which is both inconvenient and unsafe. To reduce these costs, some stores, according to online news articles, consider starting accepting bitcoins to be able to receive payments and save electronically.

Fourth, money transfers, even when strictly speaking legal, are currently prone to political interference/ policy imposed transaction costs. Not only in developing countries and dictatorships, but also in the western part of the world. In 2010, after releasing several classified documents, WikiLeaks fell victim of a financial blockade. Their funds were frozen, and it became impossible to use normal payment providers like, Visa, MasterCard or PayPal to donate money to the organisation, although such donations newer was illegal (Gillmor, 2011). Nonetheless, because of the centralised nature of the payments providers, it was easy to exert political pressure aimed at stopping an organisation undermining government authority.

In February 2012, a Danish police officer had 20,000 USD seized by U.S authorities according to several Danish newspapers like "the Copenhagen Post" (Stanners, 2012). He was legally purchasing Cuban cigars from Germany, but since all dollar transfers are routed through the U.S., the funds were frozen, as the transfer was seen as a violation of the U.S. trade embargo against Cuba. These two examples show how easily a centralised payment system may be controlled through imposing transaction costs politically. In addition, the requirement of attaching personal identities to one's bank account makes centralised payment systems desired targets for identity theft and government surveillance. As an example, Barclays had to start an investigation January 2014 after consumer data on 27,000 customers was stolen and sold to City brokers (Arnold, 2014).

To guard their anonymity and circumvent political regulation and control, some agents have a demand for a decentralised payment system. The technical properties of Bitcoin render it a potential satisfier of this demand by lowering the transaction costs for many kinds of regulated transfers.

6 What is a bitcoin worth?

If one accepts the discussion above, it follows that bitcoin has a role as a medium of exchange. As a result, bitcoin must also be a store of value as this is a necessity for any media of exchange (Ostroy & Starr, 1990). In other words, bitcoin has value because it is a medium of exchange, and it is a medium of exchange because private agents find it desirable to use bitcoins to overcome certain transaction costs. This answers the research question of why bitcoins have value, but begs the question of how the value is determined. The total quantity of bitcoins in the economy is regulated by the Bitcoin protocol and is exogenous to economic development. The total value, however, is endogenous and some of its determinants will be investigated in the following section. To keep the analysis as clear as possible, the bitcoin supply will be assumed to be fixed. In the long run, this assumption is true, and inclusion of the current predetermined growth will not alter the essence of the analysis.

When analysing money demand from an economic perspective, there are broadly speaking two main approaches. One is to start with the equation of exchange and analyse the flow element of money, with demand arising for transaction purposes. The other is to analyse money as a stock held in the portfolios of economic agents. The two approaches are complementary and consistent, highlighting different dynamics that determines the value of money. Therefore, to shed light on how the monetary regime imposed by the Bitcoin protocol may affect the value of bitcoins, both theories will be applied.

6.1 Bitcoin as a flow

An old workhorse in monetary economics is the equation of exchange (equation 1 below), stated by John Stuart Mill (1848) and algebraically formalised by Irving Fisher (1911). The equation is an identity describing the relationship between supply and demand of money as a flow over a given time period.

$$M_t V_t = \sum_i p_i q_i = P_t Q_t \tag{1}$$

According to the monetarist view, money demand is driven by nominal GDP ($P_t Q_t$), understood in the context of this thesis as the nominal value of goods bought with bitcoins, denominated in bitcoin. Furthermore, monetarists tend to assume that the quantity index (Q_t) and velocity of money (V_t) are relatively constant over time. With V_t and Q_t fixed, the only source of aggregate price (P_t) change is shifts in the quantity of money (M_t). As a result, inflation has been viewed to be *"…always and everywhere a monetary phenomenon"* (Friedman, 1970).

Different monetary regimes have different implications for the development of money supply, and thereby inflation. With commodity money and capitalist production, the marginal rate of return to investment over time must in theory be equal in all industries, including money production (equation 2).

$$\frac{1}{MC_M} = \frac{p_i}{MC_i} \tag{2}$$

This provides a long run relationship determining price of good i (p_i) as the ratio between marginal cost of that goods production (MC_i) and the marginal cost of money production (MC_M) (equation 3).

$$p_i = \frac{MC_i}{MC_M} \tag{3}$$

By creating an aggregate price level (P_t) based on these prices, the equilibrium value of money can be calculated as P_t^{-1}.

The production of some commodity monies, like the Somali shilling, exhibits constant marginal cost, thus providing a nominal anchor by endogenising the money supply. Should prices be too low (i.e. below their equilibrium value), the return to money production would exceed that of goods production. This would attract investments in the production of money, and thereby, increase money supply. With a fixed MC_M, the only source of persistent changes to P_t will be productivity shocks in goods production. Hence, persistent shocks to V_t or Q_t, will not affect the long run prices as long as marginal production costs remain constant. With bitcoins, on the other hand, M_t is exogenous and therefore independent of changes to other variables. As a result, shocks to Q_t must be accommodated by corresponding changes in V_t and/or P_t . Determination of the value of bitcoins (P_t^{-1}), and thereby prices(P_t) will

therefore hinge on assumptions about the exogeneity of V_t and Q_t relative to the equation of exchange. On the one hand, if one assumes that V_t is endogenous and a linear function of Q_t, only the likelihood that bitcoins are taken out of circulation or saved, thus reducing V_t, will affect P_t (Wang, 2014). Increases in Q_t, however, will have no effect on P_t because of the matching change in V_t. On the other hand, if one takes a more monetarist view, and assumes that V_t is exogenous relative to the equation of exchange, and stable over time, a growing economy (increasing Q_t) will imply deflation (decreasing P_t); a positive real interest rate on bitcoin holdings. To determine which of the assumptions are more plausible is an empirical task, and lies beyond the scope of this thesis. Moreover, the structural conditions surrounding Bitcoin and governing the variables in the equation of exchange, are constantly changing, making it nearly impossible to use past data to predict future behaviour.

As argued above, bitcoin denominated prices are immune to price changes driven by monetary supply shocks, because there cannot be any. However, this one-sided source of stability is bought at the price of an inability to accommodate demand shocks (changes in V_t and Q_t). Shifts in the demand for bitcoins, either for transaction purposes (Q_t) or saving/hoarding purposes (V_t) will therefore have a one-to-one effect on bitcoin denominated prices, ceteris paribus. To better understand the valuation of bitcoins, one therefore has to investigate the determination of bitcoin demand further.

6.2 Bitcoin as a stock

Although utility from money is only accessible as a flow, money itself is always held as a stock. In the same way, at every point in time the entire stock of bitcoins have to be held (voluntarily) by economic agents. Different agents will want to hold bitcoins for different purposes, and accordingly seek to realise their desired position in bitcoin, which forms a proportion of their real wealth. If the desire to hold real balances in bitcoins for some reason were to increase over the economy as a whole, the only way bitcoins could accommodate such a shift would be through an appreciation. An appreciation would increase the real value of bitcoins, and thereby bitcoins relative share of portfolios. It is important to notice, that since bitcoins are held as a stock, a reduced demand for bitcoins imply increased market-supply of bitcoins, as agents will seek to trade out of their positions. Therefore, saying that the supply of bitcoins is fixed refers to the total stock available to the economy, while the number of bitcoins for sale in the market is everything but fixed.

To investigate the determination of stock demand for bitcoins, one has to apply portfolio theory. As argued in Markowitz (1952) agents designing a portfolio first make up their minds regarding expected return to different assets, and then compose a portfolio based on these expectations. A qualified guess about the potential appreciation of bitcoin is currently very difficult due to its short history. The present value of bitcoin always hinges on expectations about the future collective decision to continue assigning a value to bitcoins. As a result, expectation formation will contain strong elements of a Keynesian beauty contest, when believes are not firmly anchored by experience. Therefore, since the bitcoin supply is fixed, increased demand based on expected appreciation will verify itself through generating the anticipated appreciation. A Bayesian reassessment may then push the appreciation expectations further up, thus turning the price formation of bitcoin into a Ponzi scheme. [41] In addition, when financial manoeuvres like short selling related to bitcoins are almost impossible, prices may remain high for longer than they would otherwise (Yermack, 2014). There are good reasons to suspect that these dynamics were at play during the bitcoin price rally that took place in 2013.

While, expected return on an asset is an important factor affecting the portfolio composition, risk aversion will make agents inclined to forego some expected return in exchange for lower risk. As a result, most portfolios tend to be diversified. Yermack (2014) finds that:

"*bitcoin's value is almost completely untethered to that of other currencies, which makes its risk nearly impossible to hedge for businesses and customers and renders it more or less useless as a tool for risk management*" (p. 3).

However, an asset's usefulness as a tool for risk management of a portfolio is not solely determined by how easy it is to hedge. Instead, since idiosyncratic risk, at least in theory, can be diversified away, the proper measure of the riskiness of individual assets is their covariance with the market portfolio relative to the market variance. [42] Bitcoins are therefore potentially very useful to hold, as they provide an independent source of variation. Nevertheless, bitcoin's lack of correlation with other assets is likely to change over time. The technical properties may turn bitcoin into a dollar hedge, a function currently served by gold (Joy (2011); Draghi (2013)). Besides, if bitcoins really were to catch on, it could develop into

[41] For the value of any currency, there is always an element of a Ponzi scheme, although, the unsustainability of the scheme only can be verified ex post, after a price collapse.
[42] This is a well-known result from CAPM, e.g. as derived in (Copeland, et al., 2005).

a safe haven currency due to its global nature, and serve as a macro hedge, currently one of the many roles of the dollar (Prasas, 2014).

A simple static portfolio model such as the one underlying the discussion above illustrates very well why agents holding diversified portfolios would like to hold bitcoins: To benefit from expected real appreciation and to manage portfolio risk. However, without including liquidity preferences (i.e. the element of moneyness) to the analysis, one only gets a limited understanding of bitcoin demand. In general, there are two principal motivations to hold different assets. One is the speculative purpose, explained above. The other, is the transaction purpose. Since different assets have different degrees of moneyness, agents will chose to hold some assets with a high degree of moneyness for transaction purposes. Hence, the easier it becomes to spend bitcoins, the higher the bitcoin demand for transaction purposes. While becoming a unit of account would likely increase the moneyness of bitcoins through increasing its speculative demand, it is not necessary as bitcoins could be demanded purely for transaction purposes. In fact, some economic commentators highlight bitcoin as a superior medium of exchange. Still, others, based on Krugman's popularisation of "Monetary Theory and the Great Capitol Hill Baby Sitting Co-op Crises (Sweeney & Sweeney, 1977), have argued that the fixed quantity of bitcoins is its Achilles heel, preventing it from ever becoming a successful medium of exchange. They claim that increased bitcoin demand, be it for transaction or speculation purposes, will end in a liquidity crisis. Since the supply is fixed, increased demand will result in deflation, which will stimulate hoarding, reduce velocity, and undermine bitcoin as a medium of exchange. However, this analysis is flawed as it confuses the decision to save with the determination of portfolio composition. The decision to save hinges on the total return to the portfolio, not, the return on any single asset alone. Therefore, the only way appreciation of bitcoins may reduce velocity is through increasing the general return to saving, assuming that the substitution effect dominates the income effect. This follows since agents deciding to spend, using bitcoins, will rebalance their portfolio to retain the desired real balance held in bitcoins. In other words, given a desire to spend, the decision to use bitcoin as the medium of exchange hinges on its moneyness, not expected appreciation. Moreover, since an appreciation of bitcoins will increase real bitcoin balances, some agents will find themselves with undesirably high exposure to bitcoin, and therefore seek to reduce their holding by increasing the market supply.

While an appreciating bitcoin could be unproblematic as long as bitcoin does not become a unit of account, the situation would be different once debt contracts emerge written in bitcoin. Credit effectively increases the velocity of the underlying asset through the creation of "inside money" (Kiyotaki & Moore, 2000). When providing a loan, the creditor normally acquires a nominal claim exceeding the value of what he lent out due to the charge of interest. Therefore, if bitcoin were to become a major currency at some point in the future, the fixed monetary base could prove very problematic. During a boom, credit supply will become increasingly elastic as described by Minsky (1982), generating a form of financial accelerator. Agents will build up increasing net claims on bitcoin, potentially exceeding the total stock. As long as the credit supply keeps expanding, thereby supporting the aggregate demand necessary to monetise past investments, and repay old debt, the boom may go on. However, eventually, a Minsky moment will be reached, where aggregate demand falls short of supply, and agents will find it hard to monetise their investment. To avoid a severe economic downturn following the dynamics of a Fisherian debt-deflation, expansionary monetary policy would be needed (Fisher, 1933). [43] Therefore, with a fixed supply of bitcoins, a downturn becomes more or less inevitable, unless governments use extreme measures like ruling bitcoin contracts invalid.

For all the reasons above, Bitcoin has many important political implications. Government regulation directly affects its value, and more importantly widespread use of bitcoins would undermine monetary and regulatory policy, hindering governments' ability to control economic activity. Therefore, the remainder of this thesis concentrates on how governments have reacted to Bitcoin so far, and then addresses the relevant research question by providing some thoughts on how governments will regulate bitcoin if it becomes widely used as a medium of exchange.

[43] Some economists, especially Austrians, argue that one should not intervene and stop debt-deflation, as it is a natural economic development, providing a foundation for renewed growth.

7 Bitcoin and the government

Bitcoin is clearly a creature of the market, undermining governments' capabilities to control economic activity. Consequently, government scepticism towards Bitcoin shall come as no surprise. Yet, officials tend to be divided in their view on the role of the state, and some even welcome innovations like Bitcoin. Moreover, since not all governments possess the same capabilities, some governments may appreciate technologies like Bitcoin, undermining other governments' ability to impose international restrictions and regulations.

To address the second research question, answering how and why governments will regulate Bitcoin, the subsequent paragraphs will present an overview of how governments have reacted to date. Thereafter, a short presentation of neo-classical market failures related to Bitcoin follows to shed light on some principal motivations to regulate, before the last and most important section looks into some of the political incentives to regulate money in general, and Bitcoin in particular.

7.1 Current regulation

The debate around how to regulate Bitcoin is still in its infancy (Law Library of Congress, 2014). Nowhere in the world is possession of bitcoins illegal, but governments seem to be uncertain about how they want to regulate it. What is certain, however, is governments' desire to tax anything to which the market assigns a positive value. For taxation purposes, bitcoins are therefore classified as a commodity or asset, and not a currency in most jurisdictions. Ironically, governments warn their citizens from using bitcoins, partly because bitcoins do not possess any "real" value, at the same time as they find this value real enough to tax.

Although many governments seem sceptical to bitcoin, the reactions by politicians and officials around the world has been very mixed. In the US, Congressman Jared Polis and former member of the House of Representatives Ron Paul embrace the use of bitcoin, while West Virginia Senator Joe Manchin *"...urge the regulators to work together, act quickly, and prohibit this dangerous currency from harming hard-working Americans.*"[44]

[44] http://www.manchin.senate.gov/public/index.cfm/2014/2/manchin-demands-federal-regulators-ban-bitcoin

The following paragraphs provide a short and selective overview of some countries official reactions to Bitcoin. For more complete and up to date lists, online pages like http://www.bitlegal.io/ and the Law Library of Congress (http://www.loc.gov/law/) are useful.

In India, capital controls, a weakening rupee and regulations on gold and silver purchases has made bitcoin an interesting investment. However, the Indian central bank have as so many other central banks warned its citizens from using bitcoin,[45] stating that *"…The absence of information of counterparties in such peer-to-peer anonymous/ pseudonymous systems could subject the users to unintentional breaches of anti-money laundering and combating the financing of terrorism (AML/CFT) laws*", a point also highlighted by the regulators in Singapore. [46] In addition, according to online news articles, several Indian exchanges have been raided and Indian authorities have seized transaction logs. [47]

In China, bitcoins were identified as a virtual commodity in an official note "Prevention of Risks Associated with Bitcoin"[48] released December 3rd, 2013. The note expressed concerns about the risks associated with Bitcoin, and the potential problems of money laundering. China is viewed as one of the most hostile countries towards Bitcoin, and the financial sector in China, including banks, is prohibited from dealing with bitcoins, both directly and indirectly. However, this does not stop China from also being one of the biggest countries within the Bitcoin economy. [49]

Another country, hostile towards the use of bitcoins, is Iceland. The tiny country was hit hard by the financial crises, and have had strict capital controls since. Therefore, the central bank, reminded the Icelandic population in a written response to Morgunblaðið (a newspaper), that any bitcoin activity involving foreign exchange trading and capital movements is prohibited by the Foreign Exchange Act. [50]

In Denmark, Finanstilsynet (Financial Supervisory Authority) warn against use of bitcoins, reject that it is a currency, and state that they will not regulate its use. [51] Furthermore, Danish

[45] http://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247
[46] http://www.mas.gov.sg/news-and-publications/press-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.aspx
[47] http://www.dnaindia.com/india/report-first-time-in-the-country-ed-raids-a-bitcoin-seller-in-ahmedabad-1941187
[48] See following webpage for a unofficial English translation https://vip.btcchina.com/page/bocnotice2013
[49] http://fiatleak.com/
[50] http://www.mbl.is/vidskipti/frettir/2013/12/19/hoftin_stodva_vidskipti_med_bitcoin/
[51] https://www.finanstilsynet.dk/da/Nyhedscenter/Pressemeddelelser/Arkiv-PM/Presse-2013/Advarsel-mod-virtuelle-valutaer-bitcom-mfl-2013.aspx

tax authorities buck the trend, and argue that capital gains from bitcoin are tax-free.[52] Norwegian tax authorities, on the other hand, identify bitcoin as an asset. Norwegians therefore have to pay VAT when bitcoins are used as payment, and report their bitcoin holdings to pay wealth and capital gains taxes. [53]

While use of bitcoin is associated with regulatory uncertainty all around the world, the Federal Financial Supervisory Authority in Germany (BaFin) have made life easier for users by providing clear judicial guidelines. BaFin has identified bitcoin as a unit of account and thereby a legally binding financial instrument, similar to foreign currency, but without legal tender status. Use of bitcoins is therefore taxed as other private forms of money, and commercial use of bitcoins may require authorisation pursuant to the German Banking Act, Kreditwesengesetz. [54]

In Japan, officials have remained silent about bitcoin, despite the fact that the Japan based Mt. Gox used to be the largest bitcoin exchange in the world, before it went bankrupt early in 2014.

In November 2013, there was a Bitcoin hearing in the U.S. Senate, which turned out in Bitcoins favour. Most news articles earlier in 2013 had focused on use of bitcoins to facilitate illegal activity and the acknowledgement of legitimate uses of bitcoin took many by surprise. Now, the IRS have determined to treat bitcoin and virtual currencies as property for tax purposes. [55] The financial regulator in New York, accepting that virtual currencies are here to stay, seeks to provide regulation allowing for the emergence of regulated and monitored bitcoin exchanges. Furthermore, under a presentation held by the Federal Reserve Bank of St. Louis March 31st entitled "Bitcoin and Beyond: The Possibilities and the Pitfalls of Virtual Currencies" David Andolfatto, vice president at the bank and professor at Simon Fraser University, claimed that "*Well-run central banks should welcome the emerging competition*" (Andolfatto, 2014). In addition, he cautioned that trying to regulate Bitcoin could be very difficult because of its decentralised structure.

[52] http://www.skat.dk/SKAT.aspx?oId=2156173&vId=0
[53] http://www.skatteetaten.no/no/Radgiver/Rettskilder/Uttalelser/Prinsipputtalelser/Bruk-av-bitcoins--skatte--og-avgiftsmessige-konsekvenser/
[54] http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html
[55] http://www.irs.gov/pub/irs-drop/n-14-21.pdf?utm_source=3.31.2014+Tax+Alert&utm_campaign=3.31.14+Tax+Alert&utm_medium=email

"*How do you regulate something that has no central head? It's like trying to slay the Hydra*" (ibid.).

The examples above serve to illustrate the limited and mixed attention Bitcoin has received from governments and regulators so far. Considering the small size of Bitcoin relative to other financial markets and instruments, this is not surprising. However, if Bitcoin catches on, it is highly likely that governments will take it more seriously, and do more to control it.

7.2 Neo-classical market failures

When trying to say something meaningful about how governments will react to Bitcoin in the future, one must directly or implicitly postulate assumptions about government preferences. One possibility is to be extremely naïve, and assume that governments are benevolent correctors of (neo-classical) market failures, and simply confine their focus to correcting these failures. While this assumption is highly unrealistic, the market failures of monopoly, asymmetric information, and externalities should influence the decision making of real governments to some extent.

The total "production" of bitcoins is independent of the production structure, making misuse of monopoly power in production impossible. Still, a very unequal distribution of bitcoins combined with the currently thin bitcoin market, could result in some agents acting as price makers rather than price takers. To implement regulations and incentive structures making such agents act as if they were price takers, would, if possible, be desirable. In practise, however, considering Bitcoin's global character, and when looking at the persistent manipulation of other financial markets,[56] it is difficult to imagine how this could be done in practise.

When it comes to asymmetric information, there is, in theory, no principal motivations for governments to regulate Bitcoin. The public ledger makes the network and ownership structures as transparent as they can be without fundamentally altering the nature of the

[56] E.g. the Libor scandal (U.S. Department of Justice, 2012), or see Financial Times' "Forex Trading Probes" page for a more general overview (Financial Times, 2014).

Bitcoin protocol. Moreover, as any actual asymmetry in information will be independent of how Bitcoin functions, there will be no need for a neo-classical government to regulate.

Possibly the most interesting market failure related to Bitcoin ties in with a property of money more generally. As a social construct, the usefulness of Bitcoin pivots on its network.

"*Our willingness to use and hold money is greater the more that money is used by other people*." (King, 2004, p. 3).

The network externalities associated with the use of bitcoins are three-sided. First, merchants will only benefit from, and start accepting, bitcoins if consumers want to spend bitcoins. Second, consumers only want to acquire and spend bitcoins if there are merchants accepting bitcoins. Third, software and hardware developers will only develop the necessary infrastructure if merchants and consumers use bitcoins. However, without the necessary infrastructure in place, neither merchants nor consumer can use bitcoins. While the network effect becomes self-reinforcing and sustains the network once it has become large enough, the necessary conditions to get initial traction is like a catch 22. Even in a hypothetical scenario in which there was no doubt that bitcoins were a superior form of money relative to all other monies, the switching cost, due to network externalities, might prevent the market from successfully adopting bitcoin as the dominant form of money (Luther, 2013). Hence, too few agents might start using bitcoins, as the social benefit exceeds the private. Furthermore, inasmuch as Bitcoin does not purely represent a compliment to existing monetary systems, a build-up of Bitcoin would necessitate the dismantling of some other network. Too many participants may leave other networks because the social cost of leaving is higher than the private cost, when network externalities are present. Therefore, the efficient reaction of a neo-classical government would be to first identify the best system and then incentivise a shift towards this by internalising the network externalities during the build-up. Given that Bitcoin should at least serve as a compliment to existing systems, the early adoption rate might potentially be too low, making government stimulus necessary. However, forward-looking agents, anticipating the network effects may be willing to undertake high-risk/high-payoff investments in Bitcoin. Such investments will only be profitable contingent on network growth, thereby, to some degree internalising the network externalities and make government stimulus less essential.

7.3 The realpolitik of money and Bitcoin

No government in the world behaves the way the neo-classical framework suggests that it should, and a neo-classical approach is inadequate to answer the research question of how and why governments will regulate Bitcoin. Instead, political economy considerations must be taken into account. Government themselves are diverse, reflecting underlying power structures and have preferences over distributional outcomes. Since institutional and social relations are unique, it is impossible to come up with a general theory about how governments will react to Bitcoin if it were to really catch on. Predicting governments' reaction to Bitcoin should therefore be done cautiously and be based on case studies of the political settlement in the countries under investigation. [57] Even so, some insights can be drawn from analysing both how governments have regulated commodity money earlier, and from analysing how certain preferences would affect government actions. Consequently, the next two sections will first present a historical account of the demonetisation of gold, to illustrate governments' capabilities and desire to control money, and then analyse and highlight political economy motivations to regulate Bitcoin.

7.3.1 Demonetisation of gold

In 1929, following the financial meltdown, Americans started to hoard gold. Officials argued that the hoarding deepened the ongoing recession and led to a stalling of economic growth. Arguing along these lines, President Franklin D. Roosevelt signed Executive Order 6102 April 5th (1933), criminalising private holdings of monetary gold like coins, bullion and certificates, both within the U.S. and abroad. All but a small amount of privately held gold had to be handed in to the Federal Reserve (FED) at a fixed exchange rate of 20.6 USD per ounce. Violation of the order was punishable with up to 10 years in prison and/or 10,000 USD. [58] The year after, 1934, the Gold Reserve Act was written into law, stating that all gold and gold certificates held by the FED had to be transferred to the U.S. Treasury. A massive one off inflation tax was imposed on dollar holdings as the fixed exchange rate of gold was raised to 35 USD per ounce. The result was a 2.8 billion USD[59] paper profit, most of which

[57] Khan (2010) Presents and uses a typology of political settlements to analyse the governance of growth enhancing institutions. The same framework could be extended and used to analyse governments' treatment of Bitcoin.

[58] 181,763 USD CPI-adjusted to February 2014, using: http://www.bls.gov/data/inflation_calculator.htm
See appendix A for a photocopy of an information poster informing about the executive order.

[59] 50.89 billion USD CPI-adjusted to 2014, using: http://www.bls.gov/data/inflation_calculator.htm

was used to finance the establishment of the Exchange Stabilization fund. To hedge against a devaluation of the dollar, private agents had written contracts redeemable in gold. However, these became invalid, and private ownership and trading in gold remained constrained until 1975.

Later around 1970, the U.S. sought to demonetise gold as an international reserve asset. Persistent trade deficits had reduced the U.S. gold reserves drastically, and the markets and some central banks (particularly the French) speculated against the regime of fixed exchange rates by hoarding gold (Garber, 1993). Being unwilling to increase the official price of gold, [60] i.e. devalue the USD, the Americans argued that Special Drawing Rights (SDR) should replace gold. As stated in a now declassified letter to the Secretary of State:

"If we want to have a chance to remain the masters of gold an international agreement on the rules of the game as outlined above seems to be a matter of urgency. We would fool ourselves in thinking that we have time enough to wait and see how the S.D.R.'s will develop. In fact, the challenge really seems to be to achieve by international agreement within a very short period of time what otherwise could only have been the outcome of a gradual development of many years." (U.S. Embassy Paris, 1968)

In the same telegram, it was suggested that gold reserves should be reshuffled, from countries with relative high holdings of gold, to countries, like the U.S with relative low holdings of gold. In 1974, a note sent to Paul Volcker, then Under Secretary of the Treasury for Monetary Affairs, further outlined how the U.S. should achieve their goal that the "*SDR should take the place once held by gold at the center of the world monetary system"* (Weintraub, 1974). The American objective was in apparent conflict with European countries' desire to continue to use gold for international settlements, reflecting *"…the interest of creditor countries in receiving gold and applying discipline to deficit countries*" (ibid). The U.S. feared unilateral arrangements by Europe and viewed it as very important to stress that there could

"…be no question of introducing a new form of gold– paper and gold–metal bimetallism, in which the SDR and gold would be in competition. … To encourage and facilitate the eventual demonetization of gold, our position is to keep the present gold price, maintain the present Bretton Woods agreement ban against official gold purchases at above the official price and

[60] Not very surprising considering their low reserve holdings. France, on the other hand, holding large gold reserves, wanted to increase the official price of gold, to among other things finance increasingly expensive oil import (Weintraub, 1974).

encourage the gradual disposition of monetary gold through sales in the private market" (ibid.).

If bitcoin is to become a dominant medium of exchange, the two examples above clearly show that governments may be both willing and capable to do whatever it takes to control money and stop it. Gold was successfully demonetised for domestic purposes, and although the SDR never really took off, the USD replaced gold as the main reserve asset internationally. Nonetheless, gold is still held by central banks and traded amongst private agents as a financial object.

7.3.2 The desire to regulate Bitcoin

To better understand the desire to control money, and thereby Bitcoin, it is natural to assume that governments have distributional preferences and seek to redistribute wealth. To this end, governments need to hold the means to command real resources. This is normally achieved through taxation. In fact, taxation under a fiat monetary system generates a double source of revenue.

"*Since a government obtains seigniorage from money creation, this benefits the fiscal position twice over, not only from the taxes levied, but also from the seigniorage resulting from the induced monetary demand*" (Goodhart, 1998, p. 416).

Moreover, to increase the tax base many governments find it desirable to introduce capital controls to enable taxation of both real and nominal capital assets. High capital mobility limits governments' ability to redistribute from capital to labour, and money competition restricts the scope of the inflation tax (Alesina, et al., 1993).

Widespread use of bitcoin would undermine governments' ability to command resources for several reasons. First, governments does not generate any seigniorage from the private creation of bitcoins, and even if the government started to produce bitcoins themselves, the resource cost would limit the scope for seigniorage. Second, bitcoins have the potential to serve as a Swiss bank account, storing wealth outside the reach of the tax authorities. Third, it is virtually impossible to impose effective capital controls against bitcoin, making monetary competition tougher and inflation taxation less sustainable. One should therefore expect governments to clamp down on use of bitcoin.

However, given that there seems to be a latent demand for digital cash, and observing that there is a substantial resource cost tied to maintaining the credibility of the Bitcoin transaction chain, this begs the question as to why governments do not create digital cash themselves. Governments could e.g. replicate the supply-structure in Bitcoin and let all transactions be settled in a centralised but pseudonymus ledger, promising to follow a "no touch policy". Such a scheme would be no worse than Bitcoin, and it would facilitate a reduction of the resource cost, which could instead accrue to the state as seingiorage. Yet, for a government to commit to a given monetary policy, in this case the supply of a digital money, is neither possible nor desirable (King, 2004). The undesirability follows from bounded rationality making the formulation of perfect contingent policy rules impossible, while the impossibility follows from the fact that collective decisions today cannot bind collective decisions tomorrow (ibid.). Since the value of all forms of money hinges on a collective decision, the latter point is as relevant for Bitcoin as for a digital government money. However, holders of bitcoins control the value of bitcoins, while in the end; governments control the value of their digital money. If wealth distribution becomes too unequal, there is no straightforward way for the dispossessed to force trough a redistribution of bitcoins. With a government money, on the other hand, the no touching policy could be abounded overnight if there was political demand for it. In this context, Bitcoin looks very anti-democratic as it consolidates the power of bitcoin owners. Actually, this is a key feature, without which bitcoins hardly would command a positive price. Nonetheless, government policy may also be undemocratic, and Bitcoin's reliance to regulation preserves a democratic element, the undermining of the powers of central authority.

Another reason for governments' desire to control money may be explained by paternalistic preferences over individuals' behaviour. Not only do governments want to redistribute wealth, they also seek to limit and support certain activities. While the motivation to regulate individuals' behaviour could be based on corrections of market failures, it is instead often founded on moral perceptions. As an example is activates such as prostitution and drug use illegal and punishable by law. For many illegal transactions, cash is used to settle exchange, because of the non-traceability and irreversibility. Since electronic payments better can be controlled and monitored, governments would prefer to demonetise cash and force agents to rely on non-anonymous electronic payments. However, since removing cash only increases the transaction costs of illegal transactions without altering the underlying demand, there will be market forces endogenously stimulating the emergence of a private money with cash

properties. Bitcoin with its pseudonymity could potentially substitute for cash, and in addition make long distance transfers related to illegal transactions easier. Thus, undermine governments' ability to control economic activity through controlling money.

For the reasons presented above it is very clear that governments with a desire to rise revenue and control economic activity, the existence of bitcoins is unwelcome. Governments also care about the welfare of their residents, and some would argue that if the agents increase their general welfare level by using bitcoin, government should, and will welcome it. However, the transaction costs overcome by Bitcoin is primarily political. In fact, any government truly wanting a form of digital cash to exist have had access to the technology to create it for a long time. The observation that no government backed, centralised and pseudonymous digital form of cash exist, therefore shows that no government have wanted it until now. Nevertheless, one should expect the black economy to come up with workarounds if the government is too restrictive, the same way the financial sector pulverised financial regulation before the crises through financial innovation. The genie is out of the bottle, and the idea of digital cash is here to stay. Admitting that the emergence and development of digital money cannot be stopped, some governments might find providing the market with a government backed digital money to be desirable as a second best solution. [61] Yet, it is not given that markets would prefer to trust a centralised government money to a decentralised one.

[61] The Royal Canadian Mint tried to develop a form of electronic money, in a project called Mintchip in 2012. The project is now halted, and the Mint intend to sell it off to the private market. http://www.mint.ca/store/news/royal-canadian-mint-launches-mintchiptm-developer-challenge-14900005?cat=News+releases&nId=700002&nodeGroup=About+the+Mint#.U15tPPmSzsE

8 Concluding remarks

In this thesis, bitcoin has been identified as a digital commodity money. In order to do so, a typology of different generic monies was developed, identifying a hierarchy in which an increasing degree of trust is required to support use of more "efficient" monies.

Money in general serves as an indirect record of transactions, and enables agents to interact through indirect exchange. To make money as a record of transactions credible, monetary units must serve as a "Proof of Work", making it costly to alter "the record". The value of any monetary unit therefore pivots on the work required to obtain it (not necessarily the cost of production), and in this regard, bitcoins are no different from other monies. Since different social relations are governed by different institutions, the nature of any money hinges on the specific set of relations it intermediates. As a result, monetary phenomena are as complex and dynamic as society itself. Network externalities strengthens the position of dominant money forms, and result in a monopolisation of the ability to buy. Still, since social relations tend not to exist in isolation, a form of money intermediating one set of relations may possess a degree of moneyness in another.

Since the supply of bitcoins is limited, and in the end fixed, its value will be determined by demand. Without use value, the demand for bitcoin must be fundamentally based on its expected future demand, and hinge on its capacity to lower transaction costs other monies cannot. As argued in this thesis, bitcoins actually lower certain transaction costs, primarily politically imposed, and should therefore command a positive price. Since seeking to affect economic activity through altering transaction costs does not change the desire to undertake such transactions, private money forms like bitcoin are likely to emerge endogenously, undermining governments' ability to control economic activity through controlling money. Observing that governments could provide the market with digital cash if they wanted to, but have chosen not to, also clearly suggests that governments will not generally welcome widespread adoption of bitcoins, and will seek to regulate it. However, as the idea and existence of digital cash can hardly be stopped, governments might find it desirable to compete with private monies in the digital world, and supply their own digital cash to at least benefit from the seigniorage.

From a broader perspective, Bitcoin as a phenomenon seems to have struck a chord with not only the Internet community but with serious investors and millions of tech savvy consumers

throughout the world. Governments are only now starting to take it seriously, and the wider public have only a nascent awareness of its capabilities. Akin to the development of the Internet, the Bitcoin protocol's full potential may not be realised for many years to come. It is the purpose of this thesis to show that this is not some passing fad that has no grounds for serious consideration, but rather that it is the culmination of years of advances in technology, that it solves real economic and political problems for millions of people, and that fundamentally all true innovation follows the age old pattern: First, it is ridiculed. Second, it is violently opposed. Third, it is accepted as self-evident.

Bibliography

Adi, S. & Dorit, R., 2013. Quantitative Analysis of the Full Bitcoin Transaction Graph. In: A. Sadeghi, ed. *Financial Cryptography and Data Security*. Berlin: Springer-Verlag, pp. 6-24.

Alchain, A. A. & Demsetz, H., 1972. Production, information costs, and economic organization. *The American economic review*, pp. 777-795.

Alesina, A., Grilli, V. & Milesi-Ferretti, G. M., 1993. *The Political Economy of Capital Controls, NBR Working Paper No. 4353.* [Online]
Available at: http://www.nber.org/papers/w4353.pdf
[Accessed 22 April 2014].

Andolfatto, D., 2014. *Bitcoin and Beyond: The Possibilities and the Pitfalls of Virtual Currency, Presentation held at the Federal Reserve Bank of St. Louis.* [Online]
Available at: http://www.stlouisfed.org/newsroom/multimedia/video/20140331-dialogue-with-the-fed-part4.cfm
[Accessed 29 April 2014].

Arnold, M., 2014. *Barclays launches investigation after reported customer data leak, Financial Times.* [Online]
Available at: http://www.ft.com/intl/cms/s/0/b1504dba-9170-11e3-adde-00144feab7de.html?siteedition=intl#axzz30ARdvlTI
[Accessed 28 Aprl 2014].

Bryan, M. F., 2004. *Island Money.* [Online]
Available at: https://www.clevelandfed.org/research/commentary/2004/0201.pdf
[Accessed 29 April 2014].

Coase, R. H., 1937. The nature of the firm. *economica,* 4(16), pp. 386-405.

CoinDesk, 2014. *State of Bitcoin report.* [Online]
Available at: http://www.coindesk.com/bitcoin-2014-report/
[Accessed 1 Mai 2014].

Communications Comission of Kenya, 2012. *QUARTERLY SECTOR STATISTICS REPORT.* [Online]
Available at:
http://www.cck.go.ke/resc/downloads/SECTOR_STATISTICS_REPORT_Q2_2011-12.pdf
[Accessed 28 April 2014].

Copeland, T. E., Weston, J. F. & Shastri, K., 2005. *Financial theory and corporate policy.* 1 ed. Boston: Ma: Addison-Wesley.

Davidson, K. & Lee, M., 2014. *What Larry Summers thinks about Bitcoin — Fiscal confidence up slightly since January, Politico.* [Online]
Available at: http://www.politico.com/morningmoney/0214/morningmoney13103.html
[Accessed 28 April 2014].

Diamond, P., 1990. Pairwise credt in search equilibrium. *quartaly journal of economics,* Volume 105, pp. 285-319.

Draghi, M., 2013. *European Central Bank Chief Mario Draghi Comments On Gold at Harvard University.* [Online]
Available at: Youtube, https://www.youtube.com/watch?v=eG4RJ4P6gm0
[Accessed 28 April 2014].

Duffy, J. & Ochs, J., 2002. Intrinsically Worthless Objects as Media of Exchange: Experimental Evidence. *International Economic Review,* 43(3), pp. 6637-673.

European Central Bank, 2012. *Virtual Currency Schemes.* [Online]
Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
[Accessed 29 April 2014].

Financial Times, 2014. *Forex Trading Probes.* [Online]
Available at: http://www.ft.com/intl/topics/themes/Forex_trading_probes
[Accessed 1 May 2014].

Fisher, I., 1911. *The Purchaising Power of Money - its determination and relation to credit interst and crises.* New York: The Macmillian Company.

Fisher, I., 1933. The debt-deglation theory of great depressions. *Econometrica: Journal of the Economic Society,* pp. 337-357.

Freixas, X. & Rochet, J.-C., 2008. *The Microeconomics of Banking.* 2 ed. Cambridge, Massachusetts: MIT Press.

Friedman, M., 1970. *The Counter-Revolution in Monetary Theory,* London: Institute of Economic Affairs.

Friedman, M., 1991. *The Island of Stone Money, Hoover Institution, Working Paper No. E-91-3.* [Online]
Available at: file:///C:/Users/Torbj%C3%B8rnBull/Downloads/E-91-3.pdf
[Accessed 19 April 2014].

Garber, P. M., 1993. The Collapse of the Bretton Woods Fixed Exchange Rate System. In: M. D. Bordo & B. and Eichengreen, eds. *: A Retrospective on the Bretton Woods System: Lessons for.* Chicago: University of Chicago Press, pp. 461-494.

Gillmor, D., 2011. *WikiLeaks payments blockade sets dangerous precedent, The Guardian.* [Online]
Available at: http://www.theguardian.com/commentisfree/cifamerica/2011/oct/27/wikileaks-

payments-blockade-dangerous-precedent
[Accessed 28 April 2014].

Goff, S., Moore, E. & Wallis, W., 2013. *Somalia warns of disaster if Barclays stops money transfers.* [Online]
Available at: http://www.ft.com/intl/cms/s/0/3ed3c56e-2f50-11e3-8cb2-00144feab7de.html#axzz30ARdvlTI
[Accessed 28 April 2014].

Goodhart, C., 1998. The two concepts of money: implications for the. *European Journal of Political Economy,* Volume 14, pp. 407-432.

Holm, E., 2014. *Nouriel Roubini: Bitcoin Is a 'Ponzi Game', The Wall Street Journal.* [Online]
Available at: http://blogs.wsj.com/moneybeat/2014/03/10/nouriel-roubini-bitcoin-is-a-ponzi-game/
[Accessed 28 April 2014].

Ingham, G., 2000. Babylonian madness': on the historical and sociological origins of money. In: J. Smithin, ed. *What is Money.* London: Routledge, pp. 16-41.

Jenkins, P., 2013. *Banks pull back from risky regions, Financial Times.* [Online]
Available at: http://www.ft.com/intl/cms/s/0/47c3432a-aa5d-11e2-9a38-00144feabdc0.html#axzz2zayYUOfD
[Accessed 22 April 2014].

Jin, Y. & Temzelides, T., 2004. On the local interaction of money and credit. *Review of Economic Fynamics,* Volume 7, pp. 143-156.

Joy, M., 2011. Gold and the US dollar: Hedge or haven?. *Finance Research Letters,* 8(3), pp. 120-131.

Kahn, C. M. & Roberds, W., 2009. Why pay? An introduction to payments economics. *Journal of Financial Intermediation,* 18(1), pp. 1-23.

Kearns, J., 2013. *Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value, Bloomberg.* [Online]
Available at: http://www.bloomberg.com/news/2013-12-04/greenspan-says-bitcoin-a-bubble-without-intrinsic-currency-value.html
[Accessed 28 April 2014].

Khan, M. H., 2010. *Political Settlements and the Governance of.* [Online]
Available at: http://eprints.soas.ac.uk/9968/1/Political_Settlements_internet.pdf
[Accessed 22 April 2014].

King, M., 2004. The Institutions of Monetary Policy. *American Economic Review,* pp. 1-13.

Kiyotaki, N. & Moore, J., 2000. Inside money and liquidity. *Unpublished manuscript, University of Edinburgh.*

Kiyotaki, N. & Wright, R., 1989. On Money as a Medium of Exchange. *Journal of Political Economy,* 97(4), pp. 927-954.

Kocherlakota, N. R., 1998. Money is memory. *Journal of Economic Theory,* 81(2), pp. 232-251.

Koopmans, T. C., 1951. Analysis of production as an efficient combination of activities. *Activity analysis of production and allocation,* Issue 13, pp. 33-37.

Kovaleski, S. F., 2014. *Banks Say No to Marijuana Money, Leagal or Not, The New York Times.* [Online]
Available at: http://www.nytimes.com/2014/01/12/us/banks-say-no-to-marijuana-money-legal-or-not.html?_r=0
[Accessed 28 April 2014].

Krugman, P., 2013. *Bitcoin Is Evil, The New York Times - The Opinion Pages.* [Online]
Available at: http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1
[Accessed 28 April 2014].

Lapavitsas, C., 2003. *Social Foundations of Markets, Money and Credit.* London: Routledge.

Law Library of Congress, 2014. *Regulation of Bitcoin in Selected.* [Online]
Available at: http://cdn1.sbnation.com/assets/3952017/2014-010233_Law_Library_of_Congress_Bitcoin_jurisdictional_survey.pdf
[Accessed 21 April 2014].

Luther, W. J., 2012. *The Monetary Mechanism of Stateless Somalia.* [Online]
Available at: SSRN, http://ssrn.com/abstract=2047494 or http://dx.doi.org/10.2139/ssrn.2047494
[Accessed 5 April 2014].

Luther, W. J., 2013. *Cryptocurrencies, Network Effects, and Switching Costs, Mercatus Center Working Paper No. 13-17.* [Online]
Available at: SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295134
[Accessed 28 April 2014].

Luther, W. J. & Olson, J., 2013. *Bitcoin is Memory, SSRN.* [Online]
Available at: http://ssrn.com/abstract=2275730 or http://dx.doi.org/10.2139/ssrn.2275730
[Accessed 28 April 2014].

Luther, W. J. & White, L. H., 2011. *Positively Valued Fiat Money after the Sovereign Disappears: The Case of Somalia, GMU Working Paper in Economics No. 11-14.*. [Online]
Available at: SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1801563
[Accessed 29 April 2014].

Markowitz, H., 1952. Portfoli Selection. *Journal of Finance,* 7(1), pp. 77-91.

Mill, J. S., 1848. *Priciples of Political Economy.* London: J.W. Parker.

Minsky, H. P., 1982. The Financial Instability Hypothesis: Capitalist Processes and the Behaviour of the Economy. In: C. P. Kindleberger & J. Laffargue, eds. *Financial Crises: Theory, History, and Policy.* Cambridge: Cambridge University Press, pp. 13-39.

Mises, L. v., 1935 [1881]. *The Theory of Money and Credit.* New York: Harcourt Brace.

Mishkin, F. S., 1993. *Money, Interest rates and inflation.* 1 ed. Aldershot: E. Elgar.

Mubarak, J. A., 2003. A Case of Private Supply of Money in Stateless Somalia. *Journal of African Economies,* 11(3), pp. 309-325.

Nakamoto, S., 2008. *bitcoin.org.* [Online]
Available at: http://bitcoin.org/bitcoin.pdf
[Accessed 3 February 2014].

North, D. C., 1991. Institutions. *The Journal of Economic Perspectives,* 5(1), pp. 97-112.

NTU/F, 1999. *Milton Friedman Interview on Anti-Trust and Tech, National Taxpayers Unioun Foundation.* [Online]
Available at: https://www.youtube.com/watch?v=mlwxdyLnMXM&feature=youtu.be
[Accessed 1 May 2014].

Ostroy, J. M. & Starr, R. M., 1990. The Transactions Role of Money. In: B. M. Friedman & F. H. Hahn, eds. *Handbook of Monetary Economics.* New York: North-Holland, pp. 3-62.

Prasas, E. s., 2014. *The Dollar Trap - how the U.S. dollar thightened its grip on global finance.* 1 ed. Woodstock, Oxfordshire: Princeton University Press.

Ramzan, Z., 2013. *Khan Academy - Bitcoin Course.* [Online]
Available at: https://www.youtube.com/watch?v=Y-w7SnQWwVA&list=PL73q2zDIiGK_O5OYdK5vxcezzC0zu_3OS
[Accessed 29 April 2014].

Robbins, L., 1953. Introduction. In: *The Theory of Money and Credit.* s.l.:Yale University Press, New Haven, pp. 11-13.

Roosevelt, F. D., 1933. *Executive Order 6102.* [Online]
Available at: http://www.presidency.ucsb.edu/ws/?pid=14611
[Accessed 28 April, Online by Gerhard Peters and John T. Woolley, The American Presidency Project 2014].

Selgin, G., 2013. *Synthetic Commodity Money.* [Online]
Available at: SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118

Shafiee, S. & Topsal, E., 2010. An overview of global gold market and gold price forecasting. *Resource Policy,* 35(3), pp. 178-189.

Shubik, M., 2004. *The theory of money and financial institutions.* Cambridge: Mit Press.

Stafford, P., 2014. *Tera sets up standards for Bitcoin swaps, Financial Times.* [Online]
Available at: http://www.ft.com/intl/cms/s/0/0cbf76de-b36e-11e3-bc21-00144feabdc0.html?siteedition=intl#axzz30TDLGJ00
[Accessed 1 May 2014].

Stanners, 2012. *US snubs out legal cigar transaction, the Copenhagen post.* [Online]
Available at: http://cphpost.dk/news/us-snubs-out-legal-cigar-transaction.898.html
[Accessed 28 April 2014].

Sweeney, J. & Sweeney, R. J., 1977. Monetary Theory and the Great Capitol Hill Baby Sitting Co-op Crisis. *Journal of Money, Credit and Banking,* 9(1), pp. 86-89.

TeleGeography, 2013. *Vodacom Tanzania reports five million M-PESA subs; transactions top USD823m.* [Online]
Available at:
http://www.telegeography.com/products/commsupdate/articles/2013/05/02/vodacom-tanzania-reports-five-million-m-pesa-subs-transactions-top-usd823m/
[Accessed 28 April 2014].

U.S. Department of Homeland Security, 2013. *Congressional hearing on the future of Bitcoin.* [Online]
Available at: https://s3.amazonaws.com/s3.documentcloud.org/documents/835843/virtual-currency-hearings.pdf
[Accessed 28 April 2014].

U.S. Department of Justice, 2012. *Barclays Bank PLC Admits Misconduct Related to Submissions for the London Interbank Offered Rate and the Euro Interbank Offered Rate and Agrees to Pay $160 Million Penalty.* [Online]
Available at: http://www.justice.gov/opa/pr/2012/June/12-crm-815.html
[Accessed 1 May 2014].

U.S. Embassy Paris, 1968. *Telegram to the Secretary of State regarding problems with gold as a reserve asset.* [Online]
Available at: http://www.scribd.com/doc/20215562/Gold-Telegram
[Accessed 28 April 2014].

United States Postal Service, 2014. *Providing Non-Bank Financial Services for the Underserved.* [Online]
Available at: http://www.uspsoig.gov/sites/default/files/document-library-files/2014/rarc-wp-14-007.pdf
[Accessed 28 April 2014].

Wang, J. C.-Y., 2014. *A Simple Macroeconomic Model of Bitcoin.* [Online]
Available at: SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2394024
[Accessed 14 April 2014].

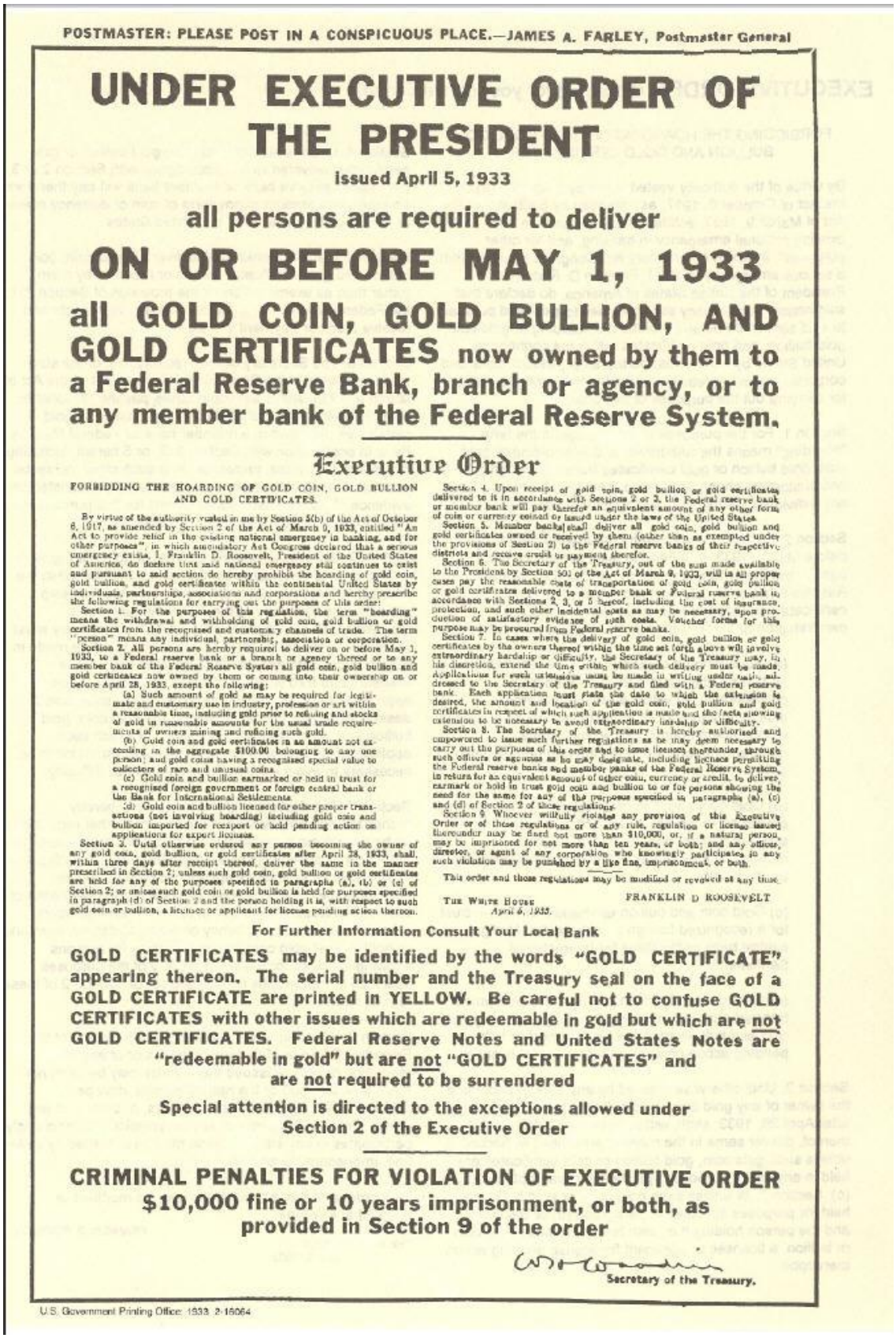
Weintraub, S., 1974. *Document 61, Foreign Relations Of The United States, 1973–1976, Volume XXXI Foreign Economic Policy.* [Online]
Available at: http://history.state.gov/historicaldocuments/frus1969-76v31/d61
[Accessed 28 April 2014].

Williamson, O. E., 1985. *The Economic Institutions of Capitalism.* London: Collier Macmillan Publishers.

World Bank, 2013. Migration and Remittance Flows: Recent Trends and Outlook, 2013-2016. *Migration and Development Brief 21*.

Yermack, D., 2014. *Is Bitcoin a Real Currency? An Economic Apprisal.* [Online]
Available at: SSRN, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2361599
[Accessed 1 May 2014].

Appendix A



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.—JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

By virtue of the authority vested in me by Section 5(b) of the Act of October 6, 1917, as amended by Section 2 of the Act of March 9, 1933, entitled "An Act to provide relief in the existing national emergency in banking, and for other purposes", in which amendatory Act Congress declared that a serious emergency exists, I, Franklin D. Roosevelt, President of the United States of America, do declare that said national emergency still continues to exist and pursuant to said section do hereby prohibit the hoarding of gold coin, gold bullion, and gold certificates within the continental United States by individuals, partnerships, associations and corporations and hereby prescribe the following regulations for carrying out the purposes of this order:

Section 1. For the purposes of this regulation, the term "hoarding" means the withdrawal and withholding of gold coin, gold bullion or gold certificates from the recognized and customary channels of trade. The term "person" means any individual, partnership, association or corporation.

Section 2. All persons are hereby required to deliver on or before May 1, 1933, to a Federal reserve bank or a branch or agency thereof or to any member bank of the Federal Reserve System all gold coin, gold bullion and gold certificates now owned by them or coming into their ownership on or before April 28, 1933, except the following:

(a) Such amount of gold as may be required for legitimate and customary use in industry, profession or art within a reasonable time, including gold prior to refining and stocks of gold in reasonable amounts for the usual trade requirements of owners mining and refining such gold.

(b) Gold coin and gold certificates in an amount not exceeding in the aggregate $100.00 belonging to any one person; and gold coins having a recognized special value to collectors of rare and unusual coins.

(c) Gold coin and bullion earmarked or held in trust for a recognized foreign government or foreign central bank or the Bank for International Settlements.

(d) Gold coin and bullion licensed for other proper transactions (not involving hoarding) including gold coin and bullion imported for reexport or held pending action on applications for export licenses.

Section 3. Until otherwise ordered any person becoming the owner of any gold coin, gold bullion, or gold certificates after April 28, 1933, shall, within three days after receipt thereof, deliver the same in the manner prescribed in Section 2; unless such gold coin, gold bullion or gold certificates are held for any of the purposes specified in paragraphs (a), (b) or (c) of Section 2; or unless such gold coin or gold bullion is held for purposes specified in paragraph (d) of Section 2 and the person holding it is, with respect to such gold coin or bullion, a licensee or applicant for license pending action thereon.

Section 4. Upon receipt of gold coin, gold bullion or gold certificates delivered to it in accordance with Sections 2 or 3, the Federal reserve bank or member bank will pay therefor an equivalent amount of any other form of coin or currency coined or issued under the laws of the United States.

Section 5. Member banks shall deliver all gold coin, gold bullion and gold certificates owned or received by them (other than as exempted under the provisions of Section 2) to the Federal reserve banks of their respective districts and receive credit or payment therefor.

Section 6. The Secretary of the Treasury, out of the sum made available to the Presidents by Section 501 of the Act of March 9, 1933, will in all proper cases pay the reasonable costs of transportation of gold coin, gold bullion or gold certificates delivered to a member bank or Federal reserve bank in accordance with Sections 2, 3, or 5 hereof, including the cost of insurance, protection, and such other incidental costs as may be necessary, upon production of satisfactory evidence of such costs. Vouchers forms for this purpose may be procured from Federal reserve banks.

Section 7. In cases where the delivery of gold coin, gold bullion or gold certificates by the owners thereof within the time set forth above will involve extraordinary hardship or difficulty, the Secretary of the Treasury may, in his discretion, extend the time within which such delivery must be made. Applications for such extensions must be made in writing under oath, addressed to the Secretary of the Treasury and filed with a Federal reserve bank. Each application must state the date to which the extension is desired, the amount and location of the gold coin, gold bullion and gold certificates in respect of which such application is made and the facts showing extension to be necessary to avoid extraordinary hardship or difficulty.

Section 8. The Secretary of the Treasury is hereby authorized and empowered to issue such further regulations as he may deem necessary to carry out the purposes of this order and to issue licenses thereunder, through such officers or agencies as he may designate, including licenses permitting the Federal reserve banks and member banks of the Federal Reserve System, in return for an equivalent amount of other coin, currency or credit, to deliver, earmark or hold in trust gold coin and bullion to or for persons showing the need for the same for any of the purposes specified in paragraphs (a), (c) and (d) of Section 2 of these regulations.

Section 9. Whoever willfully violates any provision of this Executive Order or of these regulations or of any rule, regulation or license issued thereunder may be fined not more than $10,000, or, if a natural person, may be imprisoned for not more than ten years, or both; and any officer, director, or agent of any corporation who knowingly participates in any such violation may be punished by a like fine, imprisonment, or both.

This order and those regulations may be modified or revoked at any time.

THE WHITE HOUSE
April 5, 1933.

FRANKLIN D ROOSEVELT

For Further Information Consult Your Local Bank

GOLD CERTIFICATES may be identified by the words "GOLD CERTIFICATE" appearing thereon. The serial number and the Treasury seal on the face of a GOLD CERTIFICATE are printed in YELLOW. Be careful not to confuse GOLD CERTIFICATES with other issues which are redeemable in gold but which are not GOLD CERTIFICATES. Federal Reserve Notes and United States Notes are "redeemable in gold" but are not "GOLD CERTIFICATES" and are not required to be surrendered

Special attention is directed to the exceptions allowed under Section 2 of the Executive Order

CRIMINAL PENALTIES FOR VIOLATION OF EXECUTIVE ORDER
$10,000 fine or 10 years imprisonment, or both, as provided in Section 9 of the order

Secretary of the Treasury.

U.S. Government Printing Office: 1933 2-16064

Found at: http://upload.wikimedia.org/wikipedia/commons/a/a1/Executive_Order_6102.jpg