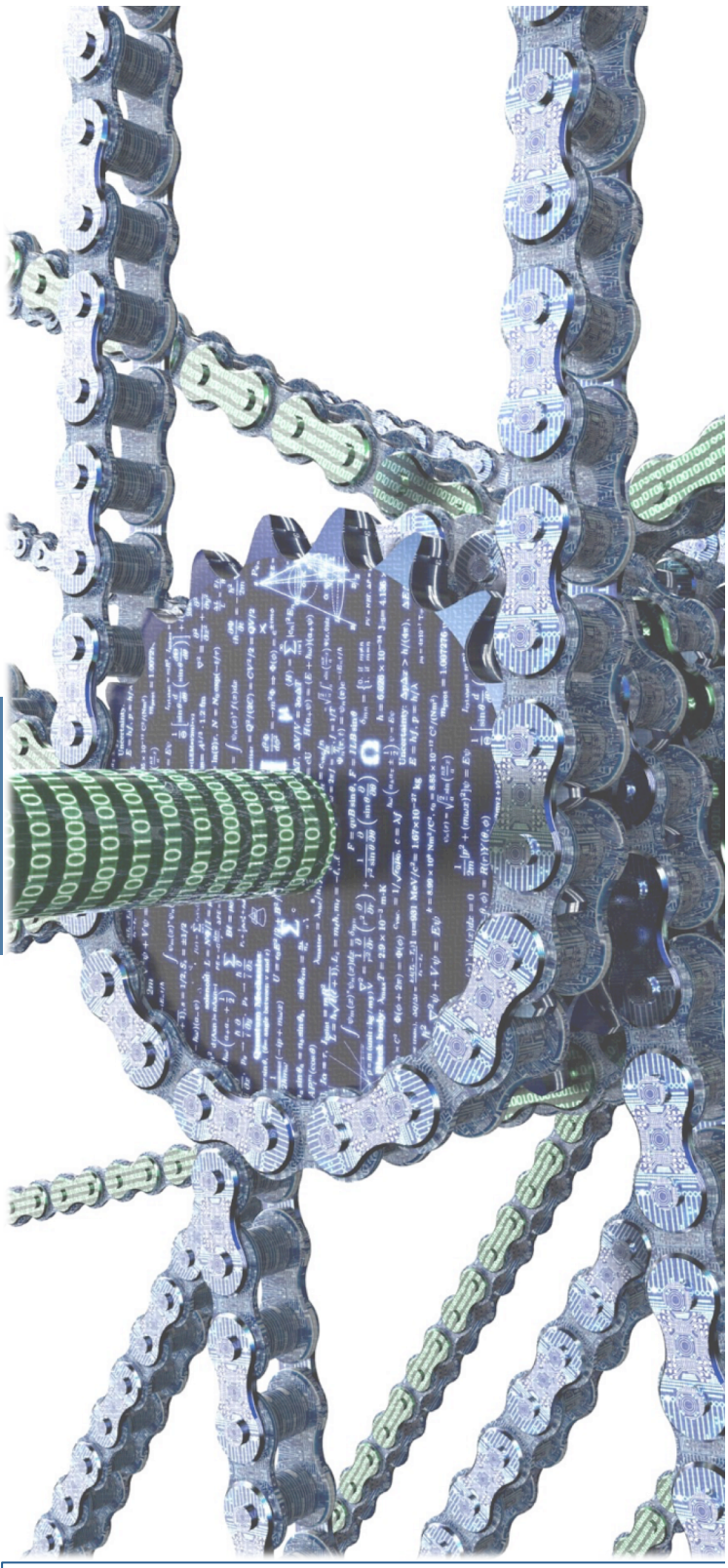
CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

An analysis of cryptocurrency as a monetary unit



Master Thesis

Sigurd Nordahl

Supervisor: Søren Korsgaard

MSc. Applied Economics and Finance

Copenhagen Business School

15th May 2017

Pages/Characters: 64 - 106430

Abstract

The purpose of this thesis is to give a comprehensive analysis of crypto currency from an economic perspective. In doing so, Bitcoin will be used as a basis for the analysis, and bitcoin will therefore be mainly used as the example of crypto currency.[1] Thus, the central question that will be investigated is:

> To what extent does crypto currency satisfy the requirements typically served by money?

In order to come up with a meaningful response to this question the thesis will start off with clarifying basic money theory. The intention behind this is to lay the basis for a framework in which will include different kinds of money and sort them by characteristics. Crypto currency will be categorized and allocated accordingly before moving on to the analysis. Considering the technical aspects of crypto currency the developed framework can be applied to identify it as digital commodity money. In this way potential uses of bitcoin are discussed, supporting its value. Moreover, it will be argued that commodity money and thus bitcoin can circulate without use value and state backing, and this is supported by examples from the real world. In addition, Bitcoin´s potential for disruption are discussed and finds that it can be applied to several functions of the economy.

[1] This thesis will use the term Bitcoin for the protocol and payment network, and bitcoin for the currency (BTC). This distinction with small and capital b is commonly used in the literature.

Table of contents

Introduction

One might argue that there are 3 eras of currency: Commodity based, politically based, and now, math based. That is, if one have faith in crypto currencies. This thesis will focus on the latter and investigate how it performs compared to money. Money has many forms and has existed for a long time. On the contrary, crypto currency emerged in 2008, and this thesis investigates whether it can be considered as a form of money. Fiat money might be the most common way of payment today, and the characteristics behind this invention can be discussed through the eyes of economics. As questioned by Milton Friedman:

"Why should they also be accepted by private persons in private transactions in exchange for goods and services? The short answer—and the right answer—is that private persons accept these pieces of paper because they are confident that others will. The pieces of green paper have value because everybody thinks they have value. Everybody thinks they have value because in everybody's experience they have had value"...) (Friedman, 1992, p. 45).

It is safe to say that there is no consensus in the academic literature regarding how money obtains value. Moreover, price and value are not always the same. One of Warren Buffet´s well known quotes also touches this issue: "Price is what you pay, value is what you get." However, this thesis finds that crypto currency satisfy the requirements served by money and identifies it as digital commodity money. Considering transaction costs as the cost of operating and enforcing property rights, it is argued that blockchain can disrupt this via decreasing the transaction cost and thus increasing the welfare level of the economy. Further, this thesis goes beyond that and finds a huge potential for disruption in the underlying technology of crypto currencies.

In 2008, the financial crisis was one of the pressing issues of the world economy. Several memorable economic happenings took place at the time such as bankruptcies, bailouts and changes in interest rates. A more discreet happening was the publishing of Satoshi Nakamoto´s paper "Bitcoin: A Peer-to-Peer Electronic Cash System". The research paper

was distributed that year in October through a cryptography mailing list.[2] The e-mail described a payment system innovated by Nakamoto, and bitcoins was the unit in which the system was built around. Nakamoto is a pseudonym and thus the person or persons behind it are anonymous to this date (Nakamoto, 2008).

This led to something remarkable in the Internet community. People worked together to create the Bitcoin network based on the protocol written by Nakamoto. This process took less than a year, and everybody worked for free. It is fair to say that the Internet community created something out of nothing, and the Bitcoin network has grown tremendously since. As a result, the market capitalization today is exceeding $15 billion with close to 13 million users[3]. Moreover, the network has so far attracted over $496 million in venture capital investments (CoinDesk, 2017).

The Bitcoin network has been subject of controversy and central banks, governments and persons of academia have expressed their negative assessment of Bitcoin. The latter has discussed several aspects of the currency, raging from whether or not bitcoin is a bubble to if the whole thing is a Ponzi scheme. In addition, well-articulated persons from the business community have also in many cases doomed bitcoin. Warren Buffet has questioned its intrinsic value,[4] while Bill Gates has opposed one of its main functions.[5] Moreover, several central banks have warned to not engage in the system, and certain countries have banned it completely (Smart, 2015).

On the other hand, Milton Friedman predicted digital currency already in 1999 (Cawrey, 2014). Furthermore, the former CEO of Google, Eric Schmidt, have claimed "The ability to create something which is not duplicable in the digital world has enormous value" (Millet, 2014).

This gives raise to the question why there are so many disagreements regarding crypto currency. One of the potentials of Bitcoin is to disrupt the function of the central banks

[2] Available at http://www.metzdowd.com/
[3] This figure is rapidly growing – see https://blockchain.info/no/charts/my-wallet-n-users?timespan=all
[4] (Rizzo, 2014)
[5] (Hajdarbegovic, 2015)

by eliminating the need of the trust offered from these institutions. In order to do that, crypto currencies have to fulfil the different functions typically served by money. This thesis will investigate whether or not something created out of nothing can at all obtain value. This raises the question of what money is, and thus what it means and how it can be given value. One of the central questions is also how likely it is that people will adopt crypto currency, as it has historically been very volatile. Moreover, various academics and newspapers have given the death sentence to crypto currency since it first was issued, something that has happened 129 times since 2010[6].

Economic considerations

While crypto currencies is somewhat technically complex, it is essential for this thesis to examine the currency from the economic viewpoint, and thus what it potentially can do in the economy. In other words, expert opinions from the law and IT areas of expertise will not be emphasized. Thus when discussing the uniqueness of crypto currencies, it would be suitable to follow "The Theory of Money and Credit" by Mises (1981).

One might argue that economics is the study of resources and how to allocate these efficiently. Having that in mind, this thesis will focus on a less popular theme from the literature, namely transactions and transaction costs. To fully understand the potential of crypto currency and its underlying payment system, it is crucial to investigate transactions.

Research question

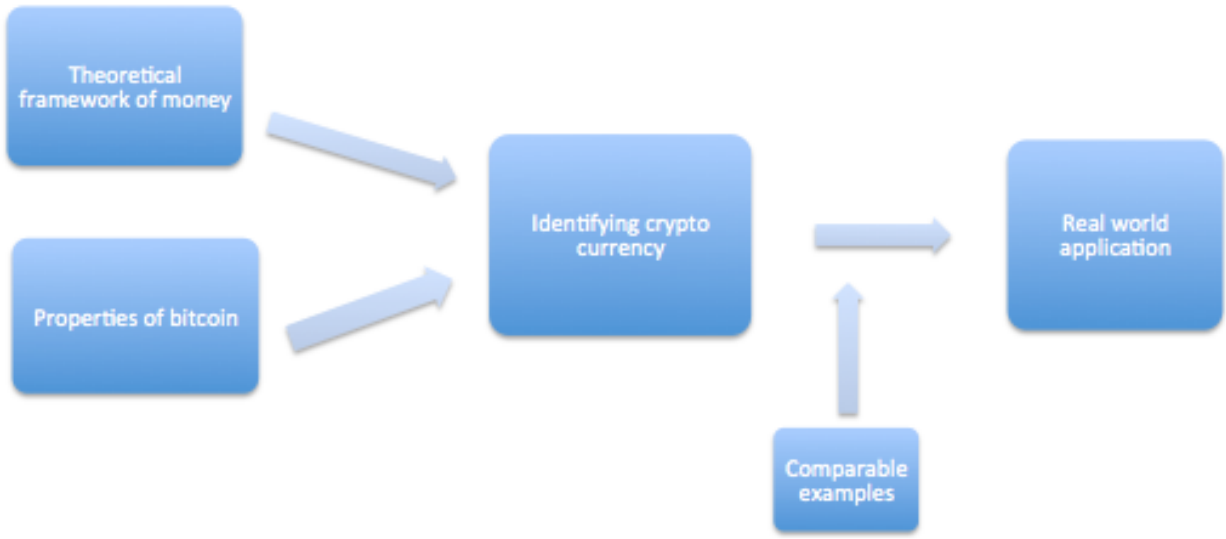
The purpose of this thesis is to give a comprehensive analysis of virtual currency from an economic perspective. In doing so, Bitcoin will be used as a basis for the analysis for blockchain, and bitcoin will therefore be mainly used as the example of crypto currency. Thus, the central question that will be investigated is:

To what extent does crypto currency satisfy the requirements typically served by money?

---

[6] Continous count at: https://99bitcoins.com/obituary-stats/

In addition, as a consequence of this question another one rises. Specifically, how might the technology behind crypto currency be a disruption in regards to more traditional money? The aim of this thesis is to answer these questions. In order to do that, economic theory will be used to give a persuasive insight into money. This will also form the basis for an analytical framework, which in turn will be applied to give a full economic understanding of crypto currency as well as the underlying technology. The thesis will then continue to give an overview of the potential that lies within Bitcoin. This method can be summarised in the figure below:



Defining Money

Economic literature often describes money through its functions. Among these, most emphasis is placed on the function as unit of account, medium of exchange and store of value (Mankiw, 2010). While this help explaining what function money has, it is more unclear what it takes to call something money. It is fair to argue that this is also something that is not easy to get a full understanding of when studying mainstream economics. When examining the Walrasian equilibrium through the neoclassical AD-model,[7] the assumptions lead to a frictionless view of the economy. As a result, there must be a set of prices such that aggregate supply will equal aggregate demand for every commodity in the economy and thus money is not needed in its traditional sense (Arrow & Debreu, 1954). Moreover, applying New-Keynesian models to economies with no money shows that it is inadequate to adjust the neoclassical framework by adding more friction in order to act as money. Thus one can argue that payments are vital for real-world economics (Kahn & Roberts, 2009). Foss & Mahnke suggests that the transaction be made the basic unit of analysis as argued by transaction economists.

As mentioned above, mainstream economics does usually not go into specifics when analysing money. However, due to the nature of money, various schools of thought have studied the matter. Historical persons and great thinkers have contributed to the literature, such as Aristotle, Sigmund Freud and Karl Marx to name a few (Smithin, 2002). The high interest in the origin of money has made the subject covered in a wide-ranging fashion, and become the subdivision of economics covered most substantially historically. However, as with many topics in economics, there is a high degree of disagreement when it comes to what part money plays in the economy. According to Lapavitsas, money is something that shows how humans interact with each other, and also how complicated those relations can be (2004). He goes on to argue that money will be socially consumed, while owning it is merely personal.
As money can be considered as a social construct, this thesis will underline the social aspects of it. Hence, a theoretical framework will be developed. In order to achieve this, a few economic concepts will be explored, such as liquidity, types of money and transaction costs. The intention behind this is to disclose relationships that yield more insight to answer the research question.

[7] Arrow–Debreu model

Liquidity

Prima facie, assets can be divided into two categories, namely non-money and money. This is also the norm in monetary economics. It is fair to suggest that this way of dividing assets is a neat one, however there might also be some drawbacks to it. It might be hard to see how financial constraints impact the market forces of the economy. Lapavitsas states that money must be the asset that is most liquid (2004). In other words, it must be the most appealing asset, so that one can increase utility by trading products for it. Consumers and producers in the market take it for granted that money can buy things in the future and shows that money has a role in production. This in turn will continuously be reinforced, as this type of consent will effectively have a monopolizing force and thus the result will be that money is the only asset that consumers will be able to purchase goods with (Lapavitsas, 2004). On the other hand, one might argue that all assets can be used for exchange. Nonetheless, it might be problematic using non-money assets, as it might not be discounted to its market value easily. Moreover, all assets have a degree of *moneyness*. This should not be confused with the same term used in finance, but can rather be described as *"The degree to which an asset approximates cash in its ready liquidity and the low transactions costs in realizing that liquidity"* (Drake, p.98, 2004). One might say that the degree of moneyness an asset has depends on the characteristics of the market, and also differ among assets. In other words, demand and supply will be a substantial backbone of the assets moneyness and thus change in response to changes in the market.

One might argue that money is not an economic concept that is easy to neither distinguish nor describe with a clear definition and delimitation. In order to get a full understanding of money and its dynamics, it might be wise to look closer into what makes assets have higher degrees of moneyness than others. To this end, one should consider addressing the way money is analysed when exploring what affects assets' liquidity.

One of the classic debates when it comes to the topic of money is the Chartalist theory versus the Metallism theory. The central argument of the former is the based on money as a unit of account, where the value is determined by what the government will accept

as payment for tax obligations. In shorter words, Chartalism argues that money does not have intrinsic value, but is given value by the government. Thus, money can be seen as a form of debt, and as a result the moneyness determined by the obligation (Graeber, 2011). On the contrary, Metalissm´s argument centre around money as a store of value, and states that for an asset to hold value, it must store value in itself. Mises states that the value of money derives from the purchasing power of the commodity upon which it is based (2009). Accordingly, what decides the moneyness is very materialistic in the sense that there are no social regards to the store of value. Mises goes on to argue that the other functions of money are derived from its perspective as medium of exchange.

As seen above, there are many ways to analyse money, where the only common denominator seem to be opposing views. That being said, it is fair to argue that to some extent these theories fulfil each other. What are notable from the above theories are the different social relations concerning the different functions of money and thus the drivers behind the degree of moneyness. On the other hand, these theories might be seen as quite specific in their nature and so gives not a clear picture of how to assess money. For that reason, when discussing theory in order to come up with a framework for the identification of crypto currency, it might be helpful to look closer into a more general analysis of money.

Transaction costs

Imagine an economy that has the properties of production technology and resource endowment. The agents have individual preferences and are pursuing utility maximization. Because of individual preferences, one can sum all utilities to calculate the welfare level of the society. Hence, any allocation of utility can be arranged hierarchical to follow the Pareto principle, and every allocation will have different utility levels.

Transaction costs will have a negative relationship with the welfare level, as it will impact the interaction among different agents. At the bottom level of welfare the society can be described as one with *autarky*, and this is where transaction costs will be at its highest level. In other words, this is when there is no exchange at all. In essence, the

importance of transaction costs is due to it driving a wedge among individual´s *MRS*[8]. Furthermore, transactions costs might be calculated as the wedge among the individual´s MRS, and reducing this wedge might increase the welfare level. As a consequence, high transaction costs results in high *WTP*[9] for a solution to overcome it.

Transaction costs can be described as the costs of operating and enforcing property rights and thus the costs of running the economic system (Williamson O., 1989). When considering a game theoretic framework, it is fair to say that transaction costs have a differing description, namely the cost of containing freeriding, distribution and conflict, and coordination. Using transaction cost economics, it is possible to analyse all allocation effects of money. However, this requires the assumption that preferences do not depend on transaction costs.

One can argue that both social and physical barriers contribute to transaction costs. Nevertheless, while these barriers can intervene each other, it is fair to suggest that social barriers are mainly resolved with organisations and physical barriers with technology. Moreover, with improvements of technology it becomes easier for agents to barter directly with each other. This in turn will decrease transaction costs and thus increase the number of possible allocations of welfare utility. However, there will to some extent still be transaction costs as a result of incomplete contracting. That being said, an economy with direct barter is more Pareto efficient than one in autarky. One should also keep in mind *the coincidence of wants problem* when discussing barter. This problem will keep the economy from reaching the highest possible level of welfare.

As mentioned earlier, money is often described through three functions. Moreover, it is possible to connect these three functions to the three categories of transaction cost mentioned above:

[8] Marginal rate of substitution.
[9] Willingness to pay.

Function	Problem	Solution
Medium of exchange.	Double coincidence of wants.	Money lowers the cost of coordination.
Store of value.	High cost of containing free riding.	Money only provides purchasing power to its holder.
Unit of account (measure of value).	High cost of conflict.	Money reduces the difficulty of agreeing to a certain distributional outcome.

Next, it could be helpful to look closer into an economy where the highest level of welfare is accomplished. This is in order to understand how transaction costs can be created as a result of money, and also how various types of money can affect transaction costs. This can be done be considering an economy with a perfect public record: the set, which manages to successfully operate with an incentivized allocation, would be the most Pareto efficient one (Kocherlakota, 1998). That is if the record would show what market production all agents had done, and all other agents could see it in the record. This in turn can then be represented as a game of iterated prisoner's dilemma, where the agents provide and collect with respect to the market, in a way that they don't profit, but rather in a zero-sum fashion. Collecting something from the market before providing will thus be public to all agents, and will lead to a request for replacing something of equal value in the future. If the request is not fulfilled, the unreliable agent will then be identified and banned from taking part of it in the future (Diamond, 1990). This in turn will motivate optimising agents to follow a tit-for-tat strategy, and the dominant strategy would be cooperation.

If one were to apply this theory to the real world however, it becomes clear that some parts of it are not realistic. A public record as the one described above does not exist, and it is not realistic to identify unreliable agents in order to get them excluded. As a result, one cannot call this a realistic game of iterated prisoner's dilemma but rather a series of static games. This in turn will change the dominant strategy to one where every agent becomes unreliable and does not contribute to the market at all. This will be the

dominant strategy because it is uncertain whether or not other agents cooperated or not, as there is no way to know. Conclusively, the economy will thus go back to direct barter.

Since the economy will be one of direct barter without a public record, one possibility is to use something that substitutes its function. One such substitution can be money, not because it is a public record, but can act indirectly as record by being credible as a *Proof of Work*.

Types of money

Commodity money

In an economy based on a monetary commodity system, one might argue that a good that is expensive to produce might serve as such a proof of work. An example of this might be different kinds of metals, such as gold and silver. These metals can only be attained in two ways, either purchasing them from the market with other goods one might have, or digging for them personally. Assuming perfect competition, in an economy where gold is used as money and the system is based on ownership of the factors of production, the ratio of work required to produce goods to work required to produce gold must equal the price of goods. If not, ROI[10] would be different amongst the different industries, and no agents seeking to maximize profit would invest in the less profitable industries.

$$Value\ of\ Commodity\ money = Production\ cost\ of\ commodity\ money$$

This however, is true over time and both the value and cost of commodity money are usually codetermined, and do not have a causal relationship. Hence, if the economy has stable production costs, the prices will be stable. Moreover, gold will serve as an indirect public record and thus be reliable to the people using it as a currency.

[10] Return to Investment

Whether or not a commodity money is easy to divide, store and identify will affect to which degree it will be adopted. When the functions of the commodity money such as a medium of exchange gets more widely spread, agents will be more confident when predicting the future demand of it. This is what is meant with identifying money, and as a result, demand will develop to be less sensitive to unsystematic shocks.

In "The Theory of Money and Credit", Mises outlines a regression theorem where adaptive expectations are assumed. He argues that because of network effects, what engenders present-day money is the agreement of that currency being reliable in the past. On the other hand, in Austrian economics, money has to come from an object with use value, being used as an input in production or increases agents' utility (Rothbard, 1976). This is in contrast to what Mises argues, albeit he also being from the Austrian school. Moreover, the regression theorem concludes that agents following a trigger strategy with an act of trust and forward looking expectations will function just as well as any use value.

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.

Fiat money

An economy with a commodity money system is more Pareto efficient than a barter system and increases the incentive-feasible allocation region (Nosal & Rocheteau, 2011). On the other hand, one might argue that commodity money has a high resource cost and is thus a costly way to create money. Furthermore, it will not be necessary to spend any resources in e.g. gold mines if a social planner can offer a reliable *proof of work* to agents offering their goods to the market. Hence, the most inexpensive way to get other goods

will be through agents offering their production to the social planner. This in turn will also be how agents get money. In comparison with a commodity monetary system, what enables the money to have the function of reliable record keeping is the underlying work behind it. In a commodity monetary system the resource cost represents a rent. This rent in turn provides the basis for the development of institutions offering less costly trust, and thus achieving profit by virtue of *seigniorage*[11]. In absence of a trustworthy social planner, a reliable government could replace its function. The government could thus operate in the same fashion as the gold mine, but instead exchanging work for money tokens. The ratio below shows how prices in state money would be determined:

$$\begin{gathered} required\ work\ in\ production \\ \div \\ work\ required\ to\ obtain\ the\ money\ from\ the\ state \end{gathered}$$

Furthermore, the state increases its flexibility concerning government spending if it also welcomes state money as payment for taxes. In addition, the purchasing power of the money will remain the same if the state chooses to adjust the difficulty to acquire its money.

Fresh fiat money can theoretically be injected into the economy through government spending. Keeping that in mind, it is fair to say that usually in an economy, there is a central bank that issues money. Such an institutional structure is one where money gets created through extension of that central banks´ balance sheet, and thus a result of increased credit. However, it would not be correct to characterize or confuse fiat money with credit money, because it does not have a claim on anything. Hence, this analysis of fiat money ought to be applicable and be equipped to hold.

Credit money

One of the traits with a system that uses fiat money is that the resource costs associated with a commodity monetary system is almost eliminated, and accrues to the central

[11] The difference between the value of money and the cost to produce it.

bank as *seigniorage.* Agents in an economy depend on the possibility to collect from the market before they produce in order to reach a complete set of incentive feasible allocations with a perfect record. This has to be applicable to both the individual and government level. Moreover, if the social planner knew the level of autonomous expenditure in the future, it would be no risk associated for her to let agents issue private debt. Debt would in this case be a *promise to work*, and thus be the same as a *proof of work* from the future. What is more, a risk free *I owe you* will thus function as a *promise to work* for the creditor and a *proof of work* to the debtor, as in the nature of debt creation. Thus, working would be the only way to acquire other individuals *I owe you´s*, and the value of them would depend on the work required to make this happen[12]. As a result, an *I owe you* with zero risk would thus circulate as money.

This is also 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.

One might argue that in the real world, *promises to work* are not free of risk. According to Kiyotaki & Moore, the cost of acquiring private information from the issuer makes *I owe you´s* circulate at a discounted rate because of incomplete contracting (2000). Moreover, when they are exchanged among private agents, one might say that they have a high degree of moneyness, although cannot be categorised as money. The result from the difference in market value and face value of private *I owe you´s* is thus a generator of rent. This in turn motivates institutions to offer private information at a lower cost than the market, and has given rise to banks. Banks are making a profit from issuing *I owe you´s* that have the ability to circulate with a higher degree of liquidity and thus moneyness than the assets they acquire. The profit is made through the difference, and so they are taking advantage of increasing returns to monitoring and diversification. Banks earn *seigniorage* in the way that they produce money through lending, as the deposits usually circulate at *face value*[13]. There seems to be conformity in the literature about banking, regarding their existence. They are often described as the financial intermediary between borrowers and lenders, acting as maturity transformers (Freixas

[12] As with commodity and fiat money, this is also how the value would be regulated.
[13] i.e. money.

& Rochet, 2008). It is fair to suggest that banks have many roles, however their main function is to make a profit. This profit is made as following:

$$moneyness\ of\ assets - moneyness\ of\ liabillities$$

Electronic money

Modern technology has spread across the world the recent decades, and as a result money is not something that is delimited to the real world any longer, but is also a digital phenomenon. In comparison with money in the real world, there are different kinds of electronic money. It is fair to suggest that the Internet is a platform where humans can interact and create relations. Moreover, one can apply the analysis above regarding how institutions emerge to the digital world. In other words, electronic money acts in accordance with money in the real world, and thus cannot be categorized as a type of money but is rather an umbrella term. Moreover, modern technology has also brought online platforms where *Virtual Currency Schemes* is often used (European Central Bank, 2015). This is often used in online games, and should not be confused with electronic money, as it is not a portrayal of other kinds of money but rather represents itself.

In many cases, e-money is just a digital representation of normal credit or fiat money.

The European central bank uses three different categories when describing *virtual currency schemes*. They are differentiated by their ability to flow from one currency to another.

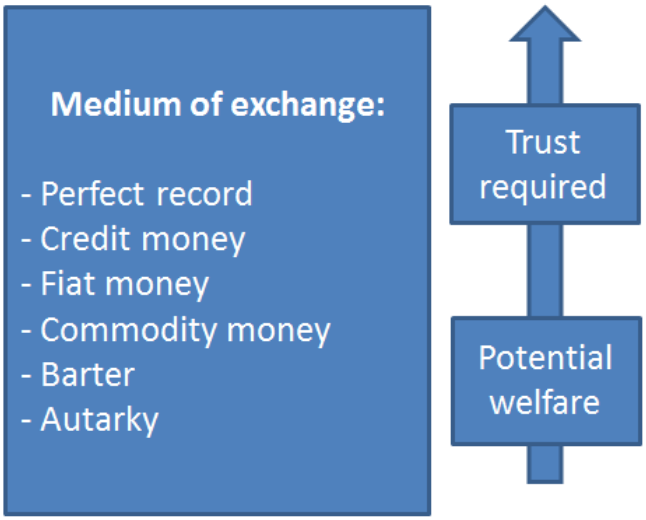
Virtual Currency Scheme:	Description:	Example:
1. Closed systems	Often in computer games.	Age of Empires
2. Unidirectional flow systems	"Normal" money can be converted into non-redeemable tokens.	Minecraft
3. Bidirectional flow systems	Agents are free to trade in and out of their position in the virtual currency schemes.	Second Life[14]

Moreover, one might argue that changes in virtual currency schemes to a small extent, if any, have the ability to affect the real economy, and that this sort of influence will mainly come from the third category.

Because one has the possibility to continually exchange bitcoins with other types of currency, it is placed within the third category. On the other hand, it is safe to say that there are many differences between the currency used in Second Life, bitcoins and other virtual currency schemes. One of the main characteristics that make Bitcoin unique is the lack of a *centralised monetary authority*, such as a central bank. Hence, this one of the critical traits that enables bitcoins to be called electronic cash. In other words, electronic money can be described as centralised whereas electronic cash cannot.

Different relationships, different money

As mentioned earlier, electronic money is ordinary money put in an electronic context. Furthermore, from the analysis above, one can conclude that credit money is the most efficient money, followed by fiat money and commodity money respectively. This in turn raises the question as to why there are so many different kinds of money. It is fair to say that different types of money require different degrees of trust. Moreover, with this increased degree of trust comes increased potential of welfare. Thus, one can suggest a hierarchy of money as the one depicted below:



There is a lower transaction cost associated with the use of money, however this is a cost that every agent face individually, and which is independent to the cost of the economy. Keeping that in mind, agents stand freely to create their own money. In this situation, the above claim would not hold. The reason behind this is essentially due to the relationship between money and its market, and thus not any market.

As argued in Coase (1937), Alchain and Demsetz (1972), and Williamson (1985).

Transaction costs are what makes institutions arise in the economy. It is standard for an economy to systematise the market with prices expressed in the economy´s money. On the contrary, at the internal level in organizations money often become unnecessary when regarding money as a record device. This is due to accounting and the following centralised planning done in a way to avoid transaction costs associated with using money. One might say that this describes a *perfect record* internal in the firm. In addition, as economic agents establish relationships, it often evolves into relationships where credit has a central role (Jin & Temzelides, 2004). To this end, as these relationships mature the agents get to know a lot of information about each other, and they get dependent on each other. Moreover, trade credit might circulate in their joint production chain. To this end, the organisations start to *trust* each other. Furthermore, the production chain thus depends on internal credit money from the firm, and trust function as a backing of circulation of credit.

Trade credit from a particular production chain normally only possess a degree of moneyness, and is not money relative to the rest of the economy.

State backing

In economies at the country level, it is fair to say that the government is usually the largest and most essential agent. The state has superior power, and can decide things such as monetary policy, whether or not to impose taxes, and how to regulate the law. Throughout the country fiat money might circulate, and the money will be reinforced by the citizens through their trust to the system and the stability of its monetary policy.

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. For international settlements, no national currency was trusted without commodity backing up until 1971. Nevertheless, the US position as the absolute hegemon in the West after the Nixon shock enabled the USD to fulfil the role as the fiat money of the world.

The social aspect of trust

As implied earlier, the function of monies as a trusted record keeper will influence to what extent different agents choose to use them. Shubic claims that from a game theoretic perspective, the optimal money has the ability to be a perfect substitute for trust (2004). Nevertheless, this is not applicable to the real world, as efficient money has a negative relationship with required trust.

In an economy with direct barter, there is no need for trust between the agents. This is also true for an even simpler economy such as one with autarky. When considering a commodity monetary system there are two aspects of trust that are vital. Firstly, the cost of production must maintain a stable inflation. Second, the market has to be in the agreement that the commodity money used today will also continue to be used

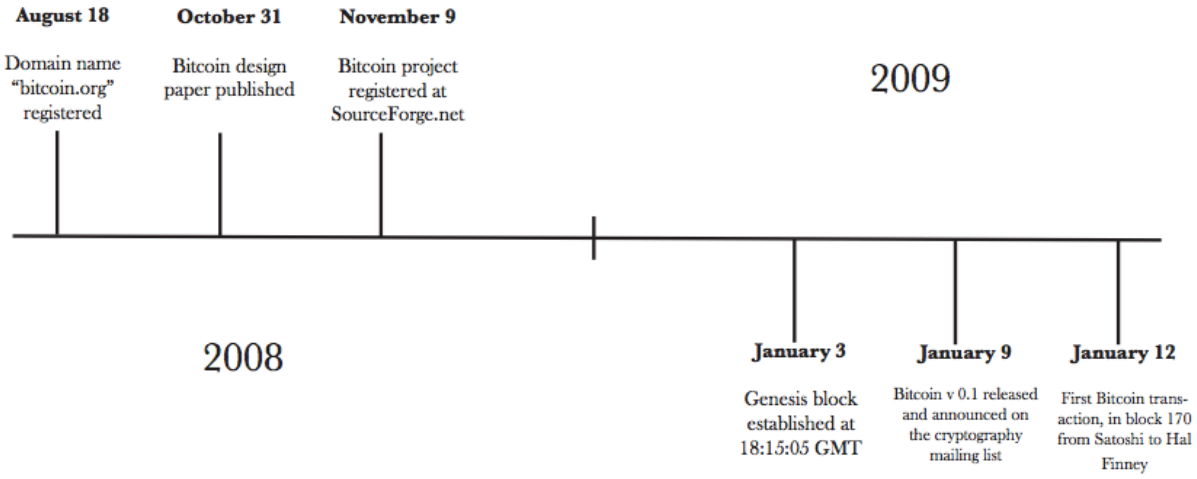
tomorrow. The agents of a monetary economy will cooperate if they find it beneficial, assuming that trusting the commodity monetary system is less costly than the benefits from participation. Moreover, considering this market as an expanding network, the cost will decrease and benefit increase as a result of positive network effects.

In an economy with a fiat monetary system however, more trust is required. As mentioned earlier, it is necessary that the agents trust the monetary policy. In addition, the taxes imposed by the central bank will also create trust in the fiat money issued by the government. This facilitates the substitution for commodity money. Having said that, it is fair to suggest that it is more difficult to establish trust in the monetary policy of a central bank, than something simpler, like the cost of gold production. This is due to the lack of power a gold mine has to affect or manipulate the cost of production of gold. This is in contrast to what a central bank or government, which has various motives and political aspects to take into consideration. To this end, the government has the ability to make it harder for agents to acquire money, by actively influencing its fiat money. Controlling money like this is one of the powers that a government will hold in a fiat monetary system. Further, having control over money creation may thus be self-reinforcing for the government´s power.

When considering an economy with credit money, there is a shift in trust. Now, individual agents as issuers of debt must be trusted instead of a network. One must give up the anonymity that is associated with other forms of money in order to trust an individual debtor. In other words, agents must sacrifice their privacy in order for credit money to work. Further, it has to be very costly to default. Due to the reliance on credit relationships, informational and enforcement costs will increase (Kahn & Roberts, 2009).

Defining the underlying technology of Crypto currencies

In order to get a full overview of crypto currencies as an economic concept, it could be helpful to look closer into the underlying technology of it. This section follows the technical research done by Swan (2015) and Franco (2014). As stated earlier, this invention is based on the paper by Nakamoto and describes the payment network that is named Bitcoin, however all crypto currencies are based on this technology and Bitcoin is just one of several blockchains. In other words, the underlying technology of crypto currencies comes from the payment network that Nakamoto called Bitcoin. The timeframe below shows how it all began:



Source: 1 Crosby et al. 2016

Bitcoin can be described as a public ledger, which functions as an operator for private property rights for bitcoins. This also applies for *Ethereum* and its virtual units *ether* transferred within that network. Working in the Bitcoin protocol requires that one operate with the correct scripting language. This allows for operating entries in the Bitcoin protocol, and the protocol in turn administers the interaction among peers. One can say that the network is governed by the protocol. One of the key characteristics of this protocol is that it is open source[14], and that it creates a peer-to-peer network. The central function of this protocol is to transfer electronic cash personally from one peer to another. In other words, the network is decentralised, and thus there is no need for trusted third parties. Hence, with crypto currencies, the banks no longer have a function as with other moneys. There is no need to help agents exchange *I owe you´s*, followed by

[14] Freely available to everyone with access to the Internet.

the verification of fiat currency or other assets. In the Bitcoin protocol, transactions of bitcoins is secured and verified, thus neatly solving the *Two Generals Paradox.*

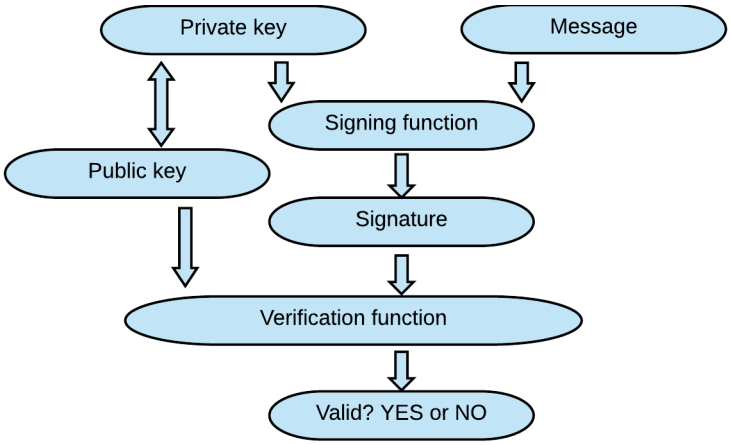
> A group of generals, each commanding a portion of the Byzantine army, encircle a city. These generals wish to formulate a plan for attacking the city. In its simplest form, the generals must only decide whether to attack or retreat. Some generals may prefer to attack, while others prefer to retreat. The important thing is that every general agrees on a common decision, for a half-hearted attack by a few generals would become a rout and be worse than a coordinated attack or a coordinated retreat (Lamport, Shostak, & Pease, 1982).

Transferring crypto currency

When describing cryptography it is common to use the names Alice and Bob for illustrating two different peers in a network. Computers participating in the work of maintaining the ledger are called nodes. Hence, if Alice decides to send Bob some bitcoins, she can just send this information to the network. At the other end of this broadcast are the nodes, which in turn manage the message of transaction and update their copy of the ledger. A *digital signature* ensures that the message has authenticity. Both Alice and Bob needs accounts in order to successfully transfer money, and these are public accounts better known as public keys. Moreover, in order to spend money one also need a private key, and one is useless without the other. Two such public accounts are depicted below:

As one can see from the above illustration, the public keys looks unrelated. However, the system is designed such that mathematically, they are related. Moreover, a unique signature is created when connecting the private key and the message of transaction, taking the form of a mathematical function. Alice´s account and her message is then sent to a function in the network that verifies, along with the signature. And so when the signature gets verified, the transaction from Alice to Bob gets validated. It is important to underline that Alice´s private key stays undisclosed, although the interaction between

the public and the private key is what makes it possible to confirm whether or not her private key was applied to create the signature. This can also be represented in a figure:



Keep in mind that this is a simplified explanation of how the digital signature works. Digital signatures are used to verify transactions. Moreover, it is important to stress that it is not possible for other peers to reuse or copy signatures that have been used. In addition, if one were to try to change past transactions, the signature would become invalid because of the message tied to it. This is one of the traits that make the Bitcoin network unique. As an analogy, one can think of a vault where deposits are only possible, unless the bank manager comes along with the key to open it. This also applies to sending bitcoins to another peers' public key.

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.

A chain of transactions

Referring back to the previous section, verification of transactions requires verification of signatures. However, the network does not contain any balances or records of accounts. In a different manner, the network keeps a transaction history of all units of bitcoin ever made. The verification of links to past transactions validates who owns the bitcoins. Hence, if Alice wants to send bitcoins to Bob, the message must contain both

transactions of how much she wants to send to Bob, and also show how she got that amount of bitcoins from before, for the signature to be created.

New transactions are better known as *outputs*, whereas incoming transactions are known as *inputs*. When Alice sends bitcoins to Bob, and does not possess the exact same amount of bitcoins as she wishes to send, the remaining bitcoins she has will have to be sent back to her as change. After this, the nodes will investigate whether or not the input adds up to the output and that Alice is the rightful owner of the input. If this is correct, the new transaction will be verified, and when the transaction is verified it is irreversible. This is done to make ownership of the bitcoins unmistakable.

The latest transaction combined with the whole chain of transactions from the past, decides whether the latest transaction is valid or not. The whole chain of transactions must be verified in order to give validity to the last transaction. It is fair to say that this process requires a lot of energy[15] and time, although it only has to be done once.

When a protocol is open source as in the case with Bitcoin, every user of the network has the opportunity to write their own software as long as they follow the rules of the protocol. However, one of the drawbacks of the system is that if one were to write something wrong when programming, there is no way to undo it. This also applies for someone losing their private key, resulting in loss of all the bitcoins. One possible solution to this problem is using third parties offering their software/service.

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.

Avoiding duplication

One of the traits of Bitcoin is that it avoids double spending, as the inputs can only be referenced once. In other words, the inputs can be use one time only. The contrary

[15] As this process is done through very powerful computers, this requires big amounts of electricity.

would result in inputs having the possibility to being referenced in earlier transactions. However, the nodes examine whether or not this is the case by matching the transaction with an index of unspent transactions. Albeit this process is done rapidly, the challenge lies in verifying the order of the transactions. In other words, if a transaction is referenced more than once, it is of vital importance for the system to have the ability to verify which of the references that was made first. On more traditional online payment systems[16] that are being used today, each transaction is logged on centralised servers. This is in contrast to how the Bitcoin network works. Hence, the nodes must be able to handle transactions that are sent at different times and order. As a result, this enables Alice to make an agreement with Bob where she buys something of his, and then reference the same input on something else while waiting for the shipment. The problem would then be that the second transaction from Alice would be registered first, and so the one to Bob would not be valid. However, Nakamoto provided a solution to this kind of situations. He created what is called a *Distributed Timestamp Server*, which is a form of *proof of work* scheme in the Bitcoin protocol.

A chain of blocks

As described in the paper by Nakamoto, the nodes collect the transactions that aren't verified and put them together to make a block. Moreover, the blocks will be referenced so that they become ordered systematically by sequence. This is different to a transaction chain, as a block will always be referenced to a previous block.

It is important to notice that the blockchain 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.

Moreover, when these blocks are created, the transaction within share a timestamp given by the block. The transactions which are broadcasted and do not yet have a block are pending and stays unconfirmed. The unconfirmed transactions are waiting on nodes

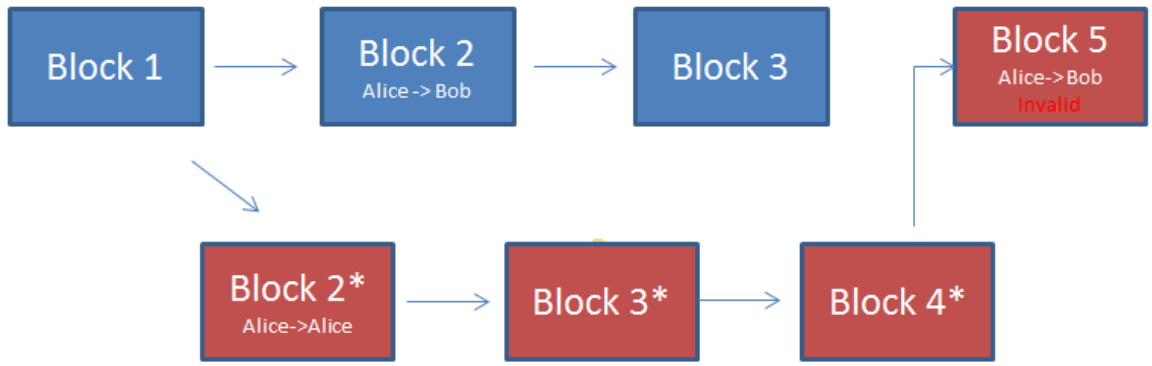
[16] E.g. Google Wallet or Paypal.

within the network to suggest and create blocks. This process of making new blocks takes form of a mathematical problem that a node tries to solve. Furthermore, *proof of work* in this setting refers to the process in which the node uses computing power to guess the solution. As mentioned earlier, this requires a lot of capacity from the computers (nodes) as well as energy. However, a node might use little energy and time to come up with the solution, if it is lucky (trial and error). The protocol was designed to regulate how much time it takes to create a new block, and takes approximately 10 minutes. For the network to adjust for the improving technology and increasing computing power by the nodes, the system changes the degree of computing power needed to solve the problems. In other words, the mathematical problem gets harder to solve as time goes, something that gets adjusted every fortnight. When a block is completed, it gets broadcasted and accepted, before the network starts working on a new block. Keeping that in mind, there is a possibility for two blocks being completed and broadcasted at the same time. In this case, the finished block will be separated into two different branches. This creates a doublet of the blockchain, however the nodes continue building new blocks on the first one they receive. As a result, one of the branches have one more block than the other, and thus the system adjust so that it continue to build on the version with most blocks, one can say that the system shifts to the longest branch. In this way, it is full agreement within the network what order the blocks have. One should also note that it is a very rare occasion when two blocks gets completed simultaneously, especially repeatedly. However, when such a branching of the blockchain do happen, the transactions from the block that is not going to be used as a further building block will not be used and thus go back to being pending unverified transactions. Hence, they have to wait to be contained in a new block.

The threat of hacking

One of the threats to the Bitcoin network stems from the circumstance that it might be branched over a period of time. This is due to additional possibility of double spending. Take again the example of Alice purchasing something from Bob that needs to be sent through the post. Bob will send the package when the transaction is included in a block. As the transaction thus is verified, Bob believes that everything is in order. However, Alice is planning to trick Bob, and thus starts to create another block behind Bob´s back.

This block contains the same transaction; only the recipient is not Bob, but a different person. If the latter chain is longer than the former, it will replace the one where Bob is the recipient. Hence, Bob will not receive any output, as the chain with his transaction will be sent back and become one of the unverified transactions. The nodes in the network will in turn will pick up this transaction later on, only to become not valid, as the input from Alice has been referenced in another transaction. In other words, Alice has generated an alternative blockchain. This is illustrated in the figure below:



In order to accomplish this, Alice would need to create an alternative blockchain on beforehand. This would not be possible, as she needs the previous block´s reference when creating a new one. Thus, after sending the message of a transaction to Bob, time is of essence to Alice. This is because she has to surpass the rest of the network and whole of its computing power. Moreover, the transfer will have increasing security over time, so that it would be an advantage to Bob if he could wait and not post the package right away. In other words, successfully hacking the Bitcoin network is highly unlikely.

> 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).

The supply of bitcoin

As described over, it is a requisite that transactions are referenced to past transactions. When a node completes a new block, it receives an award for the job done [17]. This reward is in the form of new bitcoins. Nakamoto estimates that it is not possible to create more than 21 million bitcoins. This is because every fourth year the amount of bitcoins dealt out as rewards are halved. On the other hand, there is no lower limit to a transaction, and bitcoins are dividable down to eight decimal places[18]. However, when transferring so small amounts of bitcoins, the reward from mining might be of less value than what it costs. In this case, one might want to offer a transaction fee to the miners, since they can freely choose among transactions to put in a block. Thus including a high transaction fee will naturally impact how rapidly a transaction will be verified. Moreover, it is fair to suggest that nodes in a highly competitive market will have a low transaction fee.

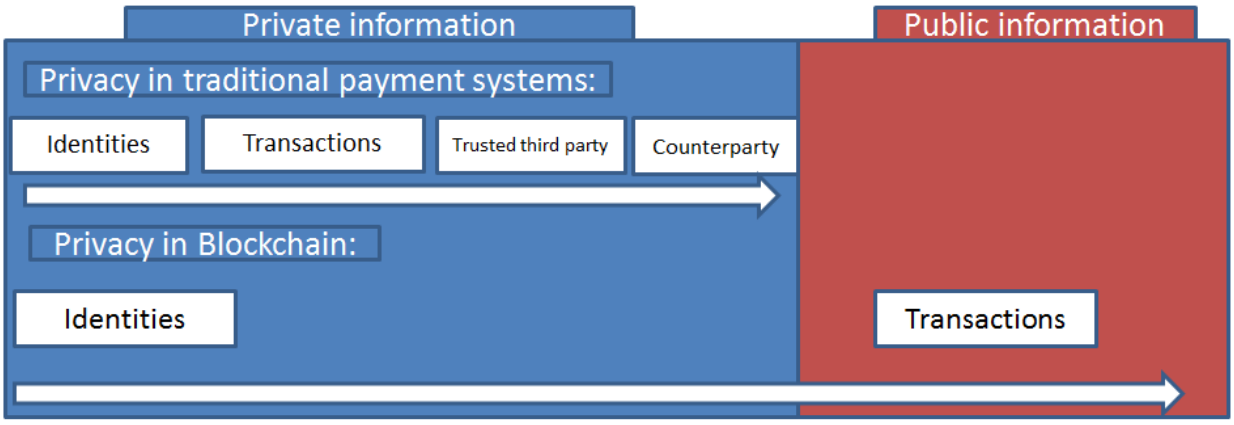
The choice of anonymity

In the Bitcoin network privacy is highly protected. This is one of the arguments frequently stated by its advocates. This is also true to some extent for other electronic payment systems like Paypal. However as in the case with Paypal, the privacy is dependent on the organization keeping it from the public as well as financial intermediaries such as banks doing the same. This results in a situation where it is very difficult to oversee bank activity. As this information is registered centrally on the banks' systems, one of the big threats to it is hacking. On the other hand, bitcoin share more similarities to cash. This is because when Alice transfers bitcoins to Bob, she can do it directly, while Bob can verify the validity of it. They do not have to know each other, and they are not dependent on a trusted third part. Moreover, everybody involved in the transactions is protected behind their pseudonyms. However, information about the transaction is open to the public. This is illustrated below:

---

[17] Since nodes use computing hardware and electricity for this, they are often referred to as miners.

[18] 10^-8 part of a bitcoin is called a satoshi.



It is voluntary to reveal personal information on the Bitcoin network, as there is no required connection between the users´ personal information and their public key. If for some reason one feel for making an extra effort to hide the person behind an account and the belonging bitcoins, this is possible through various methods [19].

More than currency

Crypto currencies like bitcoin do also have potential uses other than being money. This is due its nature as a public record. When Alice is making a transaction, she has the possibility to attach a message to it[20]. The message will also have the possibility to be verified, and also open to the public. This in turn can be applied to serve as a counteraction to fraud when exchanging legal contracts. An example for where this would be helpful is when agents use ownership certificates.

> Example: Suppose there is a car rental company. The company can release one colored coin to represent each car, and then configure the car to turn on only if it receives a message signed with the private key that currently owns the colored coin. It can then release a smartphone app that anyone can use to broadcast a message signed with his or her private key, and put up the colored coins on a trading platform. Anyone will be able to then purchase a colored coin, use the car for whatever period of time using the smartphone app as a "car key", and sell the coin again at their leisure.

[19] E.g. Hiding the IP address or the use of onetime keys for every transaction.
[20] This is called colored bitcoins.

In other words, the bitcoin will have an additional role as it represents some asset in which it has a claim. Naturally this requires that all agents involved recognize the claim attached to the bitcoin. To this end, ownership of any asset can switch hands by using the Bitcoin protocol through colored bitcoins. Another problem that is neatly solved in the Bitcoin network is the issue of ownership of intellectual property. Copyrights on songs are a good example of this. This is solved through what is called a *proof of existence*, and *hash functions*[21] are one of the main ingredients. In short words, it can be described as using a hash function in a transaction, which in turn can be a evidence of who holds the asset, and at what time.

One might say that the technical side of blockchain and crypto currencies is complex. However, the innovation is one of finesse and has many potential uses. Moreover, one of the key questions of this thesis is whether or not crypto currencies with bitcoin as a flagship are valuable as an economic principle. Moreover, while Bitcoin might be of high interest in the area of computer science, it is more unclear what impact it will have when applied as an object of economics. Hence, the next section will look closer into how bitcoin can be of economic importance.

Identifying bitcoin

With the purpose of distinguishing bitcoin as an economic concept, this section will begin with identifying concepts in which bitcoin should not be identified with. It is safe to say that bitcoins are not used in production, nor consumed by agents. Thus, one might argue that the main function of bitcoins is social. This thesis has outlined a frame work of theory in order to see whether or not bitcoins can be categorized as an economic principle. Moreover, it is fair to say that bitcoin does not fit in any of the following:

[21] A mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size.

- A perfect public record
- A form of credit
- A form of fiat money.

While the first point on the above list is true, one can argue that Bitcoin do serve as a public record when considered as a ledger. Moreover research done on this suggests that Bitcoin can be described as *imperfect memory*, which could complement other currencies that are more widely used today (Luther & Olson, Bitcoin is memory, 2015). However, while the Bitcoin network can be considered as a public record, it only works as an indirect representation of transactions. This is because the bitcoins in circulation are usually not *colored*, and thus the record will only show bitcoin balances. In addition to this, bitcoins are not anybody's liability, nor is it backed or issued by any central bank. To this end, one might argue that bitcoins can be considered as commodity money[22]. Keeping that in mind, this requires that one acknowledge bitcoins as money, or that it has the capability to become money. In order to shed light over this inquiry, it should be helpful to look closer into what characterizes commodity money, and thus comparing it to bitcoins.

Similar to one of the characteristics of commodity money, acquiring bitcoins can be done in one of the following ways:

1. Using computing capacity and electricity to *mine*.
2. Produce something else and sell the product for bitcoins/ buy bitcoins using other monies.

Furthermore, bitcoins do not have any *value in use*. It is believed that bitcoins will have value in the future; therefore the currency has obtained exchange value. On the other hand, certain types of commodity money do have value in use to begin with. Hence, users of bitcoins with expectations of the future must have followed a trigger strategy when considering bitcoins as valuable. This is in contrast to the research of Mises and

[22] Selgin describes it as a synthetic commodity money (2013).

the following regression theorem, which states that exchange value must initially have a value in use. Moreover, one cannot safely assume that all agents have a forward-looking behaviour.

It is fair to argue that the adoption of commodity money in an economy depends on its´ traits. To this end, it could be helpful to review a few of those traits that are pertinent to its aspect of a currency. Bitcoin is designed to be independent of external regulation, in addition, it is very robust in a way that outsiders cannot meddle with the system. This is due to the ledger in Bitcoin not being centralized. As a result, there is no way to change the pre-set fixed supply of bitcoins. Moreover, governments or other officials cannot seize or determine what agents can or cannot do with bitcoins.
Another neat characteristic of bitcoin is that it is easily stored. If Alice wants to store bitcoins, it only requires storing her keys. As exemplified above, these keys can be written down and kept safe, or even be memorized. Thus, there is no upper limit to quantity stored, and one does not have to worry that time might deteriorate the bitcoins.

This makes bitcoins very easy to keep safe. Furthermore, 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).

In addition to this, it is safe to say that transactions in the Bitcoin network are straightforward and rapid. Bob will know the exact amount that he receives, and there is no doubt in who owns the bitcoins due to the irreversibility of transactions. Moreover, one can divide bitcoins into any decimal point, and so the transactions can contain very small amounts. The transactions can also have a large degree of anonymity, in a way that the users behind the transactions have pseudonyms. Hence, it is possible for agents in the network to hide their identity and in spite of the possibility to track their money flow.

Liquidity

It is fair to suggest that bitcoins have a high degree of liquidity. This is because they can be continually exchanged for other currency through exchanges on the Internet. On the other hand, these exchanges are not as large and mature as the more traditional ones people are familiar with today. Moreover, there is a limit to the degree of inter exchange arbitrage trading opportunities when there is high transaction costs (Yermack, 2013). In addition, shorting of bitcoins has proven to be very difficult and there has not been much derivative contracts written over them. What is more, bitcoin swaps has now become more popular in the recent years, and the *Commodity Futures Trading Commission* the USA has granted full registration of such trading platforms (Higgins, 2016). Although derivative contracts are gaining traction, the different online exchanges have shown to have big differences in terms of the price of bitcoins. Keeping that in mind, finding a price in order to use as a reference to determine the degree of moneyness of bitcoin is not irrelevant, although for the sake of argument in this thesis it is not essential. There is an increasing acceptance of bitcoin in shops, bars and restaurants[23]. Here it is common that the prices of the goods or services are expressed in legal tender, but also in bitcoin with continuously updated prices. This is due to the volatility of bitcoin. However, when paying with bitcoin it is usually at par value, and the fee of using it is very low [24]. Hence, following this argument and stating that bitcoin is traded with a discount close to zero, it would be fair to suggest that bitcoins are money. However, this relies on merchants accepting it as payment, which currently is often not the case, and thus one can only argue that it is money for limited users. On the other hand this number is quickly increasing, but merchants or any agent would not accept bitcoins unless it has an appropriate discount rate. It is fair to suggest that with time, more serious economic agents will enter this market[25], assuming that governments do not try to stop them. When such financial actors get involved, it is fair to argue that transaction costs of trading bitcoins for other currency will be reduced. If they stay low, it is not necessary for bitcoin to develop into a unit of account to obtain moneyness over a greater extent of markets. It could rather just serve its functions as a store of value and

[23] Both directly and indirectly. There are services that help merchants with the latter. Coinbase and Bitpay are two examples.
[24] Currently around 0 to 2%.
[25] This is something that large financial actors are currently looking into.

medium of exchange. As a result, the agents that do not wish to hold bitcoin have three alternatives:

1. Liquidate their positions consecutively on exchanges.	**2. Enter offsetting financial contracts written over bitcoin.**	**3. Let third parties absorb the exchange risk.**

Case studies of commodity money

There are two characteristics of bitcoin that are interesting in terms of comparing it to commodity money. As exemplified below, it might be helpful to look at different commodity money without state backing and value of use. The intention behind this section is to give support to the claim that bitcoin can be seen as digital commodity money.

Gold

Gold has a long tradition considering it has been seen as valuable throughout history. Moreover, when looking at its price history one might argue that fluctuations of perceived value is not dependent of consumption or demand. On the contrary, Shafiee and Topal states that financial markets and the intervention of governments have been the drivers of the price of gold (2010). They argue that it is not produced to end up being consumed, but rather produced to be stored and show that one has resources. In other words, gold can be seen as a *proof of work*. Hence, this demonstrates that gold is a commodity that has exchange value without necessarily having use value. As mentioned earlier, gold has a rich history as money and this in turn shows that when obtaining moneyness, the value of use is not always relevant since commodity money can be traded above it. On the other hand, one might still say that the intrinsic value of gold is in fact very important to its exchange value when there is no government backing it. In order to argue the opposite, a few more commodity monies will be discussed.

Rai

12000 kilometres east of the Philippines is the island called Yap. Economists have found the economy on the island quite interesting due to its money. The money is called Rai, and is basically big stones shaped as wheels. The stones demonstrate wealth and are used in exchanges (Bryan, 2004).

Without any other value than the wealth they represent, they are a typical example of commodity money with value derived from its network.

What is curious in the case of the Rai is that they are made from stone that cannot be found on the island. Thus, they had to be made and transported over from other islands, something that was considered to be highly expensive. Further, this required a lot of work, and so typically a large amount of the population would help[26]. As a result, Rai achieved the ability to serve as an indirect record, indicating who where the ones to contribute to the island. In contrast to gold, Rai is not fungible, as older stones was considered more valuable than new ones. This is due to the older ones being made with shell tools and transported by canoes rather than being made with modern tools and transported by modern ships. One can say that the people of Yap acknowledged the hard work behind the stones, and thus saw this as more valuable than the stone itself. Hence, work was seen as the unit of account. That being said, one should keep in mind that prices on Yap were usually denominated in baskets of consumption goods.

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 (Jenssen, 2014).

[26] Estimates done by Bryan, states that more than 10 % of the adult male population participated.

This money was only used on the island of Yap. In the case of medium of exchange for trading outside the island, dollars and woven textiles were used. However, Rai are still used, and although it is quite seldom used, it has matured with a healthy purchasing power compared to different monies. One can argue that this is due to a network effect, as Rai has kept its value in spite of adopting dollars as a legal tender. Moreover, it is safe to suggest that Rai should continue being valuable seeing that the underlying support of social relations remains stable.

Money in Stateless Somalia

As a result of the fall of the Somalian state in 1991, the financial system and central bank fell with it. This dramatically reduced the money balances[27], and agents´ deposits were abolished. Moreover, holding monetary balances became highly demanded (Mubarak, 2002).

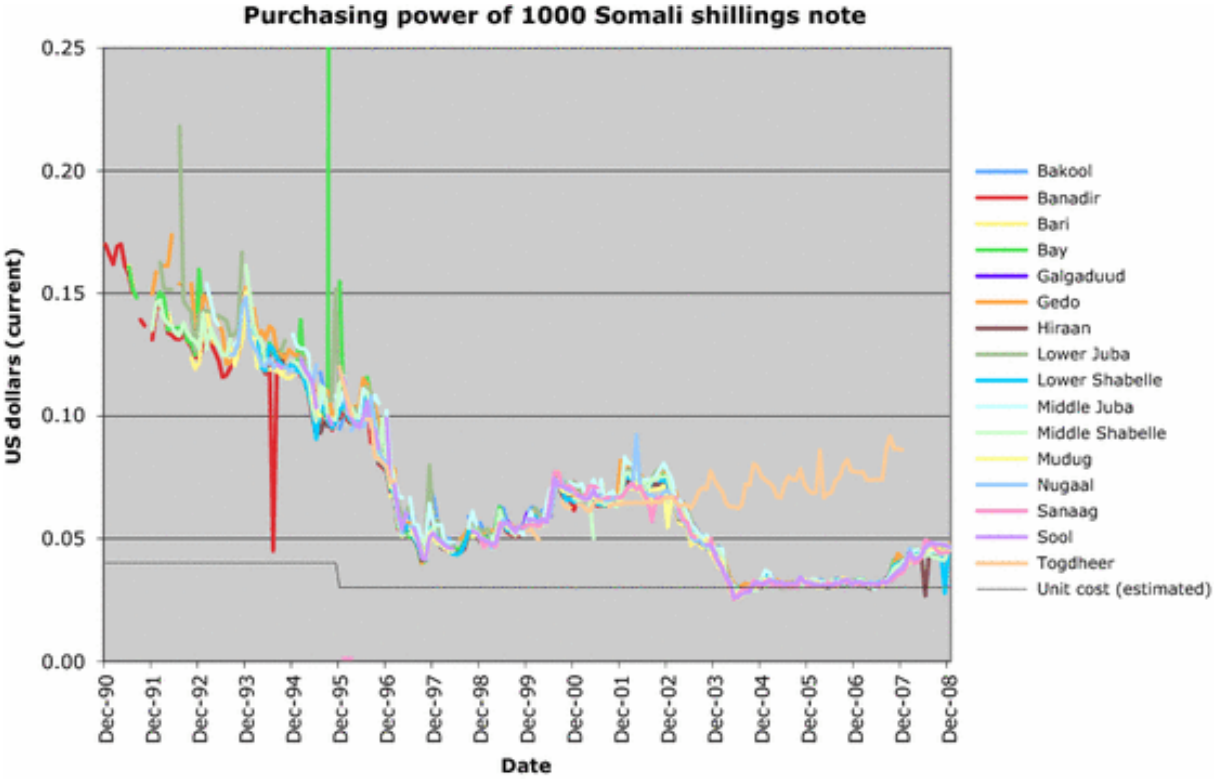
> The Somali shilling, previously backed by the state and the central bank, suddenly had no formal backing. Yet, notes issued before the state collapse continued to circulate despite the lack of use value (Luther & White, 2016).

In contrast to the Somali shilling, the stones of Yap is not fungible. This enables the people of Yap to distinguish the old stones and new stones. Had this not been the case, the people could not tell how much work was behind each and every stone, which was their way of telling how valuable they were. As a result, the marginal cost would regulate the value of the stones. In Somalia, the abolishment of the state in 1991 and the following situation with their currency is comparable to this.

As told by Luther, forgeries of the Somali shilling started appearing quite often after the fall of the state (2015). The state did not have the ability to limit the supply, and so it was a lucrative business to import fake ones. Nevertheless, the rational agents of Somalia merely accepted shilling printed by the central bank before it collapsed. As a result, the import of replicas was of the largest notes and dated before the collapse. In addition, it was possible to distinguish the fakes from the originals, and so where usually

[27] Shrunk by 54%.

discounted upon acceptance[28]. As time went on, and the notes became circulated and worn, it became impossible to distinguish the fake notes from the originals. Thus, they became equally valuable in the eyes of the market. As a result, more notes were imported because of production costs being lower than the value in which they circulated. 17 years after the collapse of the state, the value of the currency had decreased ten times its value, when measured against the US dollar[29] (Luther, 2015). From there on, the price of Somali shilling got less volatile, in addition to an increasingly real money balance. This is illustrated below, where the names on the right side are different markets in Somalia (ibid):



What is noteworthy with the Somali shilling is that it went from a fiat money to commodity money. There was no government supporting the currency, and despite this it continued to be in use for over two decades. It had a value at the marginal cost of production. In addition, the agents in the Somali markets would only accept notes made to be a replica of the notes from the pre collapse era.

[28] Normally at 5% (Muburak, 2002).
[29] From 0.30 USD in 1991 to 0.03 USD in 2008.

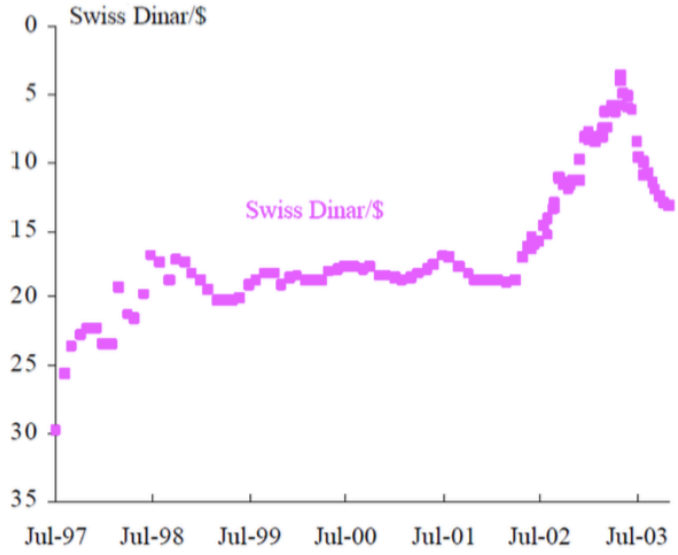
With a fixed marginal cost of production, the value of the Somali shilling became regulated by the printing and transport costs, as more zeroes could not be added to the notes.

Kurdish isolation in Iraq

As a result of the sanctions against Iraq, the state could not import currency printed abroad any longer. This happened in 1990, and USA was behind the embargo[30]. Three years later, the president at the time[31], declared that the Swiss dinar was to be taken out of circulation. His plan was to produce a new currency called Saddam dinar and thus replace the old currency (King, 2004). Moreover, due to the circumstances at the time, the new currency was not adopted in the northern part of Iraq. This Kurdish part in the northern region of the country was isolated from the rest, and so the citizens there did not get the opportunity to swap their old notes with new ones. As a consequence, Swiss dinar was the only currency accepted in the Kurdish part regardless of the new decree.

In contrast to the Somali shilling and the Rai, the Swiss dinar had a very inelastic supply. The two former had an elastic supply, and value was determined by the cost of producing them. As the latter was perfectly inelastic, this illustrates that money with no vale of use can remain in circulation in spite of no government backing it. Furthermore, it is fair to say that money supply in the Kurdish part of Iraq became fixed [32]. Quite contrary, notes will be worn over time, resulting in a declining nominal money stock (ibid). Moreover, compared to the US dollar the Swiss dinar increased in value, and its' purchasing power remained stable. This is illustrated below:

[30] The original stated purposes of the sanctions were to compel Iraq to withdraw from Kuwait and to disclose and eliminate any weapons of mass destruction.
[31] Saddam Hussein.
[32] The Swiss dinar was not printed after 1989 (King, 2004).



In contrast, the new Saddam dinar did the opposite, due to unnecessary high amounts of printing. In addition, the depreciation was in some extent due to the low quality of the notes, leading to forgeries. On the other hand, in the northern Kurdish part the local leaders was worried about having a currency that was not backed by the state, in addition to being appreciating. However, the value of the money remained high. One thing that is important to underline here, is the social relations and thus the network behind the Swiss dinar. Instead of being backed by some government, the Swiss dinar was backed by social economic relations. When a network can endure such a transformation, it shows how a piece of paper may still serve as a valuable object without backing from the state. Because of the circumstances at the time, the northern Kurdish part of Iraq acted in many cases independently of the rest of the country. Thus the Kurds did not have to take into account that their currency was not accepted outside their region.

> What gave the Swiss dinar its value was not the promise of the official Iraqi government, or indeed any other government.

The purpose behind outlining these commodity monies is to illustrate that it is not always necessary to have a government backing, nor a value of use for it to be fully functional. However, what might be of higher importance is the degree of which agents in an economy trust the currency. In other words, the money must serve a trustworthy indirect record, something that the examples above demonstrate. This in turn is

comparable to the nature of crypto currency, and function as an argument for them being valuable. It also serves as an argument against critics stating that crypto currencies are bubbles doomed to fail, or for example that crypto currencies as the bitcoin will fall to zero. While monies in the past have circulated without state backing and value of use, it is not enough to conclude that this makes crypto currencies money. Thus, the next step would be to look closer into what makes private agents adopt money. It is fair to suggest that that this happens if it is less costly for agents to adopt a new currency, compared to the initial one. To this end, it could be helpful to investigate transaction costs that may be removed or decreased by crypto currency, which in turn will answer whether or not they can be seen as valuable.

Application to the real world

The agenda motivating Nakamoto when creating Bitcoin might consist of several aspects. However, one of the main intentions behind the technology was to create a platform for digital cash. The digital cash was designed to be disruptive by nature, and have the ability to resist intervention from any leading power. Keeping in mind the examples mentioned earlier, it is fair to argue that the Bitcoin protocol has capacities that make this plausible. The Bitcoin protocol needs to cause several things to happen in order to fully reach its potential as an economic concept. For Bitcoin to affect the economics of how agents do exchanges, it must be disruptive in regards to transaction costs. This in turn will lead to high demand of bitcoins and thus have a proper impact on the economy. To this end, a selection of different transaction costs in which Bitcoin might disrupt is introduced.

International transfers

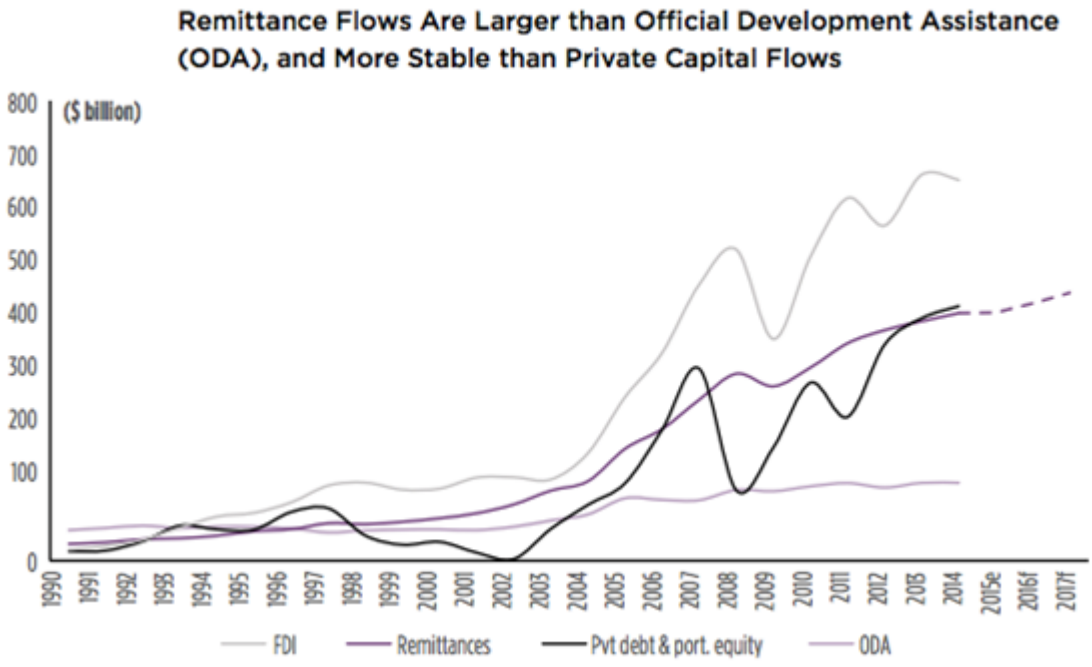
It is evident that the technology of the Internet has created huge opportunities in terms of digital services. A lot of work behind this kind of electronic services is things that do not depend on where the worker is located[33]. Moreover, if a firm in Denmark outsources such work to India, there must be a way for the firm to give salary to its employee. This requires a medium that can assist that progress. In other words, what the firm has to do is to transfer currency internationally. The traditional way of doing this is through banks, however, this requires that both the firm and the employee have bank accounts. Usually, countries regulate these flows of capital. Alternatively, they could use wire transfers through a cash office, although this is often seen as costly and time consuming. Moreover, it is fair to say that the Internet gets more widely spread and more accessible as the world gets more developed. As a result of this, there is an expansion of the *production-possibility frontier* in regards to trade. On might say that it is difficult to comprehend the full potential that trade has. Yet, in order to exploit that full potential, one might argue that transferring money must evolve into an effortless procedure.

[33] Programming for instance.

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.

Remittance transfers

The World Bank has estimated that by the end of 2016, official records of international remittance flow will be approximately 550 billion dollars. This is estimated to grow annually at 4% until it reaches 650 billion dollars in 2018 (Ratha, et al., 2016). 500 billion dollars of these remittances are expected to go to developing countries. What is noteworthy is that this is figure for developing countries is much higher than ODA [34]. In addition, this also applies for private debt and portfolio equity flows. This is illustrated in the following graph (ibid.):



This is relevant because it significantly affects the whole economy in certain countries that receive such flows. In addition, as a result this can make changes for the better in terms of welfare for the population of these countries. In many cases the remittance

[34] Official Development Assistance.

received by certain countries exceeds their total stock of foreign-exchange reserves on an annual basis. This is shown in the histogram below:

The country with the highest relative inflow of remittances is Tajikistan, which received 48% of GDP in remittances in 2012 (Ratha, Eigen-Zucchi, Plaza, Wyss, & Yi, 2013). This indicates the relative importance of these flows for foreign exchange earnings.

Looking at the figure above, it is apparent that this is a high amount of flows. Moreover, the report from the World Bank states that the cost of sending 200 dollars has an average of 7.4%. The region that is most costly to send remittances to is Sub-Saharan Africa, with an average cost of 9.5% (Ratha, et al., 2016). Hence, it is fair to suggest that money transfer services[35] could meet high competition from Bitcoin. One might think that a developing technology has opened for decreased costs regarding money transfers. However, as a result of financing of terrorism and money laundering, these institutions face high costs in terms of laws and regulation. As a consequence, international banking institutions are withdrawing their business from developing countries and thus the consumers in these countries stands without bank accounts. This has a negative impact on many countries, for instance like those in Sub-Saharan Africa, because with no

[35] Such as CurrencyFair, TransferWise or Western Union.

international banks there is no way to send money there with use of a formal channel. On the other hand, laws and regulations do not affect Bitcoin, as it is not a centralised network. However, all agents who are using bitcoin stand freely to do so. As mentioned earlier, sending bitcoins is very cheap and has a low fee, which is actually voluntarily to include. This makes the Bitcoin protocol ideal for sending remittances, and the people using it as a platform for this purpose would clearly benefit. Another platform that has become widely used in developing countries is something called M-Pesa. M-Pesa is a branchless bank service using mobile phones to transfer money. Behind the service is the largest mobile-phone company in Kenya and Tanzania. Out of this platform, a group of smaller companies developed the service further, making a bridge between bitcoins and mobile phone money. With a bitcoin wallet on their phones, the agents using this service can do international transfer at a low fee. Since both Tanzania and Kenya normally receives high amounts of remittances, this bridge between M-Pesa and the Bitcoin network opened a gate to millions of people. In addition to being an inexpensive international money transfer this technology is one that makes remittance very fast (Jack & Suri, 2011).

Exclusion of agents

It is fair to say that it exists high entry costs in addition high transaction costs in developing countries. However, this might also be true for developed countries. This in turn can be one of the factors leading to agents being financially excluded.

In the US nearly 70 million Americans are cut off from the mainstream financial system in some way, and 8% are unbanked (USPS, OIG, 2014).

When an agent is excluded from the financial system, the alternative is to operate with cash. In addition, these agents cannot purchase or sell goods or services on the Internet, as this requires a bank account. This also applies for businesses in America that sell things that are legal in one state, but not in another. One such example is Cannabis. However, since it is illegal in some states, these businesses do not have the option to open a bank account. This is because the banks are regulated by federal law. Since the

alternative is to operate with cash, this brings an aspect of inconvenience to the businesses. In addition, it may increase the risk for robberies. This is costs that can be reduced if adoption of Bitcoin happens.

Politically imposed cost

Another transaction cost that face both developed and undeveloped countries are one imposed by policy. Politics in different economies may interfere money transfers even when the agents are law abiding. This is not limited to poor countries or countries with dictatorships, but also western countries. Governments can issue financial blockades, freezing people or firms' funds. They can stop donations to organisations through hindering use of payment providers. Centralised payment systems like MasterCard or Visa may easily be controlled through imposing transaction costs politically. Moreover, if one wants to open an account it is required to give up personal information for identification. Hence, this opens a possibility for the government to start surveillance of their citizens. In addition, the risk of identity theft will be present when giving up such information.

> As an example, Barclays had to start an investigation January 2014 after consumer data on 27,000 customers was stolen and sold (Young, 2014).

As a result of this, one can say that there is demand for a decentralized payment system. This is due to some agents wanting to operate outside the government´s control and regulation. Others just want to stay anonymous in order to protect themselves. Due to its functionality, one solution to this problem is the Bitcoin network. Bitcoin decreases the transaction cost for different types of transactions prone to regulation.

What is crypto currency worth?

Drawing on the arguments in the above analysis, it is fair to say that crypto currencies have a function as a medium of exchange. According to Ostroy and Starr, for something to be called a medium of exchange, it must also be a store of value (1990). Moreover, because transaction costs is to a large extent overcome by using for instance bitcoins, it can be called a medium of exchange. Since this is beneficiary to agents, it can therefore be seen as valuable. In emergence of this concluding argument of why crypto currencies are valuable, another inquiry that naturally follows is how this value is decided. The Bitcoin protocol was designed in such a way that it controls the supply of bitcoins. As a result, this quantity will not be affected by other factors in the economy. However, it is fair to say that the bitcoin supply is fixed in the long run. While mining of bitcoins continues to increase the amount of bitcoins, this is not something that changes the basis of following analysis.

In order to analyse bitcoins in terms of economic demand, two methods will be applied. Firstly, it could be helpful to analyse bitcoins as a stock. This is done through looking closer into economic agents and their willingness to hold bitcoin in their portfolio. Secondly, the famous *equation of exchange* can be applied to examine how bitcoin function as a flow, where transactions influence demand.

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.

Crypto currency as a flow

The equation of exchange shows supply and demand of money as a flow over time:

$$M_t V_t = \sum_i p_i q_i = P_t Q_t$$

Where:

M is quantity of money.

V is the velocity of money.

P is aggregate price.

Q is an index quantity.

P*Q is nominal GDP.

In economic theory based on monetarism, nominal GDP is the driver of money demand in the sense of nominal value of goods purchased. This is denoted on the right hand side of the above identity. This can also be seen as the nominal value of goods purchased with money[36]. Moreover, shifts in quantity of money is what changes aggregate price[37]. This is why monetarist economists argue that inflation is a result of monetary involvement. Moreover, monetary policy impact money supply in an economy, and thus inflation. Over time, in theory, marginal rate of return to investment is the same for all industries[38], and his also includes production of money:

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

Where:

MC_M is marginal cost of money production

MC_i is marginal cost of producing good i

p_i is price of good i

Thus, one can express a ratio that yields a long-term relationship of p_i:

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

[36] With bitcoins in this context.

[37] In monetarist theory, quantity and velocity of money are assumed to be fixed over time.

[38] Assuming capitalist production and commodity money.

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

In a previous section, the example of the Somali shilling was used. Producing this currency was at a fixed marginal cost with endogenous money supply. The return to production of goods would be become less than the return to production of money if prices were to go below the equilibrium level. As a result, money supply would increase, since investments in producing money would increase. If marginal cost of money production is constant, only shocks of productivity in producing goods will change the price level. If marginal cost of producing continues to be fixed, prices in the long run will not be affected by shocks to quantity or velocity. As mentioned earlier, in the case of bitcoins, quantity of money is not affected by such changes. Thus, if there is a shock to quantity of money, it must change aggregate price or velocity (or both) in response.

Determination of the value of bitcoins ($Pt-1$), and thereby prices(Pt) will therefore hinge on assumptions about the exogeneity of Vt and Qt relative to the equation of exchange (Jenssen, 2014).

According to Wang, there are only two ways to reduce velocity in the Bitcoin network, and thus changing the price level. One thing that can happen is that agents save bitcoins, the other is taking bitcoins out of circulation[39] (2014). If however, for some reason the quantity of money should increase, this would not have any impact on the price level. This is due to the offsetting change in velocity. Keeping this in mind, it is fair to say that it is possible to see this from a more monetarist perspective. This would then mean that velocity was determined exogenously. Hence an increase in quantity of money would lead to a decreased price level and infer deflation. One might say that how one employ these assumptions when applying the equation of exchange in a large extent will impact what outcome it yields.

[39] This however requires the assumption that velocity is endogenous, but also a linear function of the quantity of money.

As mentioned earlier, monetary supply shocks does not exist in the Bitcoin network. Hence, this cannot change prices in terms of bitcoins. At the same time, this means that changes in velocity or quantity (the demand side), will have an efficient impact. One might say that there is a controlled and stable supply whereas demand cannot be controlled. Velocity is a result of agents saving while the quantity of money is impacted for purposes regarding transactions. Keeping everything else constant, these kinds of shifts in demand will thus have one to one relationship with price. In order to get a clearer view of what makes bitcoins valuable, it could be wise to look closer into what decides the demand for them.

Crypto currency as a stock

When evaluating crypto currency as money, it might be helpful to assess it from the perspective as a *stock*. Changes in utility are due to increase or decrease in money as a *flow*. However, money is often described as a stock when *held* by economic agents. This is also true in the case of bitcoins, however, the reasons why economic agents choose to hold them might vary. If one looks at agents holding bitcoins, one can say that the currency is a part of their portfolio of real wealth. Furthermore, bitcoins would appreciate if the demand for holding them as real balances where to increase. This is the only reaction of bitcoins if the demand for them would increase over the economy as a whole. As a result, this increased real value of bitcoins would thus increase its´ share of value compared to the other assets in economic agents´ portfolio. On the other hand, if the opposite where to happen, the holders of bitcoin would try to sell. In other words, because of bitcoins being held as a stock, demand for bitcoins would decrease. Hence, the market supply would increase, and this is where it is important to underline a key distinction. Since there can only be maximum of 21 million bitcoins in circulation, this means that supply of bitcoins is fixed as a stock in the economy. Quite contrary, this is not true for the market of bitcoins, where exchanges take place among agents.

In order to analyse what affects the demand for bitcoin as a stock, modern portfolio theory might be helpful. As mentioned earlier, different economic agents put together a portfolio consisting of various assets. In this process, the agents assess the expected

return of each asset (Markowitz, 1952). Moreover, due to its relatively short lifespan, it is fair to argue that it is hard to estimate what value bitcoins will have in the future. One might say that there is an expectation of a shared view that bitcoin will continue to have value in the future. This is what determines its present value, and might start to look like a *Keynesian beauty contest*[40]. In other words, there little knowledge about past value and agents have little experience with the asset, thus believes will not be shaped by this. Hence, if agents expect that bitcoin will appreciate, it will increase demand, which in turn will realise the expected increase in value. Moreover, one might argue that this is a characteristic that shares similarities with a Ponzi scheme. Furthermore, it has also proven to be hard to short bitcoins. As argued by Yermack, this can contribute to prices being higher for longer periods of time than they would be with this possibility (Yermack, 2013). It is fair to suggest that this was the force at work resulting in the price plummet of bitcoins in 2013.

One key takeaway from the above section is that expected return on an asset might be very significant to how economic agents construct their portfolio of wealth. Another aspect that might be of high importance is diversification. Since different agents have different degrees of risk aversion, some might choose to sacrifice more expected return in favour of lower risk than others. However, research done in regards to this issue concludes that bitcoins are useless as a tool for risk management (ibid.). This is due to value of bitcoins having no significant relationships to other currencies. As a result, it is hard to hedge bitcoin´s risk.

On the other hand, whether or not an asset can be hedged is not a final determination of how useful it is when it comes to risk management in a portfolio. If one assumes that unsystematic risk can be overcome by diversification, the CAPM[41] model yields a better measure for risk in an asset. Since bitcoins can be seen as a very independent asset, they could be beneficial to hold in terms of variance. Keeping that in mind, bitcoins might increase its correlation with different assets as it matures. Similarly, gold has served as a hedge against fluctuations in the foreign exchange value of the dollar, and this

[40] Investing that suggests that investors may guess what other investors are going to think as opposed to what they think themselves.
[41] Taking the covariance of the market portfolio relative to the market variance.

relationship has changed over time (Capie, Mills, & Wood, 2005). Furthermore, the technical characteristics of bitcoin are what can turn it into a useful dollar hedge. In a situation where the popularity of bitcoins should increase at a high degree, it could grow into becoming a *hard currency* since it easily can be traded across countries. As a result, it could function as a hedge on the macroeconomic level as a substitute for the dollar.

What we can take from the modern portfolio model in the paragraph over is that there are mainly two reasons motivating holders of diversified portfolios to include bitcoins in their portfolio. Firstly, economic agents want to manage the riskiness of their portfolio. Second, they want bitcoins to increase in value and thus increasing the value of their portfolio. That being said, economic agents have different preferences of liquidity, and one should also take this into consideration when discussing the demand for bitcoins. As mentioned above, agents may want to hold bitcoins because they expect it to appreciate. In addition to speculation, other agents may hold them because of its traits for transactions. The degree to which money or assets are liquid varies among them. Hence assets that are more liquid will be chosen of agents to be used in transactions. In other words, if bitcoins are effortless to use, they will be chosen more often than other assets for transactions and thus the demand for them will increase. On the one hand, agents holding bitcoin for speculation would increase its demand, and making bitcoins a unit of account might make it more liquid. However, because of its liquidity, bitcoins may not need this driver for demand, as its liquidity alone would make it highly demanded for transactions. Moreover, one might argue that this is what makes bitcoins an exceptional medium of exchange, something that advocates of crypto currency has underlined. On the other hand, sceptics has emphasized that the fixed supply of bitcoins is its greatest weakness, and as a result hinders it from developing into a prosperous medium of exchange. They argue that whatever drives up the demand for bitcoins, the result will be a liquidity crunch. This is due to the fixed quantity of bitcoins and that the increased demand might thus drive deflation. This will cripple bitcoins as a medium of exchange because agents will start hoarding the currency and so the velocity will decrease. Keeping this in mind, I would argue that this evaluation is weak. This is due to their argument being based on mistaking motivations for saving,

This is based on Krugman's popularisation of "Monetary Theory and the Great Capitol Hill Baby Sitting Co-op Crises" (Sweeney & Sweeney, 1977).

with agents´ preferences when it comes to how they decide to composite their portfolio. When economic agents decides to save, their decision is not formed by the return on just one asset in isolation, but on the return of the whole portfolio. As a result, if bitcoins increase in value, there is only one possible way to reduce the velocity. It has to come from a raise in general return to saving[42]. Thus, when holding bitcoins and making the decision to spend them, economic agents will counterbalance their portfolio so that they hold their preferred real balance of bitcoins. Put in a simpler way, as long as agents want to spend, they choose bitcoins as a medium of exchange not because they expect it to increase in value, but because of its liquidity. In addition, if bitcoins increase in value, it will also increase agents´ real bitcoin balance. Since agents have different preferences when it comes to their portfolio, some of them will feel that they are too heavily invested in bitcoin. As a result, they will raise the market supply when they decrease the balance of bitcoin in their portfolio.

As discussed above, there should not be any issues with bitcoins increasing in value provided that it does not develop into a unit of account. However, a far more complex situation would occur when considering that one can colour bitcoins with debt contracts. According to Kiyotaki and More, credit leads to increased velocity of the asset (2000). They go on to explain that this happens when *inside money* is issued, money issued by private intermediaries in the form of debt. When loans are issued, the issuer gets repaid the full loan plus some additional nominal claim as a result of the interest rate. As a result, if bitcoin would become more widespread than it is today, the fixed supply of quantity thus might become an obstacle. When an economy faces an expansion, the elasticity of credit supply rises, which in turn creates a financial accelerator. Moreover, over time economic agents might have so much net claim on bitcoin that it surpasses the fixed supply. The expansion may continue to go on if the supply of credit also continues, backing up the demand and repaying past debt. Nevertheless, a *Minsky moment* will arise. This is when it is excess aggregate supply, and result in economic agents having problems with monetizing investments (Minsky, 1982). In order to circumvent a recession from *debt deflation*, one of the solutions could be to stimulate the economy by introducing monetary policy. Hence, considering that

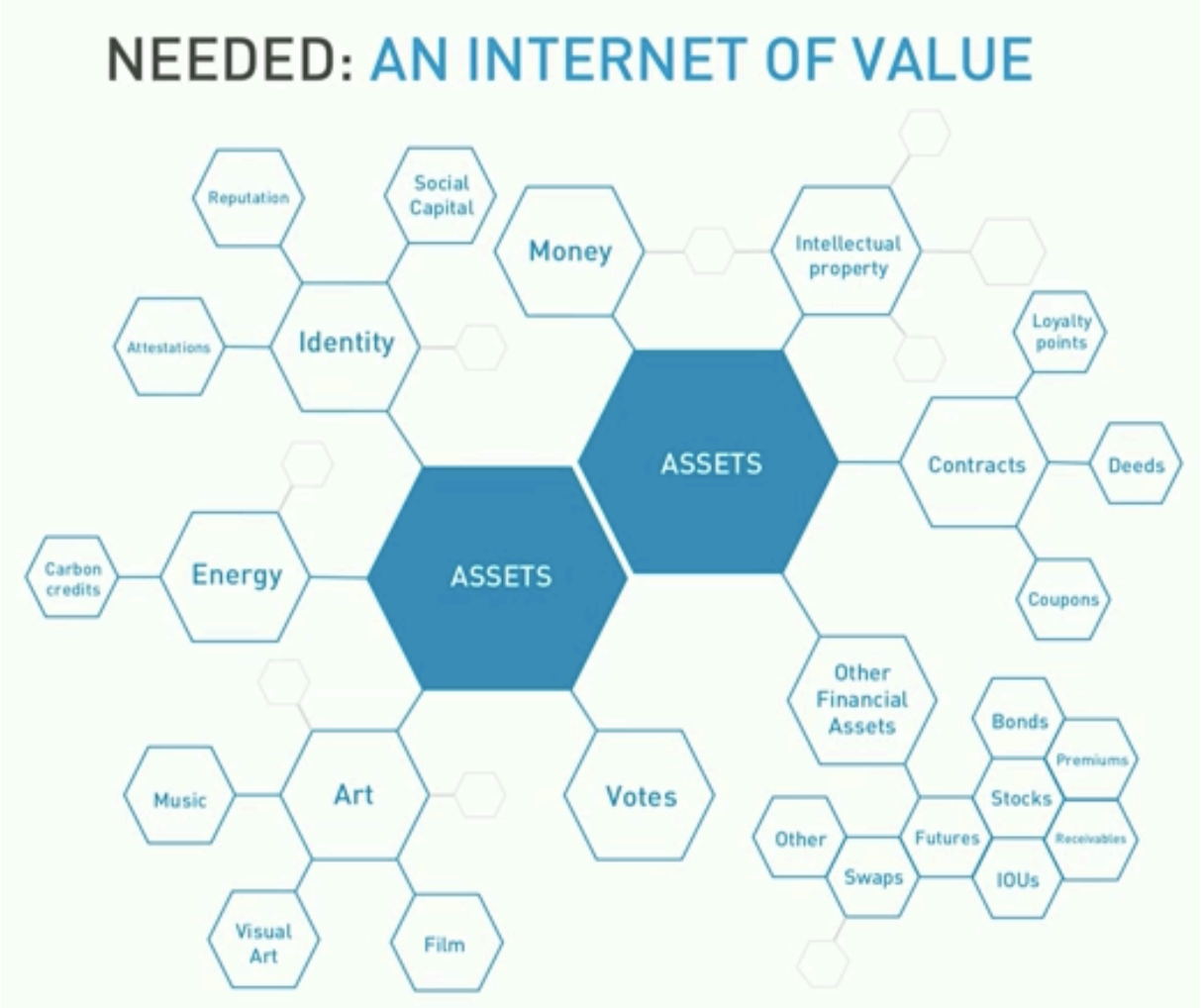
[42] This requires the assumption that the income effect is dominated by the substitution effect.

the supply of bitcoin is fixed, it is hard to imagine that there will be no downturn. However, if some central power intervenes and take extreme measures this might help avoiding such a downturn[43]. Conclusively, this is why governments may want to control crypto currency, and also why different countries have shown opposing views when it comes to how they handle these currencies. Moreover, if crypto currencies such as bitcoin were to take off, it would weaken monetary policy and governments´ regulations. As a result, it would become harder for governments to control economic activity. In this sense, crypto currencies might disrupt the function of central banks. Keeping this in mind, the use area of blockchains such as the Bitcoin protocol might be many, something that is explored in the next section.

[43] E.g. ruling bitcoin contracts invalid.

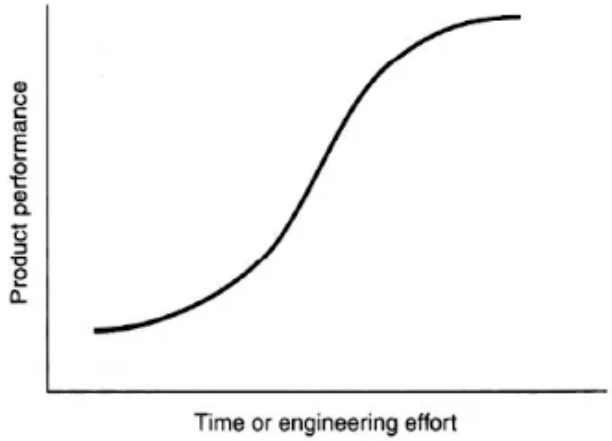
The disruptive power of blockchains

It is fair to suggest that blockchains have a tremendous potential, and is a technology that has the ability to become a disruption for several financial functions in the economy. Moreover, one might argue that to what degree it will be disruptive hinges on whether or not crypto currency emerging from this innovation can be regarded as money. Clayton Christensen's "The Innovator´s Dilemma" largely influences the theory of disruptive innovation, and describes that an innovation should create a new market and value network in order to be called disruptive (2013). Moreover, he suggests that the innovation should have a significant societal impact. This is something that applies for the Bitcoin protocol. Some of the disruptive potential that lies within Bitcoin might build on functions that are dependent on avoiding double spending. Don Tapscott identifies some of that uses in the figure below (2016):

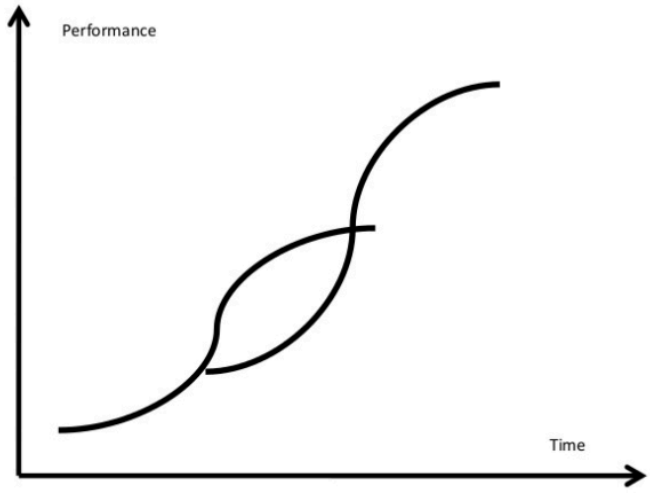


One of the qualities with Bitcoin is that it enable economic agents one-use spending, something that might be critical for the transactions and the exchange of the above assets.

Establishing that Bitcoins has a potential for being a high-impact disruptor, it is fair to say that this potential has not yet been fulfilled. One can argue that Bitcoin are in an early stage of its lifecycle. Moreover, placing the technology correctly in its life cycle may help to enlighten whether start-ups and businesses should go into this particular innovation. This in turn might facilitate spreading of the technology to the individual agents and thus reaching the full potential of the technology. Central in the theory of innovation is the technology S-curve as discussed by Christensen (1992). Prescribing developments of new technology may be of vital importance, and Christensen uses it to determine the maturity of the technology (ibid.):

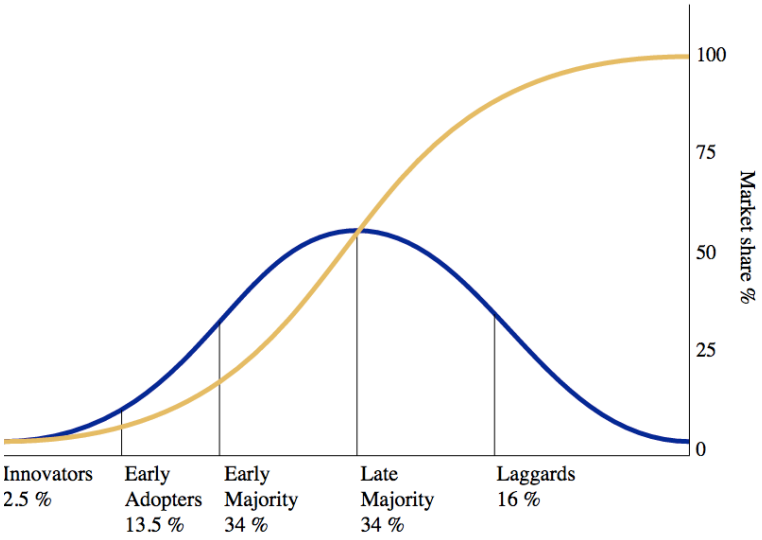


As depicted in the above figure, a technology´s performance evolves slowly in the beginning. At some point, a breakthrough happens and the technology now improves rapidly. At the maturity stage, the technology has reached the limits of what is scientifically possible, this is where performance does not improve much anymore and has reached its potential. Moreover, as a technology reaches its mature stage, it becomes increasingly vulnerable to substitute technologies. At this stage the s-curve may be subject to a shift, as depicted below (ibid.):



The initially lower performance makes it seemingly irrational for firms dominating the previous technology to invest at an early point. As performance then improves rapidly there is a risk that these firms are left behind. Due to these factors, it is very important for actors in the financial markets to seriously consider the potential benefits of the Bitcoin protocol. A too narrow focus on current performance measures of their companies could lead to falling into the innovators dilemma, where short-term profitability clouds future judgements.

If one follows that the Bitcoin technology is in its early phase of the life cycle, one can expect that the technology will be adopted in a much higher degree than it is today, and that this may happen very rapidly. This is something that Rogers has looked closer into in his research, and presents the theory diffusion of innovations (2010). Rogers' theory tries to explain why and how, and at what rate new ideas and technology is spread. The below graph show that adopters of a new technology can be categorized into smaller groups of agents, showing a timeframe of when these different groups adopt the technology. The yellow line represents market share (ibid.):



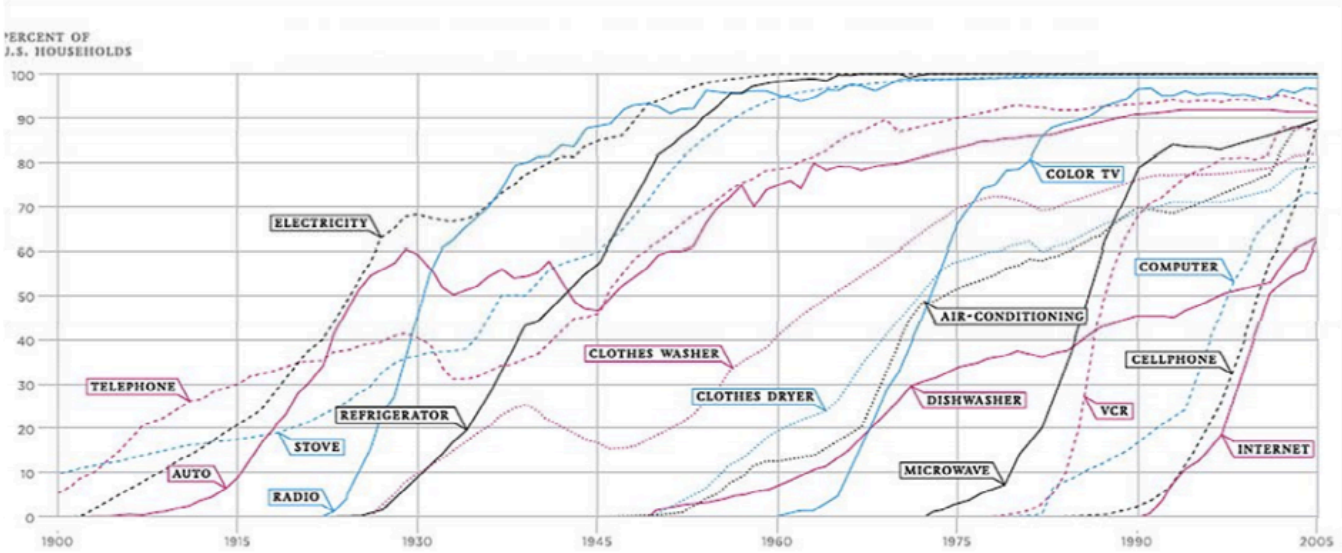
According to Rogers, there are several attributes an innovation must have in order to be adopted by agents. He goes on to say that potential adopters evaluate the innovation on factors such as:

-Relative advantage to current tools or procedures.
- Compatibility with pre-existing systems.
- Difficulty or easiness to learn.
- Testability.
- Potential for reinvention.
- Observed effects.

Moreover, these qualities interact and are judged as a whole. It is fair to argue that the Bitcoin protocol opens for opportunities that score high on all of these qualities. However, like in the case of bitcoins, factors such as perceived riskiness or instability will have the opposite effect. Keeping that in mind, what is unique with the Bitcoin technology is that it has a potential that touches many different fields in the economy. Smartcard payments, supply chains, tracking taxpayer money, online voting, recording stock exchange trades, land registries, smart contracts, cloud storage, music payment and licensing are some of the use areas to name a few[44].

[44] See the appendix for a more comprehensive list.

According to Jack & Suri, technology adoption is getting faster (2011). This illustrated below (ibid.):



The data they collected is from The World Bank and is based on numbers from the U.S. Nevertheless, they argue that this is a trend that is uniform for all countries, both developed and undeveloped[45]. When applying the theory of Rogers to real data, one can se from the graphs that this is in alignment with the theory. One should also note that technological innovations from more recent years have steeper curves. Hence, if the blockchain should reach its fully potential, firms that are hit by this disruption might have limited time if they want to stay competitive. In other words, considering a shift in the s-curve as presented by Christensen might have an immense disruptive effect on existing firms that faces disruption in their field of business. Hence, in order to stay competitive when disruption happens, existing firms should take action, and so a few examples of this are now presented.

Trade finance is no exception when it comes to the disruptive power of the blockchain. When importing goods, the importer has the opportunity to prove solvency by making a "time limited deposit". This deposit will be held in escrow until the importer receives the goods, and only the exporter can release this funds upon acknowledging receipt of the

[45] Solow's famous (1956) model of the theory on economic growth, and following later the augmented versions of e.g. (Romer, 1986) and (Lucas, 1988) have shown that higher rates of adoption of modern technologies may accelerate the development process.

goods (Ngo, 2014). This was first tried out by The Commonwealth Bank of Australia and Wells Fargo in October 2016. The trade was international, and successfully shipped $35,000 in cotton from Texas to China (Sohn, 2016). One of the biggest "headaches" associated with global trade is the movement of the paper documents that track and authenticate the transactions. As experienced when Barclays used a blockchain platform to transfer trade documentation from an agriculture co-operative to a food product distributor, this was no longer an issue (Rizzo, 2016). Mearsk and IBM recently started collaboration in order to ease this process, and also reduce cost and waste (Groenfeldt, 2017). Ports will also benefit because they receive information of when ships arrives and what they contain so that they can plan ahead how to handle the containers, and in turn increasing efficiency. Sea cargo transportation is bureaucratic and complex, and in some cases, transportation documents are used to commit commercial fraud. Using applications on the global supply chain might minimize the time products spend in the transit and shipping process, improve inventory management and thus save both time and money.

Recently, two of the largest agents within digital and blockchain payments (respectively) in Europe, Nets and Coinify, entered into a partnership where Coinify will develop integrated blockchain solutions for Nets. They have created a 'Blockchain Development Lab' to expose business opportunities within Blockchain technology. The partnership also includes cooperation with internationally recognized technology experts, and it will lead to the development of a number of so-called proof of concepts that will form the basis for the development of specific products and services (Nets, 2016). There are many similar examples of tech companies and big financial institutions. Moreover, central banks has also opened their eyes and started investigating the opportunities that lies within the technology.

As previously stated, some governments have been positive to Bitcoin, while others have expressed the opposite. Moreover, several governments and their central banks have looked into how they can capitalise on this technology, and have considered making their own currency. This has been on of the more recent trends regarding crypto currencies, and the Norwegian central bank recently stated that they will investigate the potential of a centralised digital money (Mikalsen, 2017). On the other hand, the

Swedish central bank has been doing this for some time, and what seems to be the consensus among central banks that have been looking into this for a while is that it is rather unclear whether or not a new digital currency will circulate in addition to the fiat money already issued. Moreover, if this change was to happen, it is also difficult to forecast when it will be introduced, and what impact it will have in the short run compared to the long run. Moreover, the major gain of a national digital currency is that one will separate payment systems, from being a provider of loans. Banks are both "too big" and "too important" to fail, so it is desirable to achieve an effective separation. At the same time, the central banks must be able to ensure that they are in control in case of an emergency situation (Visjø, 2016).

It is hard to predict how this technology will disrupt different markets, especially over the longer term. However, what is more certain is that the blockchain technology has a big potential when it comes to disruption. Moreover, if this innovation is at the start of its life cycle, there will be branches of different uses stemming from augmented versions of the blockchain. At the same time, economic behaviour is at constant change, and trust in financial institutions might be at an all-time low. This is something economic agents should consider when trying to stay competitive, and entrants take advantage of when trying to enter a new market.

Conclusion

This thesis has applied the characteristics of money to crypto currency in order to decide whether or not it could serve as functional money. Moreover, the thesis goes beyond that, in the sense that crypto currency gets defined as digital commodity money. To arrive at this conclusion, the thesis systematically classifies different forms of money, in order to compare how much trust is needed for efficient money to circulate.

Economic agents are connected via transactions. Money is what makes this possible and serves as indirect record. When money function as a proof of work, it is a credible record of exchange. If money can rest on its underlying work necessary to acquire it, it is a representation of its value. This should not be confused with the associated cost of producing the money. More importantly, this is also true for crypto currency. One should also keep in mind that money is a social construct, and that the responsible establishment behind the money might impact the social aspect of it. To this end, money can be seen as very complicated economic concept.

The quantity of crypto currencies is fixed. As a result, demand will be the dependent variable for value. Moreover, crypto currencies have no value of use. Hence, there are two basic determinants of demand. These are expected future demand and outperforming other money when it comes to transaction costs. One of the findings in this paper confirms that crypto currencies do have lower transaction costs than other money. The transaction costs from crypto currency are lower both directly and also in terms of costs that are imposed by politics. Hence, crypto currency ought to have a price that is positive. Moreover, since there is no central power that can affect crypto currencies in terms of transaction costs or in other ways, one can say that such central powers lack the capability to control economic activity via monetary policy. Governments have yet to issue their own crypto currency, but have started to investigate the matter. Hence, one might suggest that since they cannot control crypto currency at a high degree, they might want to issue competing digital money in order to have a satisfactory level of control.

If we look at the underlying technology of bitcoins, there is no doubt that there is a huge potential for disruption facing the economy. While crypto currency alone might be very disruptive as money, there are many use areas of blockchains. Moreover, this innovation is at the start of its lifecycle, and the technology and idea is getting more widespread. Early adopters might still be the main group of economic agents that use crypto currencies and blockchains, however the innovations are getting traction from both academia and businesses. Moreover, individual agents from countries with a lack of trust in their financial institutions or government have used crypto currency in a high degree. Similar to other innovations, it will take time before the technology reaches its full potential. It will also take time before the people in the economy understands this potential. This is similar to what happened to the Internet. This technology has the ability to solve real problems for millions of people, problems stemming from economics and politics. To this end, this innovation should be taken seriously, as it will not be some brief fad, but rather change the economy with its disruptive power.

Bibliography

Alchian, A. A., & Demsetz, H. (1972). Production, information costs, and economic organization . *The American economic review* , ss. 777-795.

Arrow, K., & Debreu, G. (1954). Existence of an Equilibrium for a Competitive Economy. *Econometrica* , ss. 265-290.

Bryan, M. F. (2004). Island Money. *Federal Reserve Bank of Cleveland* .
Capie, F., Mills, T. C., & Wood, G. (2005). Gold as a hedge against the dollar. *Journal of International Financial Markets, Institutions and Money* , 343-352.

Cawrey, D. (2014, March 5). *How Economist Milton Friedman Predicted Bitcoin*. Retrieved March 26, 2017 from CoinDesk: http://www.coindesk.com/economist-milton-friedman-predicted-bitcoin/

Christensen, C. M. (1992). Exploring the limits of the technology S-curve. Part I: component technologies. *Production and Operations Management* , *1* (4), ss. 334-357.

Christensen, C. M. (2013). *The innovator's dilemma: when new technologies cause great firms to fail.* Harvard Business Review Press.

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

CoinDesk. (2017, 3 6). *CoinDesk.com*. (P. Rizzo, Redaktør) Retrieved 3 26, 2017 from CoinDesk.com: http://www.coindesk.com/research/state-of-blockchain-q4-2016/

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation* , *1*, ss. 6-10.

Diamond, P. (1990). Pairwise credit in search equilibrium. *The Quarterly Journal of Economics* , *2* (105), ss. 285-319.

Drake, P. J. (2004). *Currency, credit and commerce: early growth in Southeast Asia.* Ashgate.

Duffy, J., & Ochs, J. (2002). Intrinsically worthless objects as media of exchange: Experimental evidence. *International Economic Review* , 637-673.

European Central Bank. (2015, February 1). *Virtual currency schemes – a further analysis.* Retrieved March 26, 2017 from European Central Bank: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

Fisher, I. (2006). *he Purchasing Power of Money: Its' Determination And Relation to Credit Interest And Crises.* Cosimo, Inc.

Fisher, I. (1933). The debt-deflation theory of great depressions. *Econometrica: Journal of the Econometric Society* , ss. 337-357.

Foss, N. J., & Mahnke, V. (2002). *Competence, governance, and entrepreneurship: advances in economic strategy research.* Oxford University Press on Demand.

Franco, P. (2014). *Understanding Bitcoin: Cryptography, engineering and economics.* John Wiley & Sons.

Freixas, X., & Rochet, J.-C. (2008). *Microeconomics of banking* (Vol. 2). Cambridge , Massachusetts : MIT Press.

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

Graeber, D. (2011). *Debt : the first 5,000 years.* Brooklyn, NY: Melville House.

Groenfeldt, T. (2017, March 5). *IBM And Maersk Apply Blockchain To Container Shipping.* Retrieved May 1, 2017 from Forbes: https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/#4f84939e3f05

Hajdarbegovic, N. (2015, January 29). *Why the Gates Foundation Doesn't Use Bitcoin.* Retrieved March 26, 2017 from CoinDesk: http://www.coindesk.com/bill-gates-gates-foundation-doesnt-use-bitcoin/

Higgins, S. (2016, May 26). *CFTC Grants Full Registration to Bitcoin Swaps Trading Platform.* Retrieved April 01, 2017 from CoinDesk: http://www.coindesk.com/us-swap-platform-registration-cftc/

Jack, W., & Suri, T. (2011, January). Mobile Money: The Economics of M-PESA. *NBER Working Paper No. 16721* .

Jenssen, T. B. (2014). *Why Bitcoins Have Value, and Why Governments Are Sceptical* . University of Oslo.

Jin, Y., & Temzelides, T. (2004). On the local interaction of money and credit. *Review of Economic Dynamics , 1* (7), ss. 143-156.

Kahn, C. M., & Roberts, W. (2009). Why pay? An introduction to payments economics. *Journal of Financial Intermediation* .

King, M. (2004). The institutions of monetary policy. *the American Economic review , 2* (94), ss. 1-13.

Kiyotaki, N., & Moore, J. (2000). *Inside money and liquidity.* Edinburgh: University of Edinburgh.

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

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, *4* (3), ss. 382-401.

Lapavitsas, C. (2004). *Social foundations of markets, money and credit*. Routledge.
Lucas, R. E. (1988). On the mechanics of economic development. *Journal of monetary economics*, *1* (22), ss. 3-42.

Luther, W. J. (2015). The monetary mechanism of stateless Somalia. *Public Choice*, *2* (165), ss. 45-58.

Luther, W. J., & Olson, J. (2015, February 25). Bitcoin is memory. *Journal of Prices & Markets*, *3* (3), ss. 22-33.

Luther, W. J., & White, L. H. (2016). Positively Valued Fiat Money after the Sovereign Disappears - The Case of Somalia. *Review of Behavioral Economics*, *3* (3-4), ss. 311-334.

Mankiw, N. G. (2010). *Macroeconomics*. Worth Publishers.

Markowitz, H. (1952). Portfolio Selection. *The journal of finance*, *1* (7), ss. 77-91.

Mikalsen, B.-E. (2017, April 25). *Sentralbanken kan bli banken din*. Retrieved May 1, 2017 from Dagens Næringsliv: https://www.dn.no/nyheter/2017/04/25/1730/Finans/sentralbanken-kan-bli-banken-din

Mill, J. S. (1848). *Principles of political economy with some of their applications to social philosophy*. JW Parker.

Millet, J. (2014, March 16). *Google Chairman Eric Schmidt: Bitcoin Architecture an Amazing Advancement*. Retrieved March 26, 2017 from NewsBTC: http://www.newsbtc.com/2014/03/16/google-chairman-eric-schmidt-bitcoin-architecture-amazing-advancement/

Minsky, H. (1982). The financial fragility hypothesis: Capitalist process and the behavior of the economy. *Kindleberger CP, Jean-Pierre Laffargue.*, *1*, s. 982.

Mises, L. v. (1981). *The theory of money and credit*. Indianapolis: Liberty Fund Inc.

Mises, L. v. (2009). *The Theory of Money and Credit*. Ludwig von Mises Institute.

Mubarak, J. A. (2002). A case of private supply of money in stateless Somalia. *Journal of African Economies*, *3* (11), ss. 309-325.

Nakamoto, S. (2008, October 31). Bitcoin: A Peer-to-Peer Electronic Cash System. *www.Cryptovest.co.uk*.

Nets. (2016, May 25). *Nets i blockchain samarbejde med Coinify*. Retrieved May 1, 2017 from Nets: https://www.nets.eu/dk-da/nyheder/Pages/Nets-udforsker-blockchain-teknologien-i-samarbejde-med-Coinify.aspx

Ngo, D. (2014, November 13). *BNP Paribas Research Reveals 5 potential Disruptive Impacts of Cryptocurrencies*. Retrieved May 1, 2017 from The Cointelegraph: https://cointelegraph.com/news/bnp-paribas-research-reveals-5-potential-disruptive-impacts-of-cryptocurrencies

Nobuhiro, K., & Wright, R. (1989). On money as a medium of exchange. *Journal of Political economy* , 927-954.

Nosal, E., & Rocheteau, G. (2011). *Money, payments, and liquidity.* MIT Press.

Ostroy, J. M., & Starr, R. M. (1990). The transactions role of money. *Handbook of monetary economics , 1*, ss. 3-62.

Ratha, D., De, S., Plaza, S., Schuettler, K., Shaw, W., Wyss, H., et al. (2016, April). Migration and Remittances – Recent Developments and Outlook. *Migration and Development Brief 26* .

Ratha, D., Eigen-Zucchi, C., Plaza, S., Wyss, H., & Yi, S. (2013, October). Migration and Remittance Flows: Recent Trends and Outlook, 2013-2016. *Migration and Development Brief 21* .

Rizzo, P. (2016, September 7). *Barclays Completes Blockchain Trade Finance Transaction*. Retrieved May 1, 2017 from CoinDesk: http://www.coindesk.com/barclays-completes-blockchain-trade-finance-transaction/

Rizzo, P. (2014, March 14). *Warren Buffett Urges Investors to 'Stay Away' from Bitcoin*. Retrieved March 26, 2017 from CoinDesk: http://www.coindesk.com/warren-buffett-investors-stay-away-bitcoin/

Rogers, E. M. (2010). *Diffusion of innovations*. Simon and Schuster.

Romer, P. M. (1986). Increasing returns and long-run growth. *Journal of political economy , 5* (94), ss. 1002-1037.

Rothbard, M. N. (1976). The Austrian Theory of Money. *The Foundations of Modern Austrian Economics* , 160-184.

Selgin, G. (2012, February 6). Synthetic Commodity Money. *SSRN* .

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

Shubik, M. (2004). *The theory of money and financial institutions* (Vol. 1). Cambridge: MIT Press.

Smart, E. (2015, May 27). *Top 10 Countries in Which Bitcoin is Banned*. Retrieved March 26, 2017 from Cryptocoinsnews: https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/

Smithin, J. (2002). *What is Money?* (J. Smithin, Red.) Routledge.

Sohn, T. (2016, October 24). *Blockchain Gets its First Test With International Trade.* Retrieved May 1, 2017 from InsideBitcoins: http://insidebitcoins.com/news/blockchain-gets-first-test-international-trade/36489

Solow, R. M. (1956). A contribution to the theory of economic growth. *The quarterly journal of economics , 1* (70), ss. 65-94.

Swan, M. (2015). *Blockchain: Blueprint for a new economy.* O'Reilly Media, Inc.

Sweeney, J., & Sweeney, R. J. (1977). Monetary theory and the great Capitol Hill Baby Sitting Co-op crisis: comment. *Journal of Money, Credit and Banking , 1* (9), ss. 86-89.

Tapscott, D. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Penguin.

USPS, OIG. (2014). Providing Non-Bank Financial Services for the Underserved. *White Paper .*

Visjø, C. T. (2016, November 20). *Forsker om utvikling av nasjonal digital valuta: – Norge henger langt etter andre land.* Retrieved 1 May, 2017 from E24: http://e24.no/digital/norges-bank/mener-norge-henger-langt-etter-i-innfoering-av-e-krone/23851255

Wang, J. C.-Y. (2014, February 11). A Simple Macroeconomic Model of Bitcoin . *Bitquant Research Laboratories .*

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

Williamson, O. E. (1989). Transaction cost economics. I *Handbook of Industrial Organization* (ss. 135-182). Elsevier B.V.

Yermack, D. (2013). Is Bitcoin a real currency? An economic appraisal. *National Bureau of Economic Research .*

Young, S. (2014, February 9). *Barclays launches investigation after customer data leak.* Retrieved April 1, 2017 from Reuters: http://www.reuters.com/article/us-barclays-data-idUSBREA1808020140209

Appendix

Potential use areas of blockchain:

I. Financial Instruments, Records and Models

1. Currency
2. Private equities
3. Public equities
4. Bonds
5. Derivatives (futures, forwards, swaps, options and more complex variations)
6. Voting rights associated with any of the above
7. Commodities
8. Spending records
9. Trading records
10. Mortgage / loan records
11. Servicing records
12. Crowd-funding
13. Micro-finance
14. Micro-charity

II. Public Records

15. Land titles
16. Vehicle registries
17. Business license
18. Business incorporation / dissolution records
19. Business ownership records
20. Regulatory records
21. Criminal records
22. Passports
23. Birth certificates
24. Death certificates
25. Voter IDs
26. Voting
27. Health / Safety Inspections
28. Building permits
29. Gun permits
30. Forensic evidence
31. Court records
32. Voting records
33. Non-profit records
34. Government/non-profit accounting/transparency

III. Private Records

35. Contracts
36. Signatures
37. Wills
38. Trusts
39. Escrows

40. GPS trails (personal)

IV. Other Semi-Public Records

41. Degree
42. Certifications
43. Learning Outcomes
44. Grades
45. HR records (salary, performance reviews, accomplishment)
46. Medical records
47. Accounting records
48. Business transaction records
49. Genome data
50. GPS trails (institutional)
51. Delivery records
52. Arbitration

V. Physical Asset Keys

53. Home / apartment keys
54. Vacation home / timeshare keys
55. Hotel room keys
56. Car keys
57. Rental car keys
58. Leased cars keys
59. Locker keys
60. Safety deposit box keys
61. Package delivery (split key between delivery firm and receiver)
62. Betting records
63. Fantasy sports records

VI. Intangibles

64. Coupons
65. Vouchers
66. Reservations (restaurants, hotels, queues, etc)
67. Movie tickets
68. Patents
69. Copyrights
70. Trademarks
71. Software licenses
72. Videogame licenses
73. Music/movie/book licenses (DRM)
74. Domain names
75. Online identities
76. Proof of authorship / Proof of prior art

VI. Other

77. Documentary records (photos, audio, video)
78. Data records (sports scores, temperature, etc)
79. Sim Cards
80. GPS network identity
81. Gun unlock codes
82. Weapons unlock codes
83. Nuclear launch codes
84. Spam control (micro-payments for posting)