universität wien

MASTERARBEIT

Titel der Masterarbeit

„Virtual Currencies:

Lessons learned from the Bitcoin example“

Verfasst von

Zuzana Bianchi, BSc.

angestrebter akademischer Grad

Master of Science (MSc)

Wien, 2015

Studienkennzahl lt. Studienblatt:	A 066 914
Studienrichtung lt. Studienblatt:	Masterstudium Internationale Betriebswirtschaft
Betreuer / Betreuerin:	Univ.-Prof. Dipl.-Vw. Thomas Gehrig, PhD

Eidesstattliche Erklärung

Ich erkläre an Eides statt,

dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe,

dass ich dieses Diplomarbeitsthema bisher weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe,

dass diese Arbeit mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Kittsee, 28.03.2015

_____

Zuzana Bianchi

Abstract

Bitcoin is a new concept of alternative or virtual currencies, which is used over the internet. Unlike other traditional currencies, Bitcoin does not have any central issuer, hence it is completely decentralized. Bitcoin is attractive due to its low transaction and operation costs. On the other side, since there are no fees, Bitcoin does not offer any additional protection or other services. Bitcoin is anonymous and its value is derived from the value assigned by people, but it is not redeemable for any commodity and they are not backed by governments.

This master thesis aims to answer the question whether alternative electronic currency, such as Bitcoin, can be considered money in terms of both classical economics view and libertarian view. The theoretical part analyzes the evolution of money in current monetary system and the alternative free banking approach and intends to put Bitcoin into one category. The reasoning shows that it is not possible to put Bitcoin into one current category, nonetheless it fulfills at the most the definition of currency that is however mixed with features of other categories (e.g. commodity). Criticism of Bitcoin in terms of money as a medium of exchange comes mainly from the Austrian School's definition, because it is not universally accepted (however could be considered secondary medium of exchange) and additionally violates Mises' regression theorem. Thus we cannot tell where the value of Bitcoin originated from. It continues with an analysis of Bitcoin technology, its merits and flaws. Empirical part shows Bitcoin prices and volumes. Last part summarizes current legal issues and regulation that is potentially applicable on Bitcoin and other virtual currencies.

Final reasoning explains that Bitcoin technology is not perfect and for now cannot be expected to replace any traditional currency. Even if Bitcoin fails, it is expected that this technological innovation and alternative idea is not going to vanish completely. It seems that the time for revising again the idea of private currencies has come. Thus it is necessary to critically examine present views about alternative currencies and to correct them if necessary.

Acknowledgements

I would like to thank my thesis supervisor, Univ.-Prof. Dipl.-Vw. Thomas Gehrig, PhD (http://ssrn.com/author=1598280) for his valuable advice and suggestions. He kept me on track with my paper and provided insights that haven't come to my mind before. In particular, he uncovered a whole new world of free banking, which is an exhaustingly interesting topic. I ended up reading various works rather than focusing on finishing my master thesis.

Additionally, I would like to thank my husband, Peter Bianchi, for his endless opinions and ideas, my step father, Igor Matecny, for his academic comments and my mother, Gabriela Matecna, for her patience, because it took so long.

And last, but not least, I would like to thank all the Bitcoin enthusiasts, who share their knowledge, observations and many interesting ideas. I'd like to give further thanks to http://blockchain.info for storing historical data.

Table of contents

List of figures

List of abbreviations

i.e.	That is
e.g.	For example
etc.	Etcetera
BTC	Bitcoin as a unit of a currency
CFTC	Commodity Futures Trading Commission
CPU	Central Processing Unit
EBA	European Banking Authority
ECB	European Central Bank
EMD	Electronic Money Directive
ESMA	European Securities and Markets Authority
FinCEN	Financial Crimes Enforcement Network
NMC	Namecoin
OTC	Over-the-Counter
LTC	Litecoin
P2P	Peer-to-Peer
POW	Proof-of-Work
PSD	Payment Services Directive
SEC	Securities and Exchange Commission

1. Introduction

In 2008 pseudonymous author(s) Satoshi Nakamoto released a paper, which described a new concept of electronic cash system and in 2009 the open-source software was released. He (they) introduced a peer-to-peer virtual money system, where online payments can be transferred directly without any involvement of a third party. They use digital signatures to prevent double-spending and additionally in this case avoid any third party by using peer-to-peer network (Nakamoto, 2008). They named it Bitcoin, which is the common name for software, network and currency. For the purpose of this paper, currency will be expressed as bitcoin (or BTC), with lower case "b", while Bitcoin will serve as a term for the whole system and network.

Since its introduction, Bitcoin has gained significant attention all over the world among hackers, libertarians and innovation-enthusiasts, but gradually also economists, governments and regulators. Bitcoin is an innovation that serves as an alternative to traditional payment systems, however it still should not be perceived as a substitution or a real competition to traditional currencies or monetary systems. In any case, Bitcoin or similar concepts of virtual currencies have a huge potential to provide consumers with the opportunity to choose something different than traditional ways of payment.

1.1 Research aim and paper structure

This paper aims to review the existing resources on virtual currencies, in particular Bitcoin, as the best-known and most spread virtual currency. Purpose of this master thesis is to describe Bitcoin as a technology, virtual currency and a potential threat to traditional currencies and monetary systems and to outline a framework of Bitcoin as a virtual payment system. Another objective of the paper is to put Bitcoin in the correct category of money, explain basic concepts of Bitcoin system, summarize current regulation possibilities and propose potential future evolution.

This paper tries to answer following questions:

1. Is Bitcoin money?
2. What is Bitcoin?
3. How does Bitcoin work?
4. Is it necessary to regulate Bitcoin (and other virtual currencies)?

5. How is it possible to regulate Bitcoin (and other virtual currencies)?
6. Is Bitcoin (and other virtual currencies) going to survive until the effective regulation arrives?

A large number of various resources can be found on the internet within this field. Even though many papers have been conducted by reliable institutions, most of the papers and articles have still been written rather by enthusiasts. Therefore this paper tries to exclude personal bias, describe only relevant aspects and value them from different perspectives. Master thesis is organized as follows: Section 2 describes the evolution of money, its functions and forms, current monetary and banking system compared to alternative libertarian view and also tries to put Bitcoin in the correct category. Section 3 illustrates Bitcoin in all its aspects. In order to provide a general overview of the extensive amount of all the relevant and less-relevant resources, this section will be divided in four parts. The first one explains Bitcoin technology and 2 types of users, the second studies historical evolution of Bitcoin prices and volumes, its volatility and liquidity, the third provides various reasons to regulate Bitcoin and summarizes current legal and regulatory issues and finally the fourth part identifies Bitcoin's possible future scenarios and its biggest competitors. Section 4 concludes.

2. Evolution of money

Money that we know today is the result of a centuries-long development. In the beginning there was barter, which was later replaced by copper, silver and other precious metals, coins, trade bills of exchange, and in the end the paper money. To describe the whole long process of money evolution would be out of the scope of this paper, but what we can clearly see from the history, is that demand for different forms of money has constantly modified. During the history, there were different authors, economist and thinkers who developed different theories on money.

If we intend to explain the origin and role of money, we have to go back to the basic question: why people actually enter into any exchange. Exchange represents the common agreement between two (or more) subjects about the exchange of ownership rights (of goods or services). It is apparent that both subjects expect some form of benefit or profit: *"Obviously, both*

benefit because each values what he receives in exchange more than what he gives up." (Rothbard M. N., 1963, p. 11).

Until the publication of Carl Menger's article "On the Origin of Money" (1892), the origin of money was perceived as a consequence of general social convention or a state decree. Menger (1892) dismissed such explanation and built up his own argument that money originated in the natural evolution on a free market in form of the most tradable commodity: *"Money has not been generated by law. In its origin it is a social, and not a state-institution.* (Menger, 1892, p. 51). During the process, the most tradable commodity will be selected, which will become the universal medium of exchange – money. Menger's (1892) original argument about "spontaneous" creation of money as a commodity on a free market was later supported by various studies by Austrian economists[1] and similarly by some "mainstream" economists.

To summarize very briefly the extensive amount of research in the field of evolution and origin of money, we can identify various streams of opinions. There were "mainstream" authors, like John Maynard Keynes representing Keynesians on one side and Milton Friedman on the other (monetarists)[2], further authors representing liberal views (e.g. Austrian School[3]), but there were also some other, rather marginal authors, like Sylvio Gesell[4] or today maybe Satoshi Nakamoto (Bergstra, J. A., De Leeuw, K., 2013). Nowadays we are witnesses of another transformation when people are looking for some change in the forms of money, or at least for some challenge to existing ones. Reasons for this desire may vary around the globe; some may be eager for technological innovations, others may not trust the current monetary systems or may need to legalize their earnings.

[1] Carl Menger is very often considered to be the founder of the Austrian school (*Investopedia.com*). The whole research regarding this topic is too extensive to describe all supporting arguments and therefore a more precise evaluation would be necessary *. This is however out of the scope of this paper, thus more subsequent and supporting arguments can be found e.g. in Mises (1990)*: Money, Method, and the Market Process*, Hayek (1978)*: Denationalisation of Money*, Rothbard (1976): *The Austrian Theory of Money*, (1983): *The Mystery of Banking*, Hülsman (1996): *Free Banking and the Free Bankers*, White (1984): *Competitive Payment Systems and the Unit of Account*, (1999): *The Theory of Monetary Institutions* and many more.
* Views of Austrian School of economics will be further applied in latter parts of the paper.

[2] Monetarism arises mainly from the quantitative theory of money and represents the idea of rational expectations of market participants and the governments' role to control money supply. The debate regarding the role of government is one of the main conflicts with Keynesians, who defend the stimulation of economy by government interventions through both monetary and fiscal policy.

[3] Austrian School believes in general in minimal government intervention.

[4] Sylvio Gesell proposed a theory of „Freigeld" – local currency with stable spending power, safe cash flow that was convertible into different currencies. It should have been a monetary system with zero interest on credit and the value that decreases over time (Roio, 2013).

2.1 Functions of money

We can find classical characteristics of money in any economic book on money, monetary systems or macroeconomics (e.g. (Mankiw, 2002)), where authors distinguish three different functions of money:

1) Medium or means of exchange – money is used as a form of payment and acts as an intermediary in exchange of products and services. Inefficiencies and inconveniences of barter system are avoided.
2) Unit of account – it is a standard measurement of cost and value of products and services or assets and liabilities, represented in a numerical unit. To fulfill this function, money must be durable, divisible, fungible, portable, acceptable, with limited supply and of specific weight, size or measure.
3) Store of value – it must be possible to save and store the money and retrieve it in the future (and once retrieved, it should be usable as a mean of exchange).

However, Austrian School of economics defines money as *"a single commodity that is universally employed as a medium of exchange"* (Mises, 1953, p. 33). According to the Austrian School, the other two classical functions of money are only the secondary functions. Menger goes even further and states that these two functions are not even necessary (Menger, 1892).

The way how money is created is also important. Originally, money was supposed to represent the tangible resource, which one could get in the exchange, e.g. precious metals and commodities, like food. If more money should be created, more resources had to be secured. But throughout the evolution of fiat[5] money, this rule has been broken and money could be "printed" without limits (Piasecki, 2012).

2.2 Current monetary and banking system vs. alternatives in terms of free banking and laissez faire[6]

Summarized picture of current monetary and banking system is represented by central banking and fractional reserve banking, where money is governed by monetary policies of

[5] Term fiat from Latin *"it shall be"* or *"let it be done"*.
[6] Term laissez-faire from French literally means *"let [them] do"*

central banks, not backed by any commodity (since 1971) and declared to be legal tenders. There is a trend of transmission of monetary competences to supranational levels, e.g. Eurozone. Main consequences of the current system are in particular growing amount of money that is not backed by any commodity, and inflation. Moreover, (non)-liquidity risk is increased (Gonda, 2008)[7].

As an offset to the current system, we can underline especially an alternative approach in terms of free banking.

> *"Professor Hayek is arguing that money is no different from other commodities and that it would be better supplied by competition between private issuers than by a monopoly of government. He argues, in the classic tradition of Adam Smith but with reference to the 20th century, that money is no exception to the rule that self-interest would be a better motive than benevolence in producing good results."* (Arthur Seldon[8]) (Hayek, 1976, p. 9)[9].

We can positively interpret this quote in a way that money does not have to be issued only by central banks. Hayek also stresses out the Diogenes'[10] quote that *"...money is the politicians' game of dice"* (Hayek, 1976, p. 33). He proposes the creation of monetary competition between money issuers and elimination of the central banks' monopoly. He additionally proposes practical schemes for switch to private currencies. However, in classical economic theory, the contrary is the case: central banks and their role are highlighted.

Clearly, we can identify two "rival" ideas: central banking (current system) on one side and free banking (alternative approach) on the other. First, the main principle of the central banking is the monopoly in currency issuance. It is only central banks, who have the authority to issue a currency. On the other hand, basic principle of free banking is to enable entering into contracts, which would be beneficial for both subjects. Everyone is allowed to open a

[7] Peter Gonda is economist and president of Slovak Conservative Institute of M.R.Štefánik, external lector of economics at Comenius University in Bratislava and a Slovak Senior Fellow of the Cobden Centre. Quotes come from the project *"Academy of classical economics"* from years 2008/2009.

[8] Citation from the preface written by Arthur Seldon in August 1976 to the *Denationalisation of Money* by Nobel Laureate F. A. Hayek

[9] For a long time, Hayek was a proponent of non-fungible role of central banks. Until publishing *Choice of Currency* (1976), Hayek was supporting neither laissez faire nor free banking unlike his mentor, Ludwig von Mises, who was on the other hand a strong supporter of both - gold standard and free banking (White, 1999). His opposite opinion, in favor of free banking, was first presented in *Choice of Currency* (1976) and after that in *Denationalisation of Money* (1976).

[10] Greek philosopher, known as *„Diogenes the Cynic"* from an early 4th century BC

bank that would issue its own (authorized) currency. Individual banks compete to attract the most clients possible. It is assumed that all market participants are following their own interest and the major goal is to maximize their own benefit. Banks would therefore issue such kind of money that complies with the demand of their clients at the best.

Arguments pro central banking system include disbelief that market alone could survive unique situations such as bank panics or bank runs. Which in turn leads to (non)-liquidity risk of commercial banks. Furthermore, central banks' role as a lender of last resort guarantees systemic liquidity and solvency (Susanu, 2011). This can however lead to moral hazard, since commercial banks are aware of this guarantee. Nevertheless, for now we could conclude that central banking system seems to safeguard the monetary stability. On the other side, opponents of central banking argue that the supply of money in centralized system cannot respond appropriately to demand changes (Selgin, 1957). And it is obvious from the past that imbalanced money creation may lead to liquidity crises caused by either inflation or deflation. On the contrary, in a free banking system, situation with imbalanced money creation is almost impossible, since one of the principles of free banking is the supply of money "controlled" by (free) market forces. Proponents of free banking argue that stability would arise automatically on a free market.

Austrian School economists propose various ideas in free banking, but for the purpose of basic illustration of the system, we can outline three concepts:

1) System of competition in currency in terms of private issuers – discussed e.g. by (Hayek, 1976) in *Denationalisation of Money*. As already the name of this work indicates, Hayek proposes to replace political influence in determining the amount and value of money by market forces, thus proposes the currency competition. In this way private money would originate. Everyone should be able to issue own "symbolic" private currency, which shall be in turn convertible for competing currencies. According to Hayek, due to competition, each issuer would try to keep the currency as stable as possible. This system would lead to the end of central banks' issuance monopoly and to the beginning of various private currencies circulating in diverse areas, without limit to state borders. However there is a risk that people must not be willing to accept such unknown currencies. Risk of inflation is not expected by Hayek, due to competition in currency and banking system (Hayek, 1976).

2) System of fractional commodity backing – discussed e.g. by Selgin (1957) in *The Theory of Free Banking: Money Supply under Competitive issue* or White (1984) in *Free Banking in Britain*. This is a system of competing issuers of notes that are (partially) exchangeable for the most tradable commodity (gold, silver, etc.). There were approximately 60 areas where using of the fractional commodity banking system was allowed (some in terms of free banking) throughout the history. Example could be Scotland (1716-1844), Switzerland (1826-1850), New England in USA (1820-1860), etc. (Gonda, 2008).
3) System of 100% commodity backing – discussed e.g. by (Mises, 1953) in *The Theory of Money and Credit*, or Rothbard (1962) in *The Case for a 100 Percent Gold Dollar*. Banks won't be allowed to lend deposited money by clients to third party, because it would lead to the situation, when two different parties have ownership rights for the same "piece of currency metal" – owner of the note or a deposit and obligor whom the bank borrowed the money. There are no significant cases of free banking system with 100% commodity backing throughout the history (Gonda, 2008).

One of the main conditions for monetary reform in terms of free banking would be the re-introduction of commodity (e.g. gold) backing as prevention against inflation. Consequently, issuance monopoly should be removed and practical conditions for currency competition should be established. The whole monetary reform would require several adjustments of current system, for example constitutional and legal amendments.

On the other hand, there are several arguments for the necessity of central banks. Central banks should first of all ensure financial stability. It should regulate inflation and price stability and as already mentioned, act as a lender of last resort, thus provide liquidity for the whole economy. (Susanu, 2011). We can see that goals of central banks are at both macroeconomic and a microeconomic level. Concept of lender of last resort is necessary in fractional reserve banking and therefore under this current scheme, central bank is inevitable.

Generally, there is a consensus about advantages of private ownership and positive effects of competition in economy. However, competition in the segment of money is supressed. Clearly, a question arises - why is the banking industry different from other industries? Personally, I cannot say that I would strongly prefer any of the two sides of this debate. I can see both - strengths and weaknesses or opportunities and threats in either point of view. But

for the purpose of this paper, free banking point of view would be definitely more favourable than the current scheme.

From the above mentioned arguments, it is obvious that the real reason for current central banking system is rather unknown. It is questionable whether the final verdict for central banking was made for the real benefit of economy (-ies) or somewhat for the benefits of centrally governed systems. There is no evidence that private currencies (or some system in terms of or similar to free banking proposal) could really harm monetary stability and public money. It is also possible that the non-allowance of private currencies is rather a precaution for potential loss of monopoly in issuance of money, since there are various economic and political influences driving decisions for monetary schemes. We can only incline to one or another stream of thoughts and I personally do not see a reason, why money is not let to be driven by market forces. I assume that competition in money, similarly as competition in any other sector, could be beneficial for consumers. In particular, to be able to choose their most preferred currency and exchange it for any other in case of changed preferences. I incline rather to libertarian ideas of free banking where consumers would be able to choose the most appropriate currency (-ies) for their particular purposes. Also in terms of this paper, reconsideration of official support of private currencies would be preferred.

2.3 Forms of money - money vs. currency

There is basically only one huge difference between money and currency. Currency fulfills all the functions of money mentioned above except for one – store of value. Money can be retrieved after long period of saving and its purchasing power will stay more or less unchanged. Many people have argued that inflation decreases the ability of money to act as a store of value. However, this decreased ability should be valid for currencies rather than money. Inflation reduces the value of currencies, but does not reduce the value of gold, for example, that indeed fulfills all the functions of money.

There are various forms of money. According to Mises (1953), money in the narrower sense can be divided into three subcategories: commodity money, fiat money and credit money. For the purpose of this paper, we can avoid credit money[11]. Commodity money originated as a

[11] In short, Mises defines credit money as: *"That sort of money which constitutes a claim against any physical or legal person"* (Mises, 1953, p. 61).

natural medium of payment, such as cloth, livestock or fur, but especially precious metals (in particular gold). Term fiat money (or symbolic money) is currently describing most of the modern currencies.

At present, services in relation with money in terms of exchange, such as travel cheques or credit and debit cards are offered by private parties. However, the situation with "real" or "final money" is different. In simplified terms, all money that we know today and that comply with general definitions, are referring to "public money". But nowadays, especially due to electronic currencies such as Bitcoin and its (rather marginal) competitors, the topic of private money comes back to life.

2.3.1 Gold

Throughout the history, gold has been widely used all around the globe. Initially, having gold was a sign of status; however the most notable is its role in history of money. During the Gold Standard system, gold was used to back the value of money, in other words paper money could be converted into a particular amount of gold. After the fall of Gold Standard, many argue, that paper money has lost its real value and therefore gold is one of the only "real money". Nowadays many suggest that in terms of functions of money, gold still fulfills the definition of money at the most. Gold has always served as a form of exchange, store of value and always was a unit of account. It is often described as commodity money (Mankiw, 2002).

2.3.2 Fiat currencies

After the fall of the Bretton Woods system (1971), most traditional currencies have often been called fiat currencies, because they are used only as a medium of payment and have no intrinsic value. They are authorized by governments to be legal tenders, but they are not backed by any physical commodity. This creates a risk of becoming worthless, caused by potential hyperinflation. People can as well lose faith in a fiat currency, which may lead to loss of any value of the money. Nowadays traditional currencies (fiat money) are not convertible and cannot be retrieved after long period of time, thus they do not fulfill the function of money as being a store of value.

2.3.3 Alternative and virtual currencies

Over the history, people always looked for some advances of current money and some decades ago, some of them started thinking even of electronic forms of money. One cannot stop the evolution and technological progress and thus the upgrades of our current monetary schemes and systems are almost inevitable. In 1994, American journalist and author of various books, Steven Levy, published an article "E-Money (That's What I Want)". He claims, that *"…credit cards and ATM cards are becoming increasingly popular, but it lacks privacy and security…"* which may lead to *"…demand for efficient electronic-money systems to prevent fraud and protect user privacy…"* (Levy, 1994). Also Milton Friedman proposed the elimination of the Federal Reserve by replacing it by some automated system or a mathematical model *"…that would keep the quantity of money going up at a steady rate"* (Roberts, 2006). Friedman argued that this would put a lid on inflation.

There are cases of alternative or digital currencies that existed for some period of time, but have ended up with a shut down. One example would be the e-gold, a digital currency backed by gold (Grinberg, 2011), whose creators were prosecuted and convicted of various financially-related crimes (Dion, 2014). Very similar story would be the one of Liberty Dollar, *"…currency backed by gold, silver, or other precious metals, and was intended to be inflation-proof…"* (Grinberg, 2011, p. 191). Anyhow, the shut-down of Liberty Dollar was rather a fight against fraud[12] and counterfeiting than against digital currencies. Liberty Dollars were declared illegal because they were too similar to official U.S. currency and government intended to avoid consumers' confusion, and simultaneously Liberty Dollars were said to attempt to compete with US Dollars (Dion, 2014; FBI, 2011).

Recently, topic of electronic money, digital cash or crypto-currencies is gaining on importance. European Central Bank (ECB, 2012) distinguishes between electronic money and virtual currencies. First one represents monetary value, it is stored electronically and it is accepted as a medium of payment. The main attribute of electronic money is its link to traditional money (e.g. EUR, USD, etc.). Electronic money is regulated and supervised, which is not valid for virtual currencies. On the other hand, virtual currencies are digital money that is commonly controlled only by its developers. They are issued by private parties and are spread over the Internet (Herpel, 2011). Virtual currencies are not denominated in traditional

[12] Value of the metal content was lower than the face value of the currency.

money; therefore the issuer has a full control and manages the supply. Digital currencies are usually very transparent and publish the information online, according to regular audits (Herpel, 2011). Digital accounts can be created for free and fees for account operations are generally offered at lower costs than those from banks. Since these operations are not dependent on any financial institution or financial intermediaries. Earnings from digital currencies are not subject to taxation, which is ensured by the anonymity (Marian, 2013).

According to ECB, three subcategories of virtual currencies can be distinguished – (1) currencies without any or only limited link to traditional money or real world (usually used in online games), (2) currencies that can be bought by traditional money at a specified exchange rate, but cannot be re-exchanged back (for example frequent-flyer programmes, since users usually get bonus points for buying a real good, or can directly buy bonus point by traditional money, cannot re-exchange them but points can be used to buy real products and services) and (3) currencies that can be bought by and sold for traditional money at a specified exchange rate and usually can also be used for purchases of virtual and real products and services (ECB, 2012).

2.3.4 Bitcoin

Unlike electronic money, Bitcoin does not really have any issuer (Marian, 2013). It is a decentralized digital crypto-currency or as well called peer-to-peer[13] currency. It is decentralized because it does not have any central authority (to create it, to issue it or to track it), digital because it is not possible to „download it" in the form of real coins or bank notes and crypto-currency because all the financial transactions are secured by cryptography SHA256 and ECDSA (Jiricek, 2012), "in order to prevent the abuse of the system" (Piasecki, 2012). One of the possible abuses could be counterfeiting by the double-spending[14], but in this case, Bitcoin has developed a solution that does not involve participation of any third party.

Transactions in the "Bitcoin world" are not denominated in traditional currencies (unlike on PayPal), instead, they are denominated in bitcoin = BTC. Its value does not come from its

[13] P2P means that there is no middleman. P2P is usually used in file-sharing or torrents – users are dealing directly with their peers. There are no banks, clearing houses, no fees to pay for credit card transactions.

[14] Many earlier developers of virtual currencies thought that it is impossible to solve the double spending problem without any central authority. However, Bitcoin created a system with *"…the list of all approved transactions to date"* (London, J.P., Melbourne, G.T., 2011).

inherent value and neither is derived from any precious metal or government fiat currencies. Its value comes from the actual value assigned by people (Brito, J., Castillo, A., 2013), its limited supply and mathematical algorithms (Piasecki, 2012). According to ECB analysis, *"…Bitcoins' theoretical roots can be found in the Austrian school of economics, in particular the criticism of fiat money system and government interventions, with the result of massive inflation and business cycles…"* (ECB, 2012, p. 22). As discussed in subchapter 2.2, Austrian economists proposed the system of private currencies, hence currency competition. However, Bitcoin does not follow completely their ideas. We can see a pattern mainly in framework of private currencies. But at this stage, Bitcoin does not seem to intend to compete with traditional currencies; it rather provides an alternative in cash systems.

In particular, in terms of free banking, Bitcoin has some attributes that do not comply with free banking ideas at all. Free banking suggests that the imbalanced money creation is not likely, because money supply will be driven by market itself. However Bitcoin has a limited supply and the amount of bitcoins in circulation grows linearly. Therefore the automatic stability driven by free market is not the case for Bitcoin. Bitcoin supply neither corresponds to the actual demand nor responds adequately to demand changes. And additionally, neither the market demand drives the supply as in free banking proposal nor does any central authority adapt it. It is driven purely by mathematical algorithms that make the supply grow linearly. And besides, it is highly questionable what will happen once the maximum amount of 21mn bitcoins will be created. This fixed money creation may lead to either inflation or deflation; however proponents of Bitcoin say that its built-in deflationary nature (more details in chapter 3) is rather a positive aspect. Additionally, free banking always proposed some commodity baking to prevent inflation. However, Bitcoin is not backed by anything, it is completely virtual. On the other hand, central banks should ensure financial stability and act as a lender of last resort. Again, this is not the case of Bitcoin. In subchapter 2.2 we have identified two different schemes, either fractional reserve system or full reserve system, however Bitcoin does not comply with any one of these. But this does not necessarily mean that Bitcoin is definitely a bad idea. It is rather an innovation because of which it will be necessary to either adapt the existing schemes or create some new frameworks, which would encompass Bitcoin and other virtual currencies with all their built-in features, unknown by now. But this is probably only valid under the condition, that Bitcoin and other virtual currencies will attract significant amount of users or reach significant volumes.

In terms of Bitcoin's precise definition, economists suffer from trying to put Bitcoin in the correct category. Is it money, currency, commodity, financial asset, platform, protocol, or something in between? Next subchapters will compare Bitcoin in terms of money, currency, commodity and security. Proper definition is an important issue, in particular for the case of some possible regulation. If bitcoins should ever be regulated, it has to be done under some regime and it has to be defined precisely. The whole story behind Bitcoin will be subsequently discussed in more detail in chapter 3 and the possible regulation in subchapter 3.3.

2.3.4.1 Bitcoin in terms of money and its functions

One of the most elementary and difficult issues regarding Bitcoin is its specification. What Bitcoin actually is? Can we define it as money? Money is any "object or record" that is accepted as payment (Piasecki, 2012) or a "method" how people can get products and services. Three main functions of money have already been described in subchapter 2.1 and now we can apply them to analyze Bitcoin in terms of money.

As mentioned before, Bitcoin, similarly as money, is used as a form of payment and acts as an intermediary in exchange of products and services and therefore fulfills the former definition of medium of exchange. However from the point of view of Austrian School, Bitcoin does not fulfill the function of money as being a medium of exchange (only the secondary medium of exchange), because it is *"not universally accepted"* (Surda, 2013). Mises states that secondary media of exchange obtain their value from two types of demand: *"the demand related to their services as secondary media of exchange, and the demand related to the other services they render"* (Mises, 1963, p. 463). Rothbard (1970) defines this type of medium of exchange quasi-money - assets that become so marketable and liquid, such that they *will "become more generally used until they could be called money"* (Rothbard M. N., 1970, p. 826). Despite the fact that it is not universally accepted in terms of money by Austrian School, we can clearly say that Bitcoin is still being used as a medium of exchange. But the crucial condition is that Bitcoin has to be commonly desired – ones must want Bitcoins, others must spend it (Meyer, 2014).

In terms of store of value, it must be possible to save and store the money and retrieve it in the future. It could be in theory true for the case of Bitcoin, however many argue, that Bitcoin definitely cannot be used as a store of value. Paul Krugman (Krugman, 2013) claims, *"…that*

it is completely unclear, why Bitcoin should be a stable store of value". J.P. Morgan also takes Bitcoin as a *"terrible store of value"* (Vaishampayan, 2014), because it *"could be replicated over and over"* (Calouro, 2014). Also the currency's huge volatility can cause many troubles, when it is used as a store of value. It is not reasonable to keep savings or manage business finances in bitcoins, when the volatility is wild and unpredictable (Brito, J., Castillo, A., 2013). Many argue that it is exactly the high volatility that keeps Bitcoin from being an appropriate store of value (Meyer, 2014). Nowadays, Bitcoin cannot be perceived as an ideal store of value and even though it is possible, that bitcoin prices and volumes will stabilize in the future, from what we can see at the moment, it is highly questionable if it can ever become a really suitable store of value.

Lastly, being a unit of account, money has to be a standard value measurement of products and services, represented in a numerical unit. This appears to be the most difficult part while defining Bitcoin as money.

Apart from the above mentioned basic definition, money should also be *durable* (since Bitcoin is a decentralized P2P money, traded over the internet, we can say that Bitcoin is as durable as internet (Keiser, 2013)), *divisible* (there are smaller units – Satoshi: 1BTC = 100.000.000 Satoshis), *fungible* (one Bitcoin always equals another Bitcoin, and the same is valid for one satoshi, which is precisely calculated by computers and can be traded without changing in value), *portable* (since Bitcoins are traded in the online world, it can be downloaded anywhere and therefore it is perfectly portable and even "more portable than traditional currencies" (Piasecki, 2012)), *acceptable* (here we cannot say that Bitcoin is universally acceptable, so far it has been accepted only by a limited community, however this could change eventually), *with limited supply* (number of Bitcoins won't ever exceed 21 million and this amount is nowadays scheduled for the year 2140) and *of specific weight, size or measure* (since Bitcoin is a digital currency, we cannot define specific measures in real terms, however it is precisely defined in terms of computer science and data).

From the above analysis, it is obvious, that it is quite difficult to put Bitcoin completely even in the category of money. It clearly does not fulfill all the conditions, but still it probably fits to this category at the most.

2.3.4.2 Bitcoin in terms of currency

In a general sense, currency is anything that is used as a medium of exchange. Legal definitions require that the currency is issued, used and accepted by a country, which is not fulfilled by Bitcoin. In the United States, *"...federal government has an "exclusive right to issue currency"..."* (Grinberg, 2011, p. 182), in European Union, it is the ECB. Generally, it is always a central bank, which issues the local currency. They have a "monopoly" on issuing their own currency and nothing else should be accepted or in some cases is even illegal[15]. There are examples of both types of alternative currencies; ones that were in the end shut down according to some US laws (e.g. Liberty Dollar), but also community currencies, which were described as non-threating.

Bitcoin indeed fulfills the characteristic of being a medium of payment. It is however questionable, whether it does not contradict some currencies laws. By currency it is often understood the "current money" that is generally accepted in a geographic area. This definition would not cover bitcoins, until it does become a generally accepted currency in any geographic area.

2.3.4.3 Bitcoin in terms of securities

Some argue that Bitcoin should be defined and regulated as a security, because it resembles "investment contracts". Supporters of Bitcoin argue that it does not fulfill the definition of investment contract, while opponents argue that Bitcoin meets all the requirements to be an investment contract.

According to Securities Act of 1933 Sec. 2. (1), security is defined as *"any note, stock,..., certificate of interest or participation in any profit-sharing agreement,..., investment contract,..."* (SEC, 1933, amended and approved on April 5, 2012, pp. 1-2) and the long list of other things. What we can find as a general definition, is that security is a financial instrument of different kinds, including stocks, bonds and other instruments, which represent financial value.

[15] e.g. The US Stamp Payments Act of 1862, which states: *„Whoever makes, issues, circulates or pays out any note, check, memorandum, token, or other obligation for less sum than $1, intended to circulate as money or to be received or used in lieu of lawful Money of the United States, shall be fined under this title or imprisoned not more than six months, or both."* (U.S. Code, Crimes and Criminal Procedure, amended in 1994, September)

Bitcoin is definitely neither a note nor a stock. What attracts the attention is the part of investment contracts. Investment contract for purposes of the Securities Act means *"…a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party…"*[16] (Grinberg, 2011, p. 196). It is almost impossible to finally prove neither the common enterprise nor individuals' intention of future returns and therefore it is improbable, that bitcoin could be defined as a security under the definition of an investment contract. But it should be anyway discussed in more detail whether bitcoin trading creates some kind of investment contract.

2.3.4.4 Bitcoin in terms of commodities

Due to the fact that there is a given fixed number of bitcoins, it is also often treated as commodity, *"… which are generally held not to be securities"* (Grinberg, 2011, p. 199). Ownership of bitcoin gives the owner right to use it, to sell it or to make contracts with it. Generally, commodities are tangible, which Bitcoin does not fulfill, even though some Bitcoin enthusiasts analyze why bitcoins are tangible. Secondly, commodities have inherent value, which is also arguable in the case of Bitcoins, since they do not have any central authority or commodity to back them. However, as already mentioned, proponents argue that bitcoins do have inherent value, resulting from the limited supply, or from their feature of being rare over time. Bitcoin's value is determined by supply and demand and it is questionable how much is the value dependent on software developers' effort.

[16] Proponents, who are usually those who think that Bitcoin cannot be defined as an investment contract, argue that individuals do not invest money. They argue that individuals invest rather their computational power and time, for which they are awarded with bitcoins (explained later in subchapter 3.1). However, obviously most of the Bitcoin users do buy bitcoins on some exchanges. They also argue that there is no common business with intention to boost money through investments and that all the Bitcoin users and promoters are independent from each other. On the other hand, Bitcoin opponents argue that individuals invest their money in a common enterprise, in a meaning that all people holding bitcoins are earning, when the value of bitcoin increases. Common enterprise can be also understood as a group of software developers, who secure money-supply and technical properties, which are very important factors that influence bitcoin's value.
Bitcoin's proponents as well argue that no general expectation of profits exists and that not even some Bitcoin speculation necessarily indicates that. However, we can assume a high probability, that many (or most) of Bitcoin users do expect profits, for example also because of its inflation-resistance. Bitcoin's opponents on the other hand argue that returns from investments do come *"…solely from the efforts of the promoter or a third party"* (Grinberg, 2011, p. 196), since investors do not play an active role in Bitcoin's management, but they indeed do need efforts of the developers. By contrast proponents also argue that bitcoins have inherent value that results from the feature of limited supply and thus no efforts of developers or any other third party is needed.

In the United States, according to Commodity Exchange Act commodities are *"…and all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in."* (U.S.Code, Commodity Exchange Act, amended in 2001). Bitcoin fulfills this definition and therefore from this perspective could be handled as commodity in the United States.

2.3.4.5 Summary on Bitcoin classification

Economists from Goldman Sachs (Shieber, 2014) argue, *"…that Bitcoin, together with other digital currencies, lie somewhere between currency, commodity and financial assets"*. They would define Bitcoin as *"speculative financial asset that can be used as a medium of exchange"* (Shieber, 2014). Selgin (2013) defined Bitcoin as a synthetic commodity money, because it lies somewhere between fiat and commodity money. It is said to be a unique hybrid, which is on one side scarce medium of exchange (however artificially) but does not have any monetary value on the other. We can also conclude, that Bitcoin, similarly as many other current (and possibly future) digital currencies, share some features with commodities, securities, currencies and monies, however does not fulfill all the characteristics of any.

From the other perspective, Bitcoin is definitely private and not centralized, but it does not follow any particular current rules or frameworks. As already mentioned, the "Austrian regime" of free banking would be favourable for Bitcoin, since private competing currencies would be allowed. However, this scheme was never widely employed and accepted, and Bitcoin alone is not going to be the reason to reopen or reconsider the case. There would need to be a significant reason to start some strong initiatives against current monetary system and central issuance, which would lead to official allowance and acceptance of private currencies.

3. Bitcoin

Bitcoin is a digital currency running on the internet. Over its existence, it has gained many supporters but also many antagonists. Bitcoin is attractive in particular due to its no or very low transaction and operation costs. But since users do not pay any transaction fee, there is no protection or additional service included. And since there is no central authority, there is neither any "institution" to "call back" nor any fraud protection available. Bitcoins are perfectly divisible, thus they can be used for micropayments and sending them is very fast.

They provide high level of anonymity and their value is derived only from the value assigned by people. On the other hand bitcoins are not redeemable for any commodity and they are not backed by any government. This may be perceived as both advantage and as well disadvantage. Transactions in bitcoins are irreversible - once you have sent the money, there is no way back. Processed and confirmed transaction cannot ever be cancelled (Jiricek, 2012).

Interesting question is whether Bitcoin does have an intrinsic value. But on the other hand, does a fiat currency have an intrinsic value? There are two opposite views on intrinsic value of fiat currencies. One group argues that fiat currencies are intrinsically valueless by definition and only used as a medium of payment. But let's now take a dollar as an example – even though the "paper" itself does not have any value. Americans still need dollars to pay their taxes and the US government does not accept any other currency. And this is what generates real value for the US dollar (Weisenthal, 2013). The similar is valid for Bitcoin. For example Max Keiser argues in his article published in Huffington Post, that Bitcoin indeed has an intrinsic value, but this intrinsic value is *"very 21st century"* (Keiser, 2013). He puts privacy on the top list of desirable and scarce assets over the past 30 years. Therefore he concludes that Bitcoin has its intrinsic value. Others put the finite amount of Bitcoins as an explanation of its intrinsic value. But this scarcity does not give Bitcoin a lasting value (Weisenthal, 2013). Bitcoin has a value only because some other people will accept it or will be willing to pay you more than you have bought it for.

Another compelling feature of Bitcoin is its limited supply. Number of Bitcoins is programed on a limit of around 21,000,000 BTC (this maximum should be reached approximately in year 2140). Total supply is set by mathematical algorithms. Since there is no central authority, no one can devalue or detract the currency. Due to some other built-in features, there is almost no inflation possibility. On the contrary, Bitcoin is actually deflationary and the value of 1 BTC should rise. Many people ask if it really makes sense to decrease the rate of bitcoin creation with time, because it may cause huge deflation if the demand grows faster than new bitcoins are created. There are two opposite arguments to this issue. First of all is the factor of mining (explained below in subchapter 3.1.2), where Bitcoin has a system for adding new money at a rate that is decreasing. Second is the almost infinite divisibility of bitcoin.

The earliest users that adopted Bitcoin were usually members of hacker community who never really used bitcoins as a currency. Later, bitcoins started spreading in black market, because it was easy to use bitcoins for buying drugs or gambling. Some people decided to put

some money into this technology and currency innovation just for fun and because price of 1 BTC was really small at the inception. Subsequently, people started "investing" in Bitcoin and hoping for increasing exchange rate. Nowadays different businesses accept payments and micropayments in bitcoins, there are many ways where and how to use them and people have various reasons for buying and trusting the whole Bitcoin idea. Many of Bitcoin enthusiasts can be defined as being sceptical of financial institutions, governments or central banks; as libertarian oriented types, who fear constant inflation and believe that some currency, which would be resistant to inflation, would be economically beneficial; as types who are looking for privacy, anonymity or autonomy in financial transactions (Serwer A., Liebelson D., 2013); or as criminals or speculators.

Bitcoin market is expanding and its usage is increasing. One can pay with BTC in e-shops, buy gold, rent servers and web hosting, but also buy normal goods in shops that accept bitcoins. They can be traded as well and price for the buy and sell is set by supply and demand. There is a number of BTC applications and exchanges[17] that offer the exchange of bitcoins for other currency and vice versa. Some systems also allow users to exchange bitcoins between each other. Nowadays, there are also several ATMs for Bitcoins, which are mostly used as an exchange machine, where people can buy bitcoins for cash. Some models should as well allow the sale of bitcoins for cash. There are also less formal OTC exchanges, where option contracts are being sold.

3.1 Bitcoin Technology

Bitcoin is based on Proof-Of-Work[18] and its service operates on Peer-to-Peer (P2P) network, referred to as Bitcoin network (Karame G. O., et al., 2012). There are 2 types of Bitcoin users.

[17] The most reputable exchange was MtGox.com (name is derived from "Magic: The Gathering Online eXchange"). It was one of the oldest Bitcoin exchanges, offered quick and secure trading of Bitcoins and recorded historical statistics of BTC exchange rates. By 2013, 70% of all transactions were held on MtGox. However in February 2014, MtGox closed its exchange services, website and discontinued trading. In April 2014, MtGox began liquidation proceedings and informed that ca. 850,000 BTC are missing and that they were very likely stolen. At that time, the value of missing Bitcoins was more than $450mn. 200,000 BTC have been found since, but it is still unclear, why they even disappeared. There are various speculations, but none of them has been proven yet.

[18] Proof-of-work protocol is a vehicle, which can effectively prove to one user that someone else has engaged significant amount of computational effort (to validate the transaction). POW system helps solving the problem of double spending without any central authority. System itself combines two ideas: on one hand it should be computationally costly and difficult for users of the network to verify transactions and on the other, users should be awarded for their efforts to verify these

First are traditional Bitcoin users - clients, who perform money transactions and the second are "miners", who confirm money transactions of traditional Bitcoin users. New Bitcoins are created by "mining" performed by the second group of users.

3.1.1 Traditional BTC users

From the most basic perspective, Bitcoin can be described as a mobile application or a computer program, which serves as a personal Bitcoin wallet that can be used for sending and receiving bitcoins. Most of the Bitcoin users know bitcoins in this way.

Everyone who wants to own or transact bitcoins has two possibilities. Either to install a program on their computer, which implements the Bitcoin protocol (referred to as Bitcoin client) or to make an account on website (Grinberg, 2011). Bitcoins are saved by Bitcoin client in a special file called the wallet. Transactions are anonymous because wallet is represented only by a text chain, which includes information about source address, destination address and amount. There is no information that could identify persons. Wallet is placed on computer drive and therefore no one can freeze it, but with insufficient security, someone can steal it. Therefore each user has to secure and backup his wallet. The online wallet is a web application, which creates a wallet right after the registration of the user. Main advantage of the online wallet is that user can access it anywhere in the world and perform transactions immediately, right after the authentication. However it bears as much risks as Internet itself and it might also happen that the provider of the page denies or blocks the access to the wallet.

In this part of Bitcoin story, concepts of digital signatures[19] and public key cryptography[20] are very important. Each Bitcoin user owns two keys – private (kept secret such as password) and public (can be shared). Every bitcoin address has its own keypair (private and public), which

---

transactions. Since it is too costly for one user to validate the transaction, it is it is much quicker to find a block collectively that individually. The whole concept of proof-of-work is said to be the least intuitive part of Bitcoin.

[19] Digital signature is a scheme used for verifying the authenticity of digital documents, messages, financial transactions, etc. Digital signatures serve as a proof to the recipient that the sender has sent the document, message or transaction and that it hasn't been changed during the process.

[20] Public key cryptography is a type of cryptographic algorithms, where two separate keys are necessary. One is secret (private) and the other one is public. These two keys are mathematically linked. Private key is used to create a digital signature and public key is used to verify it. It is also known as asymmetric cryptography, in which two different keys have opposite ("asymmetric") functions.

is stored in the wallet. These keys do not contain any information, which could identify the user and therefore all the transactions are pseudo- or quasi-anonymous[21] (Luther, W. J., Olson, J., 2013). If someone wants to send money, he creates a transaction, which he has to sign with his private key. This transaction authorizes a reference to some previous transaction that justifies the user, so that bitcoins cannot be created out of thin air and in the same time prevents from spending the same coins twice (double-spending). We could compare this transaction with a bank transfer. All transactions are registered in a public ledger – block chain and transmitted to the Bitcoin Network so that it becomes valid and spendable (Piasecki, 2012). When a transaction is encrypted by a private key, it can only be decrypted by a public key and vice versa.

3.1.2 Miners

The most interesting way how to get bitcoins is via mining. The most common reasons for mining are basically fun and reward. In the early stages of Bitcoin history, every user was also a miner. Nowadays, most of miners are Bitcoin enthusiasts rather than people who want to get rich. Precise technical analysis would be out of the scope of this paper, but some quick overview is anyway necessary.

User of the network provides his "computer power" for confirming transactions and in return he is rewarded with a particular amount of bitcoins. Computers look for codes and numbers (often named as "solving mathematical problems" or "solving puzzles") that haven't been discovered yet and once they discover them, they can be transmitted as coins into the network. In reality, this does not really involve solving of complex mathematical problems, but it is rather a systematic attempt to match different potential solutions to the current prerequisites. In other words, the purpose of mining is that miners provide their processing powers to contribute in verifying bitcoin transactions. All the miners over the network try to solve the puzzle over and over, until only one miner finally "solves the puzzle", thus his computer finds an answer to the particular mathematical problem, needed to validate the transaction. It takes on average ten minutes for some miner to become successful. This successful miner will be

[21] There is a public database, where anyone can see all transactions form all the accounts, but it does not match transactions to individuals, who can create unlimited number of accounts. So if a user never reveals his personal identity in connection with his private key, Bitcoin system provides him with anonymity. However, when purchasing bitcoins on some exchange, user has to provide some information, such as a bank account number or credit card number.

rewarded for his effort with a particular amount of bitcoins. Afterwards, other miners will see the result and if the transaction is really valid, they will continue solving the next puzzle.

More specifically, miner is a "peer" in the (peer-to-peer) network who collects transactions that need to be verified and tries to organize them into blocks. Once a miner finally verifies a transaction, he puts it into a "memory pool" together with other verified transactions and continues with verification to create a block (every block contains around 200 to 300 transactions). All miners in the network receive all transactions and all miners try to create a block. If a miner finally builds a valid block, he transmits it to the network. Afterwards, each user will verify its validity and add it to the block chain (will be explained in the next subchapter). Once the valid block has been created, miner will be rewarded with newly created bitcoins. Since bitcoin protocol is based on the proof-of-work system, miners have to prove that they have invested a certain amount of computational (processing) power in the process of building a valid block.

Since the total supply of bitcoins is limited, the remuneration for miners will be decreasing over time. In the beginning it was 50 BTC, in spring 2012 this reward decreased to 25, four years later, in 2016, it will be 12.5, etc, always one half of the current reward after reaching the amount of 210.000 blocks, which is approximately every 4 years. These bitcoins created by "mining" are the new ones and the process of obtaining them is described to be similar as mining gold. Bitcoin mining is basically a search for "algorithmic precious metal" and monetizing it into a usable token (Roio, 2013). New bitcoins that were created "out of thin air" are transferred to the miner, which is called a "coinbase" transaction. These mined bitcoins are part of the total supply, which haven't been "discovered" before. In the beginning it was assumed, that the last bitcoin will be mined around year 2140, but many users say that nowadays it takes less than 10 minutes on average to create a block and therefore they suppose that the last bitcoin will be created earlier. However, the problems to be solved are getting more and more difficult, and also the algorithm is set in a way that difficulty of problems adjusts so that the average solving time stays at 10 minutes (Nakamoto, 2008). On the other hand, miners' processing powers are increasing, and therefore they could eventually continue with the trend of lower average times. Still, increased computer power requires higher costs and therefore the question is whether this whole system is sustainable and whether the reward remains so attractive that miners will keep verifying. Different question is, whether miners mine because of the reward or because of fun or their other personal reasons. What is clear is that increased demand for bitcoins will also increase the incentive to mine. On

the other hand the fixed supply means that miners who maintain the functioning of confirmation of Bitcoin transactions will lose their reward and thus the incentive to confirm transactions will decrease. This could lead to the collapse of the system, since it will be too costly to maintain along with no real reward. But still, it is uncertain if Bitcoin survives until the last BTC is mined.

Mining requires one other application – Bitcoin miner, which connects to the network and right after that it starts confirming transactions. "Computer power" that is usually used is CPU[22]. Disadvantage is a huge cost, because computer consumes more money for these operations than it can actually earn (Jiricek, 2012). In 2011, Mira Luna posted a blog article, with a quick analysis of costs of electricity versus BTC reward. We can clearly see that by the time of writing the article, the electricity used by computer was more expensive than the value of Bitcoins that one could get for mining. *"It does not matter how efficient your processors are – you are spending more money to make money"* (Luna, 2011). Even though the value of BTC has risen dramatically since, the reward decreased and the amount of computer power needed is increasing, seeing that algorithms to solve are getting more and more difficult with every new mined bitcoin. And here we come again to the similar question, if the system is sustainable.

3.1.3 Blocks and block chain

From the internal technical point of view, the whole Bitcoin network relies on a shared public ledger called the block chain. Block chain is a database of addresses and the amounts that each address holds. Therefore each block is basically a set of updates of the balances. Each block refers to the previous block, linking back to the starting point (so called Genesis Block) of the whole Bitcoin network and together they all create a block chain (Piasecki, 2012). Block chain includes all the ever processed and confirmed transactions, which allows users' computers to verify and validate each transaction. Transactions are protected with digital signatures to be authentic and these digital signatures provide users with the full control over their Bitcoin accounts and the amounts sent from their own Bitcoin addresses. Since all the transactions are incorporated in the block chain, Bitcoin wallets can calculate the spendable balance.

[22] Central processing unit – hardware within a computer that performs arithmetical and logical operations of the system (Wikipedia, Central processing unit, 2014)

Approximately every 10 minutes, a “block” of accepted transactions is recorded to the block chain and consequently published to the network. This way, Bitcoin software registers when bitcoins have been spent and prevents the double-spending in the Bitcoin’s peer-to-peer system. Therefore for this issue, obviously no central authority is needed.

3.1.4 Bitcoin exchanges

Bitcoin exchanges channel willing sellers and buyers, which often means that those who trade on Bitcoin exchanges are seeking some future return dependent on actions of other users. Bitcoin exchanges have a virtual trading floor and operate in a way comparable to currency exchanges. They usually work as non-profit entities and are registered to non US subjects. As non-profit exchanges they are trying to evade the registration requirements, though they should anyway comply with anti-fraud requirements.

Some Bitcoin exchanges have shown their willingness to cooperate on the application of laws. For example in 2012 French authorities have given a licence to the Bitcoin-Central exchange, which allows them to operate much like a bank (Dion, 2014). Bitcoin-Central is therefore the first licensed exchange that will run within the framework of European legislation and regulation (Santos, 2012).

3.2 Historical prices and volumes

3.2.1 Data set

Available quantitative information and statistics is generally provided by some scheme owner. Data for Bitcoin market prices in USD and volumes were taken from blockchain.info, where complete price history is available either in JSON or CSV format, which was used to produce graphs in current section.

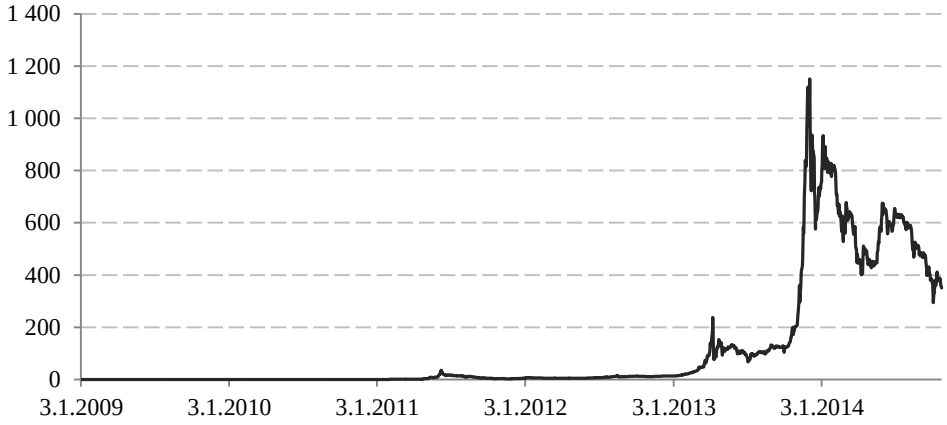

Figure 1: All time Bitcoin prices (in USD)

3.2.2 What drives the value of Bitcoin

In theoretical terms, it is necessary to explain, how prices of money in general (or media of exchange) are created and how money obtains the inherent value. Ludwig von Mises (1953) answers this question in his regression theorem. It states: *"Before an economic good begins to function as money it must already possess exchange-value based on some other cause than its monetary function"* (Mises, 1953, p. 111). What it says is that the value of money is derived from the tomorrow's similar expected value and also from yesterday's value. Since people expect the money's purchasing power, they are willing to give up goods today, but they keep the money for tomorrow's usage. Price of money is a purchasing power of a monetary unit, thus the exchange value of money, determined by supply and demand of money (Rothbard M. N., 1962). Based on this theorem, the value of money can be traced backwards until the point where money originated from the basic barter. However Bitcoin seems to violate the theorem, since the origin of its value is not traceable[23]. Bitcoin seems to have accumulated some demand earlier than it has reached value higher than zero. Reasons for this demand may vary - it might have been convenience, pure interest, Bitcoin's perceived advantageous components or its liquidity.

In real terms, price of bitcoin is set by supply and demand, thus the value is a result of what people actually assign to bitcoin. Therefore its price can change rapidly in relatively short time frames. From the price evolution we can clearly see that Bitcoin prices fluctuated

[23] Violation of the regression theorem by Bitcoin and its effect on Bitcoin perceived as money by Austrian School is one of the fields for possible further study. One possibility would be the reformation of the theorem in a way that it could encompass up-to-date types of money with technical and IT advances, such as Bitcoin has.

dramatically. Since there is only a small amount of coins available and relatively few transactions, price can change significantly after some few hundred trades (Dion, 2014). Bitcoin prices are too "event-sensitive" and rapid fluctuation could be associated with different things, for example increased media attention (Serwer A., Liebelson D., 2013). Events that could drive the price up include investor speculation, announcement of reasonable regulation, increasing adoption of Bitcoin by various merchants, financial crises, various banks' support, etc. On the other hand announcement of strict regulation, too many illegal activities, attacks on exchanges, liquidity issues, Bitcoin protocol problems, evolution of superior currencies, etc. could drive the price down.

For example in late 2013 first congressional hearing took place, where US officials suggested that Bitcoin could be a legitimate source of money, instead of only criticizing it as a source of illegal business. As a response to the Senate hearing, Ben Bernanke said in a letter that *"(virtual currencies)… may hold long-term promise, particularly if the innovations promote a faster, more secure, and more efficient payment system"* (Gilpin, 2014). Besides, Mythili Raman, assistant attorney general for the U.S. Department of Justice's criminal division, said that *"The Department of Justice recognizes that many virtual currency systems offer legitimate financial services and have the potential to promote more efficient global commerce"* (Chaffin, 2013). As a result, prices jumped almost instantly after the hearing and its rather positive comments.

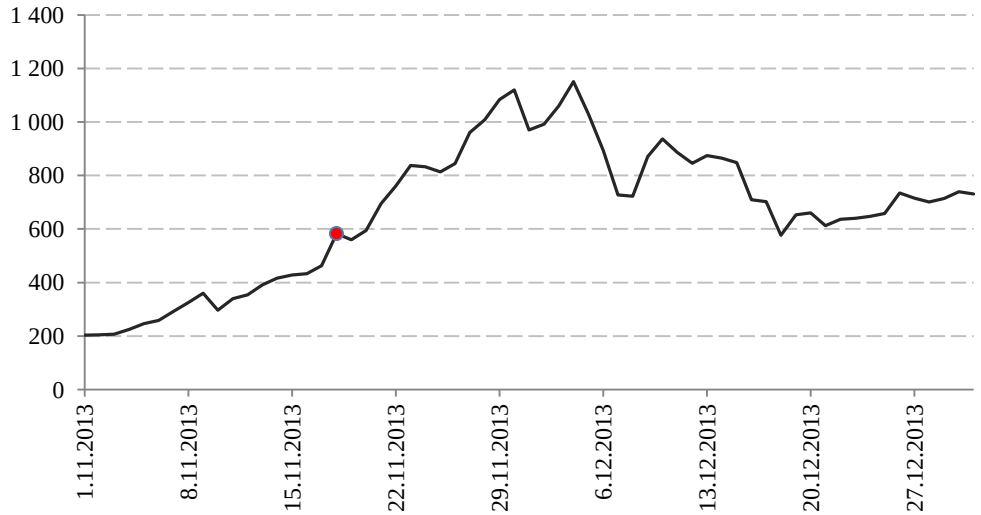

Figure 2: US Senate hearing on 18.11.2013

Even though events do influence prices in the short-term, they do not determine the market direction in the long-run. The overall trend in Bitcoin prices is of increasing nature and many suggest that prices will constantly go up while gradually stabilizing in terms of volatility.

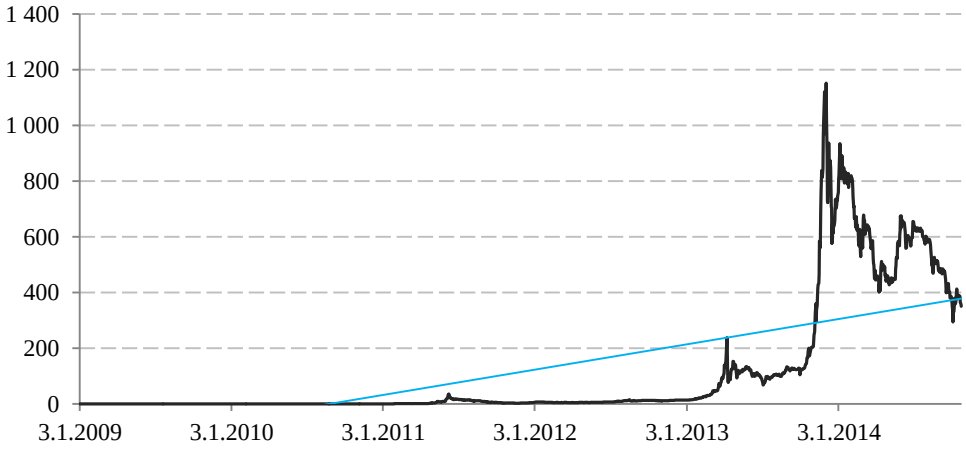

Figure 3: All time Bitcoin increasing trend

3.2.3 Historical volumes

The data that can be found are showing the total output volume, which shows the total value of all transactions per day. However this data include coins that were returned to the sender. Reasons for sending coins back may for example include transactions that have not been accepted or verified due to a double-spending threat. Source of the data, blockchain.info provides also some estimated transaction volumes where they created an algorithm to eliminate returned transactions. The estimated transaction volume is supposed to be an accurate reflection of real transaction volume, because these numbers represent the volume with added algorithm that removes change from the total value. Unfortunately, the algorithm is not described in more detail, but for the comparison it is shown together with total output volumes in a figure 5. However we cannot asses how relevant the estimated volume is.

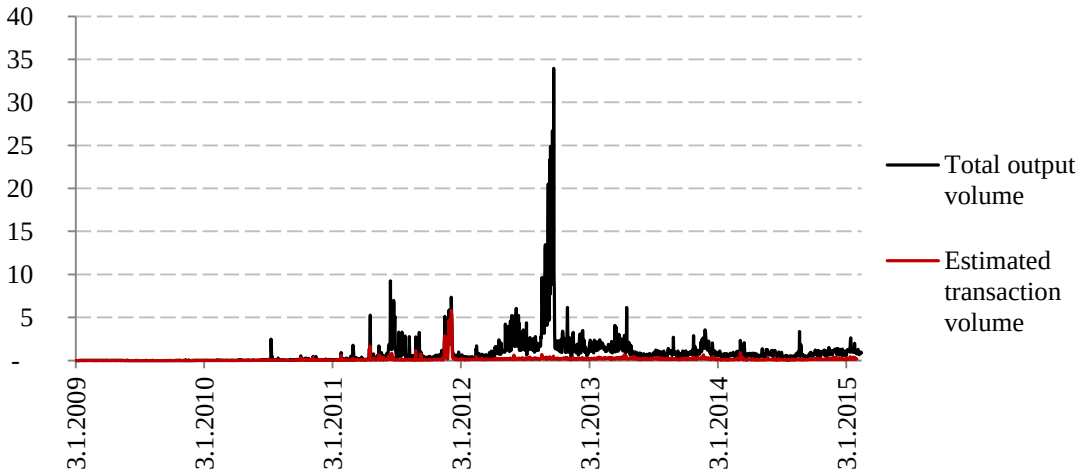

Figure 4: Total output volume and estimated transaction volumes in millions

Estimated transaction volumes are ranging between 0 and 6mn. Total output volumes are ranging between 0 and 10mn, with the exception of one month between the end of August 2012 and end of September 2012. Since Bitcoin is highly event-sensitive, one of the reasons for this increased interest could have been the 2nd Bitcoin conference that took place in London on 15-16 September 2012.

As of end of November 2014, more than 13,5 millions of bitcoins were in circulation and the amount of newly mined bitcoins grows linearly. Predictions of final date when the last bitcoin will be discovered are rather mixed, but it is quite difficult to estimate precisely. Mining becomes more difficult and the reward for mining keeps decreasing. But since the total volume in circulation is growing linearly, the originally predicted year 2140 is probably not realistic. Nowadays much earlier date is expected.

Number of unique transactions in bitcoins per day is also growing constantly, which could be again interpreted as an increased interest of its users. Total number of transactions is also growing linearly.

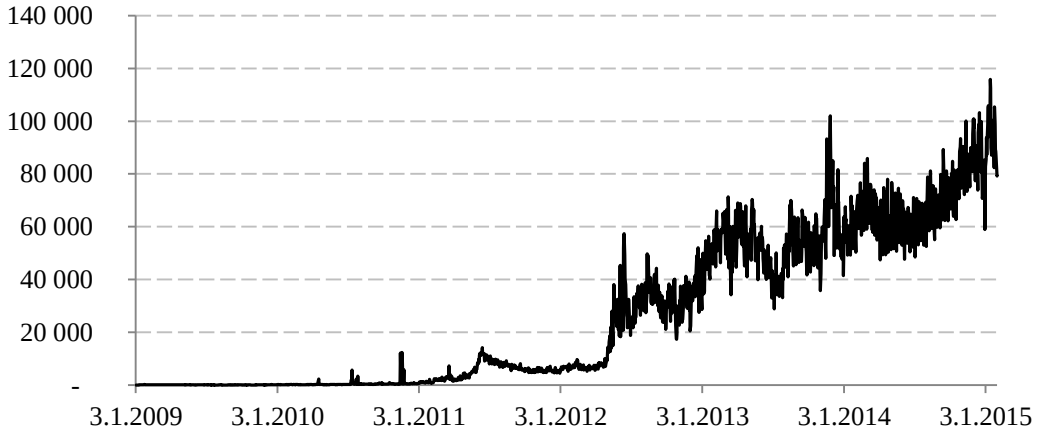

Figure 5: Number of transactions per day

3.2.4 Volatility

What we can clearly see from the historical data is that prices and volumes are pretty volatile. Since 2011 there have been several significant price adjustments, which led many people to say that Bitcoin is just another speculative bubble.

Yearly price and volume volatilities were calculated by using a variance or a standard deviation calculated from logarithmical price and volume change. Afterwards, volatilities were annualized by days in a year, 365 (data available for each calendar day), by multiplying the standard deviation with square root of 365. Even though there were some bitcoin volumes basically already from the beginning, we can identify first non-zero prices only since 17.08.2010. Since from the mathematical point of view, division by zero is not defined, the first price change is available for 18.08.2010. Calculated standard deviation of prices for the period from 18.08.2010 to 14.02.2015 is 7,47% and annualized price volatility is 147,81%. Calculated standard deviation of volumes for the same period is 48,91% and annualized volume volatility is 934,38%.

To see the development of volatilities, annualized yearly volatility was calculated for each consecutive day since 17.08.2011 (the first date with full year-long history of both price and volume changes) until 14.02.2015. On the left primary axis of the following figure 7, we can see price volatilities and on the right secondary axis, volume volatilities.

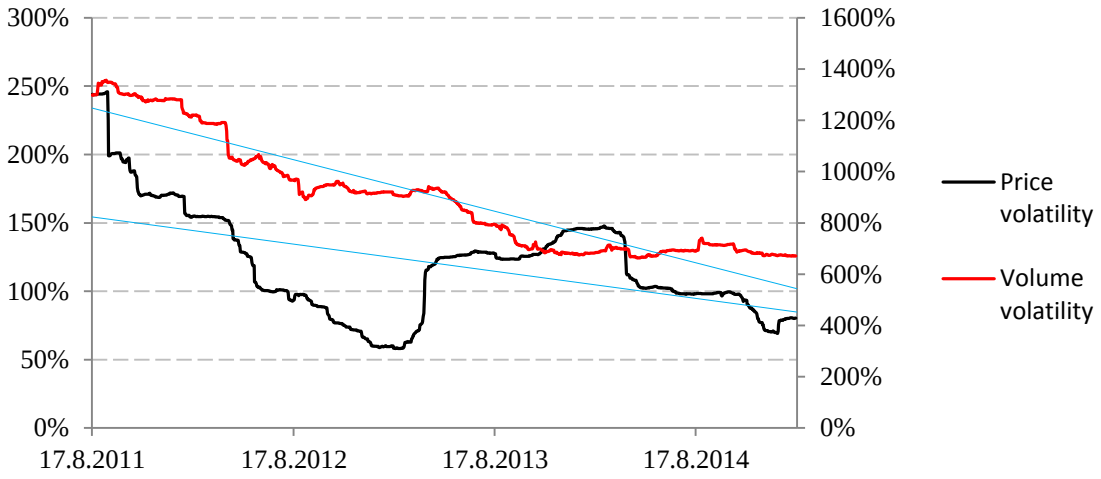

Figure 6: Evolution of annualized yearly price and volume volatilities

Clearly, the volatility of both prices and volumes is pretty high. High price volatility confirms how risky bitcoin investments are, while extremely high volume volatility confirms again that bitcoin has problems with low liquidity, which is described in next subchapter. Figure 7 also shows the decreasing trend of both price and volume volatilities, which rather supports the opinion of Bitcoin proponents, that Bitcoin volatilities are going to decrease in the future and that prices and volumes are going to stabilize. Nevertheless, Bitcoin volatilities are still extreme and Bitcoin still cannot be considered as an optimal investment option.

If bitcoin should be used as a store of value, its volatility could be a huge danger. It is not reasonable to keep money in bitcoins, when it is such unpredictable and volatile. However, if bitcoin should be used as a medium of exchange, its volatility wouldn't be so problematic. Goods and services can be priced in bitcoins, but in terms of traditional currencies. Thus the bitcoin price would adjust accordingly. This is also the way how most of the retailers who accept Bitcoin as a form of payment think and therefore they usually immediately sell it (Baverman, 2014). Customers often use bitcoins due to its lower transaction costs and they do not care that much about the tomorrow's exchange rate. We can see that the popularity of bitcoins among both customers and merchants is growing in terms of medium of exchange, in spite of the high volatility (Brito, J., Castillo, A., 2013).

There is a possibility that Bitcoin will become less volatile in the future, once more people start using bitcoins, understand the technology and assess its value more realistically. Proponents argue that the actual price decrease is a good sign, because Bitcoin is finally

getting to more realistic price. This could be caused by either fewer speculators, growing use of Bitcoin as a currency without exchanging it instantly for traditional currencies, or a mix of both. And as a result, this might be the first step in the Bitcoin's story as a "real currency".

3.2.5 Liquidity

One of the biggest Bitcoin's problems is its liquidity. From the past evidence, we can detect several market failures, which hurt Bitcoin and many sceptics are concerned about its limited liquidity. Bitcoin does not have any market makers who would hold bitcoins and thus ensure the liquidity for its users. Bitcoin exchanges should execute this, but in reality they do only to a small extent.

For now, Bitcoin market is rather illiquid due to relatively low trading volumes and because it still *"…relies on others wanting to join the scheme"* (ECB, 2012, p. 39). This could result in a situation when users are holding bitcoins but no one else is willing to buy them.

From the other point of view, Bitcoin provided liquidity in areas where it is difficult to get cash. One example is in Iran, where many people have used Bitcoin, due to the lack of local currency (Dion, 2014). In the future, Bitcoin could eventually serve as a form of payment in developing countries.

3.3 Legal issues and Regulation

Up to this date, Bitcoin still operates in a legally grey area and there have been only a few actions taken against Bitcoin[24]. Anyway, neither any ultimate conclusions have been reached nor there is any final legislation that would handle virtual currencies. As already mentioned in subchapter 2.2, nowadays we do not have any legislation supporting private currencies. There are no frameworks under which private currencies could operate de jure. There is always one official (national or supranational) currency and even though local private currencies may exist and they are neither prohibited nor illegal, they are not yet supported in legislation and users of the currency have only the owner of the scheme to address themselves to. People use the currency based upon their trust either in the owner or the currency itself. The case of

[24] For example in 2011 Mt.Gox had to close their French bank account. Bank said that Bitcoin is electronic money and because a company that was representing Mt. Gox in France was not a bank, it was illegal that the company was handling Bitcoins.

Bitcoin is however different - the owner of the scheme is unknown and yet (some) people seem to trust it anyway.

From the enforcement perspective, it would be impossible to track the "responsible" person, or a victim in case of some conviction, since it is not clear who is the "issuer" of Bitcoin. The best candidate is Satoshi Nakamoto, however it is highly probable that this is just a pseudonym and still the identity of person(s) is not known. And from the nature of Bitcoin, it is also clear that it would be very difficult to either freeze the Bitcoin accounts or physically shut down the whole "Bitcoin system", since it does not have any central authority and it is anonymous. But if some future regulations were really strict, it might prevent or significantly limit the usage of bitcoins. And if Bitcoin was frequently used for illegal business, it could itself discourage many people, who do not want to use currency associated with criminality, from using it. Bitcoin could eventually ruin itself either by above mentioned possible reasons, some negative events or general loss of trust, leading to highly decreased demand.

If people do not completely lose trust in Bitcoin, many questions arise regarding regulation of Bitcoin and other virtual currencies. One of the first and probably the most important question is, whether Bitcoin can become so significant, that the economists and governments would feel the necessity to legally handle the case. It is impossible to answer this question at this point, but we can expect the continuing growth of virtual currencies. There are various reasons why this trend could continue: electronic commerce is growing, which is ideal for virtual currencies; people start valuing more their anonymity in money transactions; transaction costs and times are lower when using virtual currencies and also the trend of technological innovation and growing access to the internet is unstoppable. In the same time, there are people who start mistrusting fiat currencies, which may also be a reason for trying to use the virtual ones.

It is almost certain, that some legal actions will be taken only if Bitcoin should threaten current monetary system or the illegal usage would increase too rapidly. But if Bitcoin won't threaten traditional currencies, we can also ask why any policymakers should invest their resources for any regulation at all. Many suggest that Bitcoin does not necessarily need to be regulated, however some legal framework for consumer protection might be developed in the future. On the other hand, there is an argument that usage of Bitcoins is completely voluntary, thus people enter the scheme on a basis of their own trust and with knowledge that the system does not have any legal support or protection.

Second question, assuming that virtual currencies will reach a significant mass or attention, under which category and regime should it be regulated? As already mentioned in subchapter 2.3.4, it is really difficult to put bitcoin into one particular category. It fulfills some characteristics of each, however cannot be defined as any with complete certainty. Therefore it is likely that bitcoin will have to be regulated by several policymakers. There is no current legislation that could cover Bitcoin in its all aspects. Bitcoin together with other virtual currencies is a new concept, which requires new definitions and should be handled separately from money, traditional currencies, securities or commodities. If it should be regulated effectively, some new category likely needs to be generated. Third question is related to the physical regulation. Bitcoin is a virtual currency with global coverage and therefore it is questionable whether it is possible to regulate Bitcoin on a global level. However, some international approach will be rather necessary because of Bitcoin's global nature. Even if some regulation will be implemented in some countries, the risk for global financial crimes won't be reduced in remaining countries (Hollingshead, 2014). But it is too early to speak about global regulation, when legal issues are not solved even locally. Nevertheless global regulation will be an important issue to discuss, once the final decision to regulate Bitcoin is made.

One of the biggest challenges would be to create a regulatory scheme that would reduce concerns, minimize negative consequences, prevent customers and prevent the illegal use of bitcoins without harming its beneficial uses. As mentioned earlier, it would be impossible to shut down Bitcoin, but neither making it completely illegal would ruin the whole network. Passionate users would continue, since many of them would probably not play according to regulation rules, criminal use would not drop, but they will only do it under the illegal tag. It is not possible to regulate just a little bit, but regulators are still not even unified about exact Bitcoin definition, so that they could regulate it properly all at once. But if Bitcoin was completely prohibited, governments would lose the opportunity to effectively regulate it and criminals would be even more encouraged to use it.

3.3.1 Reasons to regulate Bitcoin

Proponents of Bitcoin claim, that one of the essential reasons, why there are different initiatives to fight and regulate Bitcoin, is that governments want to prevent the competition with the existing monopoly on money and related products. They say that most concerns come mainly from various banking institutions, credit card institutions and central banks.

Extreme views go even further. It is too far from Bitcoin reality and its spread but some say that officials fear the harm to the value of traditional currencies and monetary policies, due to new potential competition to legal tenders, thus it is necessary to do all the possible to prevent it. This fear of competition reminds of the discussion from subchapter 2.2 where free banking proponents support the allowance of private currencies. They propose competition in currencies where only such currencies would exist, which fulfill the needs of their clients. Bitcoin obviously fulfills these needs but it is questionable for how long and if enough customers will be attracted by this innovation that is not backed by any valuable commodity. But still Bitcoin does not seem to intend to compete with traditional public currencies.

Another reason is said to be the legitimization of Bitcoin in terms of currency. This is however quite cumbersome, because Bitcoin has already been widely used as a currency. Those currently active users do not need governments to officially claim that Bitcoin is a currency. Besides legitimization there are various reasons why are officials concerned with Bitcoin. These concerns include for example the usage for illegal purposes, threat to price stability or anonymity and transparency. And besides policymakers concerns, customer or user protection might also be a case for some legal guidance.

3.3.1.1 Black market usage, illegal payment processing and money laundering

There are maybe too many ways how people can and how people really do spend their bitcoins. Since Bitcoin is quasi-anonymous, people used the opportunity to conduct illegal transactions with bitcoins. It easily allows for anonymous donations and anonymous business administration and facilitates money laundering or tax evasion (Grinberg, 2011). In connection with anonymous and hidden online market Silk Road[25], bitcoins could have been spent for drugs, child pornography or even assassinations. Argument pro Bitcoin is that all the above mentioned can be and also is done by cash, which is even more difficult to trace. Bitcoin is anonymous, but it is not completely impossible to match the transactions with a real person. Even if there is no open list of individuals attached to account numbers, it is still possible to trace the identity. It is possible to start the initiative with the intention to create a database of such accounts, which might lead to better identification of people conducting illegal business with bitcoins.

[25] Silk Road was an underground auction market founded in 2011. More than 10,000 products were for sale in 2013, where 70% were drugs. Estimated volume of transactions was $ 15mn annually, but some people suggested that it might be even twice as much. In October 2013, Silk Road was shut down by FBI, but four days later, Silk Road 2.0 was again online.

"In May 2012 an FBI report on Bitcoin was leaked to the Internet…" (Piasecki, 2012). Report included the assessment of likely illegal activities in connection with Bitcoin. It mentioned probability that Bitcoin will become a cyber-criminals' medium of payment, possibility of its use for money laundering and potential theft of bitcoins from third party services and private users. In the United States, there was a case when two senators wanted to take down Silk Road, because it enabled users to conduct illegal business with bitcoins. Even though there was no official response to this particular desire, Silk Road was shut down by FBI in October 2013.

One of the main reasons, why authorities want to regulate Bitcoin, is the illegal business, which is done by using bitcoins. But even with regulation, this is exactly the area that likely would not be affected by any regulation. If there is any reason why Bitcoin would survive all the strong regulations, it is especially the illegal business.

3.3.1.2 Price stability

Governments and policymakers identified another potential risk of virtual currencies that might be a reason for some regulation. Innovative payment systems might impact the price stability and monetary policies. Price stability could be in particular affected if virtual currencies regularly modify the quantity of money or interact significantly with the real economy (ECB, 2012).

Even though this is highly improbable, but in the extreme situation, if virtual currencies became widely accepted, central bank money usage could decrease. This would lead to a decreased ability of central banks to control short-term interest rates and as a consequence threaten the price stability.

For now virtual currencies do not pose any real threat to price stability, however volumes of virtual currencies and their interaction with real economy should be monitored.

3.3.1.3 Anonymity and transparency

Next concern regarding Bitcoin is its (quasi-) anonymity. One of the Bitcoin's features is that transactions are highly anonymous. Users can send and receive bitcoins with high level of privacy, but there is a public database of all transactions. However it does not link any

transaction to an individual, if he does not reveal his private key. On the other hand, when using any exchange, user has to reveal some information.

Most concerns result from the fact that anonymous transactions can be used for illegal purposes. But this worry is rather not in place, because Bitcoin can never be as anonymous as cash. And since there is a public database available, with some effort this database could be stepwise transformed into the more personalized list of transactions.

Transparent policy usually leads to higher confidence and could strengthen the currency. Proponents of Bitcoin argue that Bitcoin is perfectly transparent because all the information is available in the block chain and everyone can anytime verify it.

Therefore possible regulation should not concentrate on Bitcoin's anonymity or transparency but rather impose some reporting requirements.

3.3.2 Current legal and regulatory issues of Bitcoins

This part will be divided into several subchapters, starting with regulations of Bitcoin according to the category to which it could belong and continuing with different bodies that could regulate Bitcoin with some of its current laws.

3.3.2.1 Money and Currency

When regulating Bitcoin as currency, first question appears. Is private currency even legal? European Union hasn't declared private or electronic currencies illegal. Some suggest that in EU Bitcoin could fulfill the definition of electronic money within Electronic Money Directive[26], while others argue that Bitcoin should rather fall within the Payment Services Directive[27] (European Parliament and Council, 2007). For example Finnish Central Bank declared that digital currencies are not illegal and consequently many businesses have started accepting bitcoins. However, Finland has already launched instructions for the taxation of virtual currencies. *"When transferred to another currency, the rules on taxation of capital*

[26] Electronic money is defined as: "*...electronically stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer."* (European Parliament and Council, 2009). Bitcoin is an electronic storage and is accepted as a means of payment however is not issued upon receipt of funds.

[27] Payment Services Directive defines rules associated with execution of payments via electronic money, but does not regulate their issuance.

gains apply." (The Law Library of Congress, 2014, p. 9). When bitcoins are used to buy goods and services, it is treated as a trade, and it is taxable if the value increases over the price at which it was bought (Hills, 2014).

Under US laws, private currencies are also legal. American constitution prohibits the coining money, private money cannot resemble US money, but private currencies are not forbidden (Brito, J., Castillo, A., 2013). Therefore we can conclude that *"…private currencies are not per se illegal"* (Dion, 2014, p. 190).

If Bitcoin was defined as a currency, in the United States it might be regulated according to Stamp Payments Act under some circumstances. The main purpose of this Act is to outlaw those currencies that threaten the circulation of U.S. coins. Nonetheless those currencies that are exchangeable only for goods are not threatening. It is questionable whether this Act could be even applied on Bitcoin. On one other hand, Bitcoin obviously violates the Stamp Payments Act in some aspects (as mentioned in footnote 6). First of all, Bitcoin transactions are very often worth less than $1. Secondly, Bitcoin seems to intend to compete with other traditional currencies. Others argue that bitcoin is not competing with U.S. coins as much as it is competing with for example PayPal. Another example is the opinion of Grinberg (2011), who concludes from the evidence of different cases throughout the history: *"…The Act is unlikely to apply to anything that (1) circulates in a limited area. (2) is redeemable only in goods, (3) does not resemble official U.S. currency and is otherwise unlikely to compete with small-denominations of U.S. currency, or (4) is a commercial check…"* (Grinberg, 2011, p. 185). However, since the Stamp Payment Act is a 150 years old statue, it would need some more current interpretation and possibly some amendment, which would be better applicable on digital currencies. We can conclude that in case of publication of some actual court opinion and update of interpretation from 1899, this Act indeed might cause some troubles for virtual currencies.

Another legal framework that could be applied to regulate Bitcoin is the counterfeiting prohibition. In the United States there is a set of laws, which prohibit copying and imitating (i.e. even original designs) of U.S. legal tender[28]. Even original designs could confuse consumers and can compete with the official U.S. currency.

[28] Legal tender is defined as any official medium of exchange that is recognized by law or by a legal system to be a valid medium for meeting financial obligations. The national currency is classified as a legal tender in basically every country and

In August, 2013, US federal judge decided that for means of securities regulation, Bitcoin will be defined as money. Almost in the same time, in Germany, Bitcoin was acknowledged as a legal form of tender (Marian, 2013).

3.3.2.2 Commodity

Bitcoins fulfill some characteristics of commodity and for example the economist George Selgin defined bitcoin as "synthetic-commodity money" (Selgin, Synthetic Commodity Money, 2013). In the US, Commodity Futures Trading Commission (CFTC) is in charge to regulate commodity futures, markets where they are traded, some foreign-exchange instruments, etc. (U.S.Code, Commodity Exchange Act, amended in 2001). Bitcoin would fall outside the definition of foreign-exchange instrument, since it is not a currency of any government. But it would fall within the definition of commodity as mentioned in subchapter 2.3.4.4. Thus, bitcoins in terms of commodity futures could fall under the jurisdiction of CFTC in the United States. However, exchange of bitcoins for other traditional currencies usually occur right away and not as a futures contract. Therefore regulation of Bitcoin in terms of commodities could be limited also for CFTC.

3.3.2.3 Security

Next already existing jurisdiction that could be applied on the case of Bitcoin is the Securities Exchange Act. Even though Bitcoin cannot be certainly defined as security, thus cannot be regulated with securities laws, Bitcoin exchanges could indeed fall within the reach of these laws. When bitcoins are traded for other traditional currencies, engaged exchanges might be trading securities and therefore fall under the authority of Securities and Exchange Commission (SEC) (Dion, 2014). Act applies primarily to notes, stocks, investments and commodities, but can be also applied on investment contracts (SEC, 1933, amended and approved on April 5, 2012). What is important to mention, foreign currencies are excluded. Interpretation of the Act shows that definitions of each instrument are relatively flexible, should not be taken too narrowly and should concentrate on its real-world implications and as well cover instruments that could be discovered in the future (Dion, 2014). Since Bitcoin fulfills number of definitions of securities, under certain circumstances it could be considered

---

can be issued only by the government or the institution authorized to do that. For example U.S. dollar and euro are accepted as legal tender in many other countries outside US and EU.

security. Therefore virtual exchanges could potentially fall within jurisdiction of the SEC and could be reviewed within the Securities Exchange Act.

If it was decided that Bitcoin exchanges shall comply with securities laws, they would need to register with the Securities and Exchange Commission in the first place. Secondly, they would also have to compile various reports, which could provide governments with different data that was absent before and also investors about the real situation in Bitcoin investments. Thirdly, Bitcoin exchanges would be officially *"…liable for instances of fraud"* (Dion, 2014, p. 194). Registration with SEC would definitely lead to higher transaction costs, but this could at least allow them to continue to run.

3.3.2.4 Various authorities across Europe

Some national jurisdictions across EU started taking local approaches about Bitcoin, which differed one from another. For example, in Croatia Bitcoin is not illegal and in some cases, payments in other currencies are allowed. Denmark's Financial Supervisory Authority rejected Bitcoin as a currency and also rejected its regulation. They concluded that it does not belong into any financial services category, but should be considered an electronic service and therefore should be taxable. As already mentioned, the Finnish Tax Authority has released instructions for taxation. In December 2013 the German Federal Financial Supervisory Authority decided that Bitcoin is a legally binding financial instrument that belongs to the category of units of account and is comparable to foreign currencies. Ireland is considering possible taxation. Italy adopted European Directive of 2009 (European Parliament and Council, 2009) and permits the usage of electronic currencies as understood by EU Directive. Netherlands does not see Bitcoin as electronic money because it does not correspond to the Dutch law. The Dutch Central Bank recommended consumers to be cautious, due to various risks. For example in Estonia, France or Greece, there are no specific regulations or laws regarding Bitcoin (The Law Library of Congress, 2014).

3.3.2.5 European Banking Authority (EBA)

In the European Union regulation of payment services and relevant EU directives (i.e. Payment Services Directive (PSD) or Electronic Money Directive (EMD)) fall within the competence of EBA (EBA, 2014). Therefore the EBA started analysing virtual currencies, with the special emphasis on Bitcoin as the most used virtual currency. In December 2013,

EBA released a first opinion on virtual currencies with the main message, which warned that virtual currencies pose various risks, mainly due to missing current regulation (EBA, 2013). In July 2014 EBA released official opinion addressed to EU Council, European Commission and European Parliament (EBA (2), 2014). *"One of the tasks of the EBA is to monitor new and existing financial activities and to adopt guidelines and recommendations with a view to promoting the safety and soundness of markets and convergence of regulatory practice.*" (EBA, EBA Opinion on 'virtual currencies', 2014).

EBA analyzed different benefits (such as lower transaction costs and faster transactions) and more than 70 risks of virtual currencies. They identified risks for different parties involved (i.e. users, non-user market participants, regulatory authorities) and other risks (i.e. risks to financial integrity and risks to payment systems and payment service providers in fiat currencies) (EBA, 2014). Based on this analysis they proposed different possible regulation for the short- and long-term that should be adopted by EU institutions. They highlighted the importance of EU response in order to prevent national regulations, which could differ one from another.

EBA has not proposed any conclusive regulation but rather provided a list of recommendations what next steps could be executed by EU legislators. Since many of risks and possible regulation to prevent those risks need to be analyzed in more detail, for now EBA *"…advises national supervisory authorities to discourage credit institutions, payment institutions and e-money institutions from buying, holding, or selling virtual currencies."* (EBA (2), 2014). Within the European Union, other authorities should be involved in this topic, for example European Central Bank (ECB) or the European Securities and Markets Authority (ESMA), each responsible for regulation within its mandate.

3.3.2.6 Financial Crimes Enforcement Network (FinCEN)

According to different statues (e.g. Bank Secrecy Act[29] and Money Laundering Statute), financial institutions are required to help reducing fraud, money laundering and tax evasion (Dion, 2014). Financial institutions also have to report suspicious activity to the FinCEN. The main mission of FinCEN is *"to safeguard the financial system from illicit use and combat money laundering"* (FinCEN, 2014). Since Bitcoin exchanges are very often used to trade bitcoins for other traditional currencies, they could be defined as currency exchanges and

[29] Financial institutions have to report currency transactions over $10.000

therefore should be a subject to different requirements and laws (e.g. again the Bank Secrecy Act in US). FinCEN has already issued some guidance on virtual currencies, including Bitcoin and imposed the same reporting requirement for Bitcoin regarding money laundering (Bitcoin also has to report currency transactions over $10.000). The last release from January 2014 excludes from the regulation rules both miners who mine currency only for their own purposes and companies that trade virtual currencies only for the company's benefit (FinCEN, 2014). On the other hand, users who *"…pay bitcoins to a third party at the direction of a seller or creditor…"* (Mont, 2014), might be considered money transmitters and therefore be liable to regulation. As well transactions to third party demanded by company's owners or creditors designated to direct payments may be subject to regulation.

It is known that Bitcoin is also often used to pay for illegal transactions and as a mean for money laundering. Assuming it is true, this could also be a reason why Bitcoin could eventually fall under the radar of FinCEN. However, Bitcoin has not started reporting and is probably still too far from doing it, unless it will be forced by some laws.

3.3.3 Conclusion on regulation

From the existing research it is clear that Bitcoin is gradually attracting more institutions to look closer into the case. Some countries have already taken a few local actions to put Bitcoin in some category or rather released some recommendation regarding Bitcoin. We can see that even though concerns about Bitcoin increase and thus officials are trying to analyze the situation, the discussion is still only in the beginning phase, where no final decisions have been made. The biggest problem seems to be that not even institutions like EBA, ECB, FinCEN, SEC, etc. do not really know how to regulate Bitcoin and under which classification. Growing amount of official reports can be understood as a growing interest in the matter, however it is obvious that they are struggling and still cannot take any final actions.

We have seen already several times that Bitcoin does not fully fit into any existing category or legal definition. To conclude this part of the paper, we can return to the second question in subchapter 3.3 regarding legal issues and regulation. Since Bitcoin is not the only virtual currency, it would be definitely appropriate to create a completely new category for virtual currencies all together, including Bitcoin. This should also take into account a unique nature of this innovative technology (technologies). Policymakers all over the globe should afterwards decide which particular regulation should be applied for exchanges, payment

processors, miners and basic users. It is a very difficult task to do, because Bitcoin has different features that haven't been known before, such as its completely decentralized nature and also its global coverage.

First of all, in any case Bitcoin should not be completely outlawed but rather more strictly regulated. On one hand, outlawing could cause a shutdown of some exchanges and abandoning of Bitcoin by many users. However, "anarchist" users will likely remain and will be more encouraged by the official illegality. On the other hand, some effective regulation could result in maximizing Bitcoin's positive aspects and minimizing negative. It could also help governments and different institutions to gain valuable information that has been lacked before. Second of all, effective global regulatory framework is necessary, since the topic of virtual currencies is more alive than ever and it is almost certain that this trend will continue.

3.4 Future scenarios for Bitcoin - Is Bitcoin doomed to failure?

There are different alternatives how the whole "Bitcoin project" could end up. At this stage it is almost impossible to tell with certainty how is Bitcoin going to develop. Many argue that Bitcoin with its "inflation-proof" concept has a high potential and that one day it might become a standard form of exchange. Others suggest that it will fail due to various reasons, or that it will be strictly regulated, such that it will either discourage many people from using or even be banned from use. The most important issue in Bitcoin's future is the general public acceptance.

One of the most probable possibilities is that nothing will actually change compared to today's situation. There will be some enthusiasts, who will continue using it as a form of payment, some rather small companies will be attracted to start accepting bitcoins, but still it won't reach any significant mass. It is highly questionable (perhaps even improbable) if Bitcoin can captivate mainstream. People do not care that much about anonymity when buying clothes online, standard customers do not think of inflation when going grocery shopping, however they usually do care about some security when using their credit cards or PayPal. Therefore, with what we know today, Bitcoin does not seem to have any benefit for common consumer.

Where Bitcoin could offer some perceived benefits in future, is the area of micropayments or in other words very small payments. Low or no transaction fees could attract some people to

use bitcoins rather than some traditional way. Bitcoin is designed in a way that transaction costs are reduced. Usually transaction costs are generated when some third party has to validate transactions. Bitcoin solved this problem with a concept where all the users of the network validate transactions together. Second area would be virtual-gaming world and commerce, where some virtual currencies are already being used (See subchapter 2.3.3). Bitcoin has a potential to penetrate this market and become a *"…de facto standard for certain virtual and game-related currencies"* (Grinberg, 2011, p. 171). Another opportunity area is the field of international transactions and transactions in developing countries, especially countries where it might be difficult to get cash or where it is too costly to send money to via traditional ways.

Manny suggest that Bitcoin is just an irrational bubble, which sooner or later has to lose the confidence. This would lead to lower demand than supply and thus a collapse of the system, where bitcoins' worth is determined only by supply and demand. There are many reasons why Bitcoin might collapse: unexpected changes in the inflation rate (Grinberg, 2011), evolution of superior alternative currencies, technical problems, such as failure of anonymity or thefts or loss of Bitcoins. Possible regulations or constant hacking problems might also harm the usage and confidence of Bitcoins. One of the strong arguments against Bitcoin is its deflationary nature, which may even lead to deflationary spiral. Another important issue is the legally grey area where Bitcoin currently operates. As already mentioned, people themselves might not want to use currency, which would be associated with illegal businesses. Even without any real regulation, bitcoins could still be "labelled illegal", which could drive away many potential users.

From the future regulation perspective, it is improbable that we will see any significant regulation in the near future, even though the topic has already attracted attention of several institutions and regulators. To agree a final and globally-reaching form of regulation will be a very challenging and lengthy process. From the growing amount of official analyses we can deduce some intentions to regulate or create a legal framework for Bitcoin and other virtual currencies, but even authors themselves conclude that it will take a lot of effort and time to find some efficient design of regulation. If Bitcoin reached higher transaction volumes and bigger threats for global economy, this process might quicken. But in current situation when Bitcoin does not pose any immediate threat, there is no real pressure to take any impulsive and hasty decisions. And the possibility that it even won't be necessary to regulate is also still present.

However, even if it won't be necessary to regulate Bitcoin or if Bitcoin itself fails, the whole idea together with the need for alternative or digital currencies will probably outlast. There are some attributes of Bitcoin that could be improved or rebuilt from scratch, but in the future, Bitcoin might serve as a reference for some new digital or crypto-currencies. Needless to say, Bitcoin has at least brought the attention of wider audience, showed that one may dare to invent a different form of currency and payment and that it might actually work. Therefore it is indeed inevitable to prepare some future regulative or legislative framework for virtual or crypto-currencies, because it is almost certain that this area is going to develop further.

3.4.1 Evolution of other virtual currencies - Possibilities to replace Bitcoin

Even if Bitcoin is a "first-mover" (at least in terms of being the first virtual currency that has been accepted more widely and attracted the most attention), it is not the only one. There exist some other virtual currencies and it is highly probable that some more will develop in the future. It is also possible that Bitcoin will be replaced by another crypto-currency with some better features.

Most of the protagonists of Bitcoin value in particular its technological aspects. However Bitcoin is supposed to have some flaws that could be fixed – confirmation time could be quicker or mining process could be more effective. Another problem is the consumption of electricity, as mentioned in subchapter 3.1.2. The more computing power leads to higher bitcoin earnings and therefore miners spend more and more money on hardware, which consumes even more electricity. Some Bitcoin alternatives started using different principle, namely "proof-of-stake"[30] instead of "proof-of-work". Since the introduction of Bitcoin, many people tried to propose some amendments or improvements and some even tried to run their own new alternative currency. It is said that to change the core Bitcoin protocol would be really difficult; mainly due to its decentralization. Therefore the option of own virtual currency is often easier than to find support for some Bitcoin improvements within the Bitcoin community. Since Bitcoin is an open-source project, anyone can get its source code and anyone can modify it and start their own new network with similar software.

[30] In this alternative principle, miners who own the most virtual cash, also earn the most, which decreases motives for spending more money on hardware (Lee, 2013).

3.4.2 Crypto-currency alternatives to Bitcoin

Bitcoin's first competitor – Litecoin, promotes, that transactions are confirmed faster, volumes can be bigger and storage efficiency is improved. Litecoin is also a decentralized P2P virtual crypto-currency with almost zero transaction costs. Within the mining process, basically everything valid for Bitcoin is also valid for Litecoin. The only difference is that Litecoin is not that wide-spread and the mining configuration is more difficult than in the Bitcoin system. The advantage compared to Bitcoin is that with more simple "computer power" and lower amount of energy used for mining, miner is able to get higher remuneration (in a month one can mine up to 60LTC whereas on average only 1BTC – in terms of U.S. Dollars, on June 1st, 2014 1BTC ~ $460 and 60LTC ~ $600). However the price of Litecoin keeps decreasing. But since mining of Litecoin is easier and price is expected to rise (similarly as Bitcoin prices have risen), within the virtual currencies community it is suggested that mining of Litecoin is going to repay more in the longer-term perspective.

Dogecoin's creator, Billy Markus from Oregon, has the intention to grasp broader demographic than Bitcoin (Gilpin, 2014). This currency initially started as an internet joke and now its market cap is growing fast and it is the most traded virtual currency. Dogecoins are mined in bigger amounts than bitcoins – by March 2014 more than 65 billion have been in circulation. Therefore it is valued much less than other virtual currencies – 1.000 dogecoins were worth around $0,40 in the beginning of June 2014. Dogecoin is best known for its system of granting tips over the internet – users tip other users for interesting or useful information. Additionally, the dogecoin community raised funds for various sportsmen, for example Jamaican bobsled team or a NASCAR driver. Even though Dogecoin wins in the field of the most traded crypto-currencies, it is very unlikely that it could ever be the most valuable one (dogecoin.com, 2013).

Peercoin is said to be more environmentally sustainable compared to other virtual currencies, due to its lower use of energy. It uses the proof-of-stake to maintain its network. Users verify transactions and secure the network based on the peercoins they hold. Therefore no massive power houses are needed to verify transactions. It tries to be the most secure peer-to-peer network, where all computers can participate equally. Users receive 1% annual reward as a compensation for maintaining the network, which results in a fair distribution. Peercoin states that it has a built-in 1% inflation rate (peercoin.net, 2012).

Namecoin is a virtual currency based on Bitcoin. It is a decentralized open source system and equally as Bitcoin uses the proof-of-work algorithm and also has the limited supply of 21 million NMC coins. The main difference is the possibility of storing the data within the blockchain. It is the first virtual currency that acts as a decentralized domain name system, so that user can register domains with it (.bit websites). It is much cheaper to register and it is said to be the perfect backup for existing .com websites. When a user registers the domain, it is resistant to being highjacked or shut down. Namecoin is trying to explore the record-keeping within the virtual currency (namecoin.info, 2011).

There are many more virtual currencies, for example Primecoin, Ripple, Quark, Freicoin, Mastercoin, etc. Most of them have some attributes in common. They are decentralized, open source, with limited supply and operate on a P2P network. They usually differentiate only slightly from Bitcoin. Generally, they were created with the intention to be superior at least in one aspect than Bitcoin. Some alternative currencies were created for the purpose of being direct competitors to Bitcoin, others wanted to provide an alternative that would not be associated with Silk Road marketplace or other criminal use. The biggest Bitcoin advantage compared to its competitors is the "first mover" position. Because Bitcoin was the first more widely accepted virtual currency, it has the biggest publicity, it is the most supported by various start-ups, it is the most accepted and the most users have actually invested in it. And since none of the improvements or alternatives to Bitcoin was persuasive enough and at the same time Bitcoin keeps fulfilling the needs of its users, it seems that Bitcoin has a good chance at remaining the most popular alternative or virtual currency.

However it is probable that the future will bring some new alternative virtual currencies that will be superior in significant amount of aspects, such that they will provide more benefits than any other currently existing virtual currency and people will start moving towards these new ones. It is also possible that Bitcoin as we know it today won't exist anymore, so it would be easier for competitors to develop and attract more users. But what is clear, is that it is very likely that the need for some alternative in payment or money transfer systems will remain.

4. Conclusion

A lot has changed in the Bitcoin story since January 2014, when I started following Bitcoin. Bitcoin reached its maximum price on 4th December 2013 – 1BTC was worth 1.151 U.S. dollars. Since then bitcoin price has been constantly decreasing and nowadays its price lies somewhere around $250 for 1BTC. However when we take into the account the whole price evolution, the trend is obviously increasing. Bitcoin is still in its beginning phase and has not stabilized yet, which we can conclude from high volatilities, but this might change in the future, once Bitcoin starts being using more widely.

On 2nd October 2013 original Silkroad was shut down and few weeks later, Silkroad 2.0 came alive. On 6th November 2014 Silkroad 2.0 was shut down by the FBI, its operator has been arrested and only few hours later, new version Silkroad 3.0 was launched. It is obvious that it is really difficult to fight the illegal side of the Bitcoin usage but officials at least try to do so. During the last year various regulations have been proposed, many reports have been released and even more recommendations have been made in connection with Bitcoin. Nevertheless nothing really restrictive or regulative has been performed. But it is clear from the current actions that policymakers won't allow Bitcoin and other virtual currencies to operate completely as they do today and some fundamental aspects of Bitcoin will have to be reduced, in particular privacy and anonymity. Regulators call for more compliant versions of Bitcoin and it is obvious that Bitcoin businesses will have to reveal some of users' private information to be able to function further.

Despite some drawbacks and many attempts to reduce Bitcoin's reach, Bitcoin together with other virtual currencies is a very interesting and lively topic that will outlive even if Bitcoin should fail. Nowadays the Bitcoin network is so huge, that it is assumed, that the total processing power of the whole Bitcoin network is faster at computing mathematical problems to verify transactions than the combined 500 most powerful computers in the world. Bitcoin has brought new concepts that have not been used before, has shown that the idea of virtual decentralized currencies could work and has achieved significant attention. However we still should not think of Bitcoin as a substitution for traditional currencies or a real competition to traditional monetary systems. Bitcoin does not have a special legal status, does not allow borrowing or lending and still does not fulfill the needs of significant masses. Bitcoin is rather an experiment of a new, alternative payment system that resembles community currencies. In some aspects, we could connect Bitcoin to thoughts of Austrian School of economics and

their free banking proposal, in particular their support of private currencies and thus creating a competition to public currencies. However there are many aspects in which Bitcoin does not follow their ideas, but we can also conclude that there are many aspects in which Bitcoin does not follow basically any existing ideas. Nonetheless it is yet impossible to put Bitcoin in one particular existing category, since it is a new concept that still lacks a proper classification.

Paper provides an overview of Bitcoin in terms of its technology and summarizes current legal issues and possible regulation. Since it is currently the best known and the most popular virtual currency, Bitcoin itself provides the best framework for understanding virtual currency schemes in general. Bitcoin's technology is the root of many other virtual currencies and serves as an example for future ones. Also from the regulation point of view, Bitcoin will probably serve as a reference, due to its technological concepts.

Weakness of this paper is the amount of reliable resources. Almost all of the available information on Bitcoin can be found only on the Internet. Many of this information come from blogs or analyses of various enthusiasts, where we cannot exclude some personal bias. Only a few articles were published in economic journals or by official institutions. However official reports are rather of descriptive nature than concluding. Therefore this paper tries to provide an objective and critical insight into the topic, with an emphasis on official reports and valuing both proponents' and antagonists' opinions.

The most of the information provided in this paper simultaneously applies on virtual, decentralized, P2P currencies in general. New information and articles keep appearing every day within this field and I believe that in the next years we are going to witness the increasing usage and spread of virtual currencies and also their increasing values.

Bibliography

Androulaki, E., et al. (2013). *Evaluating User Privacy in Bitcoin*. Retrieved March 2014, from http://eprint.iacr.org/2012/596.pdf

Babaioff, M., et al. (2012). *On Bitcoin and Red Balloons*. Retrieved March 2014, from http://research.microsoft.com/pubs/156072/bitcoin.pdf

Barber, S., et al. (2012). *Bitter to Better - How to Make Bitcoin a Better Currency*. Retrieved March 2014, from http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf

Baverman, L. (2014, September). *Bitcoin's future depends on public acceptance*. Retrieved October 2014, from http://www.usatoday.com/story/money/business/2014/09/02/baverman-bitcoin/14728425/

Bergstra, J. A., De Leeuw, K. (2013). *Bitcoin and Beyond: Exclusively Informational Money*. Retrieved March 2014, from http://arxiv.org/pdf/1304.4758.pdf

Bergstra, J. A., De Leeuw, K. (2013). *Questions related to Bitcoin and other Informational Money*. Retrieved March 2014, from http://arxiv.org/pdf/1305.5956.pdf

Brito, J., Castillo, A. (2013). *Bitcoin - A Primer for Policymakers*. Retrieved March 2014, from http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf

Calouro, E. (2014, January). *JP Morgan Chase CEO: Bitcoin a "Terrible Store of Value"*. Retrieved April 2014, from http://newsbtc.com/2014/01/23/jp-morgan-chase-ceo-bitcoin-terrible-store-value/

Chaffin, B. (2013, November). *U.S. Powers Acknowledge Benefits of Bitcoin, Price Soars and Corrects*. Retrieved June 2014, from http://www.macobserver.com/tmo/article/u.s.-powers-acknowledge-benefits-of-bitcoin-price-soars-and-corrects

Christin, N. (2012). *Travelling the Silk Road: A measurement analysis of a large anonymous online marketplace*. Retrieved March 2014, from http://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf

Dion, D. A. (2014). *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacked-Cash*. Retrieved March 2014, from http://illinoisjltp.com/journal/wp-content/uploads/2013/05/Dion.pdf

dogecoin.com. (2013, December). *dogecoin.com*. Retrieved June 2014, from dogecoin.com

EBA (2). (2014, July). *EBA proposes potential regulatory regime for virtual currencies, but also advises that financial institutions should not buy, hold or sell them whilst no such regime is in place*. Retrieved October 2014, from https://www.eba.europa.eu/-/eba-proposes-potential-regulatory-regime-for-virtual-currencies-but-also-advises-that-financial-institutions-should-not-buy-hold-or-sell-them-whilst-n

EBA. (2013, December). *EBA warns consumers on virtual currencies*. Retrieved October 2014, from https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies

EBA. (2014, July). *EBA Opinion on 'virtual currencies'*. Retrieved October 2014, from http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

ECB. (2012). *Virtual Currency Schemes*. Retrieved March 2014, from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Elwell, C. K., et al. (2013). *Bitcoin: Questions, Answers and Analysis of Legal Issues*. Retrieved April 2014, from http://www.fas.org/sgp/crs/misc/R43339.pdf

European Parliament and Council. (2007, November). *DIRECTIVE 2007/64/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 November 2007*. Retrieved October 2014, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF

European Parliament and Council. (2009, September). *DIRECTIVE 2009/110/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 September 2009*. Retrieved October 2014, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF

Eyal, I., Sirer, E.G. (2013). *Majority is not Enough: Bitcoin Mining is Vulnerable*. Retrieved March 2014, from http://fc14.ifca.ai/papers/fc14_submission_82.pdf

FBI. (2011, March). *Defendant Convicted of Minting His Own Currency*. Retrieved October 2014, from http://www.fbi.gov/charlotte/press-releases/2011/defendant-convicted-of-minting-his-own-currency

FinCEN. (2014). Retrieved October 2014, from http://www.fincen.gov/

FinCEN. (2014, January). *FinCEN Publishes Two Rulings on Virtual Currency Miners and Investors*. Retrieved October 2014, from http://www.fincen.gov/news_room/nr/pdf/20140130.pdf

Gilpin, L. (2014, May). *10 things you should know about Bitcoin and digital currencies*. Retrieved June 2014, from http://www.techrepublic.com/article/10-things-you-should-know-about-bitcoin-and-digital-currencies/

Gonda, P. (2008). *"Alternative approaches in money and banking, focusing on free banking" from slovak original Alternatívne prístupy k peniazom a bankovníctvu, so zameraním na slobodné bankovníctvo*. Retrieved January 2015, from http://www.konzervativizmus.sk/upload/pdf/3_4_seminar_AKE_2008_2009.pdf

Gonda, P. (2008). *"Theoretical and practical perspective on importance of money" from slovak original Rámcový teoretický a praktický pohľad na význam peňazí*. Retrieved January 2015, from http://www.konzervativizmus.sk/upload/pdf/8_seminar_AKE_peniaze.pdf

Grinberg, R. (2011). *Bitcoin: An Innovative Alternative Digital Currency*. Retrieved March 2014, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857

Güring, P., Grigg, I. (2011). *Bitcoin & Gresham's Law - the economic inevitability of Collapse*. Retrieved March 2014, from http://iang.org/papers/BitcoinBreachesGreshamsLaw.pdf

Hayek, F. A. (1976). *Denationalisation of Money - The Argument Refined - An Analysis of the Theory and Practice of Concurrent Currencies*. Retrieved January 2015, from http://mises.org/sites/default/files/Denationalisation%20of%20Money%20The%20Argument%20Refined_5.pdf

Herpel, M. (2011). *2011 Observations on the Digital Currency Industry*. Retrieved March 2014, from http://www.dgcmagazine.com/pdf/Digital-Gold-Currency-Magazine-Industry-Overview-2011.pdf

Hills, K. (2014, January). *Bitcoin's Legality Around The World*. Retrieved October 2014, from http://www.forbes.com/sites/kashmirhill/2014/01/31/bitcoins-legality-around-the-world/

Hollingshead, A. (2014, July). *Recent Efforts To Regulate Bitcoin Fall Flat*. Retrieved October 2014, from http://www.financialtransparency.org/2014/07/31/recent-efforts-to-regulate-bitcoin-fall-flat/

Investopedia. (n.d.). *Fiat Money*. Retrieved April 2014, from http://www.investopedia.com/terms/f/fiatmoney.asp

Jiricek, T. (2012). *Bitcoin smenarna*. Retrieved March 2014, from https://dip.felk.cvut.cz/browse/pdfcache/jiricto2_2012bach.pdf

Karame G. O., et al. (2012). *Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin*. Retrieved March 2014, from https://eprint.iacr.org/2012/248.pdf

Keiser, M. (2013, October). *Is Bitcoin Money*. Retrieved April 2014, from http://www.huffingtonpost.com/max-keiser/is-bitcoin-money_b_2849031.html

Krugman, P. (2013, December). *Bitcoin is evil*. Retrieved April 2014, from http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/

Krugman, P. (2013, April). *La Red Antisocial de los Bitcoins*. Retrieved April 2014, from http://economia.elpais.com/economia/2013/04/18/actualidad/1366310784_208220.html

Lee, T. B. (2013, December). *Dogecoins and Litecoins and Peercoins oh my: What you need to know about Bitcoin alternatives*. Retrieved September 2014, from http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/26/dogecoins-and-litecoins-and-peercoins-oh-my-what-you-need-to-know-about-bitcoin-alternatives/

Levy, S. (1994). *E-Money (That's What I Want)*. Retrieved May 2014, from http://archive.wired.com/wired/archive/2.12/emoney.html

London, J.P., Melbourne, G.T. (2011, June). *Bits and bob*. Retrieved September 2014, from http://www.economist.com/blogs/babbage/2011/06/virtual-currency

Luna, M. (2011). *BitCoin: a rube-goldberg machine for buying electricity*. Retrieved May 2014, from http://trustcurrency.blogspot.co.at/2011/03/bitcoin-rube-goldberg-machine-for.html

Luther, W. J., Olson, J. (2013). *Bitcoin is Memory*. Retrieved March 2014, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2275730

Mankiw, N. (2002). *Macroeconomics, 5th edition.* Worth Publishers Inc., U.S.

Marian, O. (2013). *Are Cryptocurrencies Super Tax Heavens?* Retrieved March 2014, from http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1365&context=facultypub

Meiklejohn, S., et al. (2013). *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*. Retrieved March 2014, from http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

Menger, K. (1892, Jun). *On the Origin of Money.* Retrieved January 2015, from The Economic Journal, Vol. 2, No. 6 (Jun., 1892), pp. 239-255: http://cas.umkc.edu/econ/economics/faculty/wray/631Wray/Menger.pdf

Meyer, R. (2014, March). *Why Bitcoin Can No Longer Work as a Virtual Currency, in 1 Paragraph*. Retrieved March 2014, from http://www.theatlantic.com/technology/archive/2014/03/why-bitcoin-can-no-longer-work-as-a-virtual-currency-in-1-paragraph/359648/

Mises, L. v. (1953). *The Theory of Money and Credit*. Retrieved January 2015, from http://mises.org/sites/default/files/The%20Theory%20of%20Money%20and%20Credit_3.pdf

Mises, L. v. (1963). *Human Action: A Treatise on Economics*. Retrieved January 2015, from http://www.cmi-gold-silver.com/pdf/humanaction.pdf

Mont, J. (2014, February). *New FinCEN Guidance Clarifies Corporate Bitcoin Requirements*. Retrieved October 2014, from http://www.complianceweek.com/blogs/the-filing-cabinet/new-fincen-guidance-clarifies-corporate-bitcoin-requirements#.VEuYXvl_s1I

Moore, T., Christin, N. (2013). *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*. Retrieved March 2014, from http://fc13.ifca.ai/proc/1-2.pdf

Möser, M. (2013). *Anonymity of Bitcoin Transactions*. Retrieved March 2014, from https://www.wi.uni-muenster.de/sites/default/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf

Nakamoto, S. (2008). *Bitcoin: A peer-to-Peer Electronic Cash System*. Retrieved March 2014, from https://bitcoin.org/bitcoin.pdf

namecoin.info. (2011, April). *namecoin.info*. Retrieved June 2014, from namecoin.info

peercoin.net. (2012, August). *www.peercoin.net*. Retrieved June 2014, from www.peercoin.net

Piasecki, P. (2012). *Design and security analysis of Bitcoin infrastructure using application deployed on Google Apps Engine*. Retrieved March 2014, from https://dl.dropboxusercontent.com/u/3658181/PiotrPiasecki-BitcoinMasterThesis.pdf

Plassaras, N. A. (2013). *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*. Retrieved March 2014, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2248419

Roberts, R. (2006, September). *An Interview with Milton Friedman*. Retrieved September 2014, from http://www.econlib.org/library/Columns/y2006/Friedmantranscript.html

Roio, D. J. (2013). *Bitcoin, the end of Taboo in Money*. Retrieved March 2014, from http://jaromil.dyne.org/writings-files/Bitcoin_end_of_taboo_on_money.pdf

Ron, D., Shamir, A. (2012). *Quantitative Analysis of the Full Bitcoin Transaction Graph*. Retrieved March 2014, from https://eprint.iacr.org/2012/584.pdf

Rothbard, M. N. (1962). *The Case for a 100 Percent Gold Dollar*. Retrieved January 2015, from http://mises.org/sites/default/files/Case%20for%20a%20100%20Percent%20Gold%20Dollar_2.pdf

Rothbard, M. N. (1963). *What Has Government Done to Our Money?* Retrieved January 2015, from The Ludwig von Mises Institute, Auburn University: http://www.solib.ro/sites/default/files/what_has_government_done_to_our_money_-_rothbard_0.pdf

Rothbard, M. N. (1970). *Man, Economy and State with Power and Market*. Retrieved January 2015, from http://mises.org/sites/default/files/Man,%20Economy,%20and%20State,%20with%20Power%20and%20Market_2.pdf

Santos, A. (2012, December). *Bitcoin-Central becomes first Bitcoin exchange licensed to operate like a bank*. Retrieved October 2014, from http://www.engadget.com/2012/12/09/bitcoin-exchange-bitcoin-central-licensed-bank/

SEC. (1933, amended and approved on April 5, 2012). *Securities Act of 1933.* Retrieved October 2014, from https://www.sec.gov/about/laws/sa33.pdf

Selgin, G. A. (1957). *The Theory of Free Banking - Money Supply under Competitive Note Issue*. Retrieved January 2015, from http://files.libertyfund.org/files/2307/Selgin_1544_Bk.pdf

Selgin, G. A. (2013, April). *Synthetic Commodity Money*. Retrieved October 2014, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118

Serwer A., Liebelson D. (2013, April). *Bitcoin, Explained*. Retrieved September 2014, from http://www.motherjones.com/politics/2013/04/what-is-bitcoin-explained

Shieber, J. (2014, March). *Goldman Sachs: Bitcoin Is Not A Currency*. Retrieved April 2014, from http://techcrunch.com/2014/03/12/goldman-sachs-bitcoin-is-not-a-currency/

Skudnov, R. (2012). *Bicoin Clients*. Retrieved March 2014, from http://bitcoinmalaysia.com/wp-content/uploads/2012/12/Bitcoin_Clients_Thesis_Skudnov_Rostislav.pdf

Surda, P. (2013). *Economics of Bitcoin: is Bitcoin an alternative to fiat currencies and gold?* Retrieved March 2014, from http://dev.economicsofbitcoin.com/mastersthesis/mastersthesis-surda-2012-11-19b.pdf

Susanu, C. G. (2011). *The Money Creation: Free Banking versus Central Banking Debate*. Retrieved January 2015, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1785253

The Law Library of Congress. (2014, January). *Regulation of Bitcoin in Selected Jurisdictions*. Retrieved October 2014, from http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

U.S. Code, Crimes and Criminal Procedure. (amended in 1994, September). *18 U.S. Code § 336 - Issuance of circulating obligations of less than $1*. Retrieved September 2014, from http://www.law.cornell.edu/uscode/text/18/336

U.S.Code, Commodity Exchange Act. (amended in 2001, May). *7 U.S. Code § 2 - Jurisdiction of Commission; liability of principal for act of agent; Commodity Futures Trading Commission; transaction in interstate commerce*. Retrieved October 2014, from http://www.law.cornell.edu/uscode/text/7/2

Vaishampayan, S. (2014, January). *J.P. Morgan's Jamie Dimon says bitcoin is a 'terrible store of value'*. Retrieved April 2014, from http://blogs.marketwatch.com/thetell/2014/01/23/j-p-morgans-jamie-dimon-says-bitcoin-is-a-terrible-store-of-value/

Wallace, B. (2011). *The Rise and Fall of Bitcoin*. Retrieved March 2014, from http://fromm.robertkeahey.com/wp-content/uploads/2013/07/Session-7-The-Rise-and-Fall-of-Bitcoin.pdf

Weisenthal, J. (2013, April). *Bitcoin Has No Intrinsic Value, And Will Never Be A Threat To Fiat Currency*. Retrieved April 2014, from http://www.businessinsider.com/bitcoins-have-no-value-2013-4

Weisenthal, J. (2013, December). *Here's The Answer To Paul Krugman's Difficult Question About Bitcoin*. Retrieved April 2014, from http://www.businessinsider.com/why-bitcoin-has-value-2013-12

White, L. (1999). *Why Didn't Hayek Favor Laissez Faire in Banking?* Retrieved January 2015, from http://www.cameroneconomics.com/white-hayek-hope.pdf

Wikipedia. (2014). *Central processing unit*. Retrieved May 2014, from http://en.wikipedia.org/wiki/Central_processing_unit

Wikipedia. (n.d.). *Central processing unit*. Retrieved May 2014, from http://en.wikipedia.org/wiki/Central_processing_unit

Worstall, T. (2013, December). *Paul Krugman on Bitcoin, It's Not A Stable Store Of Value*. Retrieved April 2014, from http://www.forbes.com/sites/timworstall/2013/12/29/paul-krugman-on-bitcoin-its-not-a-stable-store-of-value/

Zusammenfassung

Bitcoin ist ein neues alternatives Konzept der virtuellen Währung oder des Bargelds, das im Internet benutzt wird. Anders als traditionelle Währungen hat Bitcoin keinen zentralen Emittent und es ist komplett dezentralisiert. Bitcoin ist attraktiv wegen seinen niedrigen Transaktions- und Betriebskosten. Auf der anderen Seite, da es keine Gebühren gibt, bietet Bitcoin keinen Schutz oder anderen zusätzlichen Dienste. Bitcoin ist anonym und sein Wert ist nur von dem von den Benutzern(-innen) zugewiesenen Wert abgeleitet, aber es ist gegen keine Handelsware einlösbar und es ist nicht staatlich garantiert.

Diese Masterarbeit beschäftigt sich mit der Frage, ob die alternative elektronische Währungen als Geld, aus der Perspektive der sowohl klassischen Ökonomie als auch liberalen Ökonomie, wahrgenommen werden können. Der theoretische Teil der Arbeit untersucht die Geldentwicklung in dem aktuellen Geldpolitiksystem und in dem alternativen Bankfreiheitsystem (free banking) und beabsichtigt das Bitcoin in eine derzeitige Kategorie zu stellen. Bitcoin erfüllt am besten die Definition der Währung, aber es ist mit den Eigenschaften den anderen Kategorien gemischt (z.B. Handelsware). Die Kritik des Bitcoins als Zahlungsmittel kommt vor allem aus der Definition der österreichischen Schule, weil es nicht als ein universelles Zahlungsmittel akzeptiert wurde (trotzdem könnte Bitcoin als ein sekundäres Zahlungsmittel betrachtet sein). Außerdem übertritt Bitcoin das Regression Theorem von Mises. Es ist also nicht möglich die Herkunft seines Wertes zu identifizieren. Der empirische Teil der Arbeit beschäftigt sich mit den Bitcoin Preisen und Volumen. Der letzte Teil zusammenfasst die aktuellen gesetzlichen Angelegenheiten und Regulierungen, die möglicherweise auf Bitcoin und anderen virtuellen Währungen einsetzbar wären.

Finale Argumentation erklärt, dass Bitcoin Technologie nicht perfekt ist. Zurzeit ist es nicht erwartet, dass Bitcoin irgendeine traditionelle Währung ersetzen könnte. Auch wenn Bitcoin scheitern sollte, wird es auf jedem Fall erwartet, dass diese spannende technologische Innovation nicht komplett verschwindet. Es sieht so aus, dass die Idee der privaten Währungen umzuwerten ist. Deswegen ist es notwendig, unsere gegenwärtigen Ansichten auf alternative Währungen kritisch zu betrachten und gegebenenfalls zu korrigieren.

Currículum Vitae

PERSONAL DATA:

Surname:	**Bianchi**
First name:	Zuzana
Degree:	BSc.
Nationality:	Slovak
E-mail:	bianchi.zuzana@gmail.com

EDUCATION:

October 2012 - present	**Master degree International Business Administration** Specialisation: Financial Markets, International Management Universität Wien
October 2008 – Jun 2012	**Bachelor degree International Business Administration** Specialisation: International Management, Business Spanish Universität Wien
February 2011 – July 2011	**Semester abroad - Erasmus Program** Additionally: Language course Universidad de Barcelona
September 2000 – May 2008	**Honoured school leaving examination** Specialisation: Languages, Economics Private secondary school Mercury, Bratislava, Slovakia

WORK EXPERIENCE:

July 2014 – present	**Erste Group Bank AG, Vienna, Austria** ALM Analyst in ALM Analytics department
March 2014 – June 2014	**Erste Group Bank AG, Vienna, Austria** Part-time working student in ALM Analytics department
September 2013 – February 2014	**Raiffeisen Bank International AG, Vienna, Austria** Fulltime internship in treasury division: Funding management department
September 2012 – February 2013	**Dell, a.s., Bratislava, Slovakia** Part-time working student: Member of "Financial Internship Program" in accounting department, Team: international Consolidation
July 2011 – September 2011	**Seat, S.A., Martorell, Spain** Fulltime internship in controlling department

July 2010 – December 2010	**Volkswagen Slovakia, AG, Bratislava, Slovakia** 3 months fulltime internship and 3 months part-time working student in logistics planning department

July 2008 – August 2008	**Aurus**, **s.r.o, IT economic systems, Bratislava, Slovakia** Fulltime assistant

2006 - 2008	**Synovate, Market Research Agency, Bratislava, Slovakia** Part-time market research referent

PERSONAL AND OTHER SKILLS:

Language skills:	**Slovak** – Mother language **English** –Level C1 *Oxford Language Centre Certificate* - Adult Upper-Intermediate Level 4, 2008 **German** – Level C1 *Deutsches Sprachdiplom der KMK* – Stufe II, 2008 **Spanish** – Level B2 **Italian** – Level A2-B1 **Russian** – Level B1

Other skills:	Computer (MS Windows, MS Office, Internet, SPSS, EViews, Oracle Novora Financials, QRM) Driver's licence category B