Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Economics

Diploma Thesis

Virtual currencies analysis: Case study of Bitcoin

Bc. Markéta Gajdorusová

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Markéta Gajdorusová

Economics and Management

Thesis title

Virtual currencies analysis: Case study of Bitcoin

Objectives of thesis

The objective of the thesis is to explain and describe the substance of virtual currencies, reasons of their creation and development in time. Furthermore, to clarify the origin and utilization, describe transactions in contrast with fiat currency transactions under surveillance of banks. Special focus is aimed to the most significant performer of digital currency Bitcoin. The aim is to analyse factors influencing the value of Bitcoin. Furthermore, to describe both benefits and risks of Bitcoin application in practise. It is included detail study of two the most popular digital currencies to explain and compare these different competitive crypto currencies. Last but not least, the thesis is focused on economic impacts along with the likely future development and consequences in banking sector. It is followed by the explanation of contrast between fiat and cryptocurrency characteristic, complemented by explanation the digital currency transaction system. The practical's part aim is to analyse the Bitcoin price depending on selected variable factors. The goal of the thesis is to verify stated hypothesis and to determine the variable factors, that influence Bitcoin the most. The analysis primarily serves to compare inconsistent characteristics, highly volatile trend and secondary to show and clarify risks in case of future investment into these digital currencies. Finally, to evaluate the digital currency as a whole to show benefits of using digital currency in practise as well as associated risks and threads.

Methodology

Theoretical part is concentrated on the description and explanation of theory, definition of individual terms and characterization of attributes in this problematic. Practical part is directed to the analysis of selected cryptocurrency Bitcoin. There are collected time series daily data in time period 2016-2017. It is used in analysis time series data of secondary type from publicly accessible resources in order to obtain primary data.

Fundamental analysis compares digital currency transaction system with bank transaction using ratio, difference, frequency, electricity energy consumption and its costing. Regional usage, conditions and legal regulation is depicted by methods of: observation, syntheses, description and explanation.

Technical analysis includes real life investment scenario. Explanation of Bitcoin value determinants is done by regression and autoregression analysis using open source software. It is used econometric, mathematical-statistical methods: mean, median, mode, variance, standard deviation, ordinary least square method,

correlation matrix and autoregressive integrated moving average. There are used econometric models and tests in order to prove and verify stated hypothesis. As well to reveal mutual dependence of Bitcoin price on variable factors. Results are processed into tables with graphical representation and description of development in time to visualize determinants, progress development and comparison.

The proposed extent of the thesis

60 pages

Keywords

Virtual currency, digital, crypto currency, Bitcoin, blockchain, means of payment, decentralization, online transactions

---

Recommended information sources

Blockchain. (2018). Bitcoin Charts & Graphs – Blockchain. [online] Available at: https://blockchain.info/charts [Accessed 21 Oct. 2018

FRISBY, Dominic. Bitcoin: The Future of Money? London: Unbound, 2014. 304 pages. ISBN: 1783520779.

Investing.com. (2018). BTC USD | Bitcoin US Dollar Bitfinex – Investing.com. [online] Available at: https://www.investing.com/currencies/btc-usd [Accessed 1 Nov. 2018].

LEE, David. Handbook of digital currency: bitcoin, innovation, financial instruments, and big data. Amsterdam: Elsevier/ AP, 2015. ISBN 9780128021170.

RIZZO, Pete. Bitcoin Hearings Day 1: Bitcoin Hits 'Tipping Point' with New York Regulators

STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin: peníze budoucnosti : historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky. Praha: Ludwig von Mises Institut CZ&SK, 2015. ISBN 978-80-87733-26-4.

TAPSCOTT, Don. Blockchain Revolution

VIGNA, Paul. a Michael J. CASEY. The age of cryptocurrency: how bitcoin and digital money are challenging the global economic order. New York: St. Martin's Press, 2015.

Expected date of thesis defence

2018/19 WS – FEM (February 2019)

The Diploma Thesis Supervisor

Ing. Petr Procházka, Ph.D., MSc

Supervising department

Department of Economics

Electronic approval: 15. 11. 2018

prof. Ing. Miroslav Svatoš, CSc.

Head of department

Electronic approval: 20. 11. 2018

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 29. 11. 2018

Declaration

I declare that I have worked on my diploma thesis titled "Virtual currencies analysis: Case study of Bitcoin" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the diploma thesis, I declare that the thesis does not break copyrights of any third person.

In Prague on Signature _____

Acknowledgement

I would like to thank my supervisor Ing. Petr Procházka, MSc, Ph.D. for his support, assistance and kind help within the processing this diploma thesis. I would like to thank my friends for their support and advices.

Virtual currencies analysis: Case study of Bitcoin

Abstract

This diploma thesis deals with digital currencies. There is described in details digital currency Bitcoin. Theoretical part explains principles, functions and applicability of virtual currencies in comparison with fiat currencies. Attention is paid to basis of both kinds of currency transaction systems. It is included explanation of usage legality and regulations in selected regions. Furthermore, there are described value determinants, utilization, influence and consequences in relation with using virtual currency. Thesis also presents origins, development, current situation and future prognosis in digital world from monetary point of view.

The practical part is focused on virtual currency Bitcoin from point of view analysing the value fluctuation in time. There is carried out comparative analysis of Bitcoin vs Ethereum characteristics, application and time trend. In addition, there is explained and depicted the energy consumption connected with creating new virtual coins. Practical part is dedicated to regression and autoregression analysis of time series data consisted of Bitcoin price value explained by selected determinants. There are stated and subsequently verified hypothesis from collected data representing Bitcoin price and its determinants. Time series analysis is then tested and verified using open source software. Time series is concluded with dynamic prognosis and evaluation of models obtained from calculated results. Discussion and recommendation options are included in final part. The thesis concludes with summary of benefits together with security, risks and threats of virtual currency from both objective and subjective point of view.

Key Words: Virtual, Digital, Crypto Currency, Bitcoin, Blockchain, Value, Decentralization, Network, Online Transaction, Anonymity

Analýza virtuálních měn: Případová studie Bitcoin

Abstrakt

Tato diplomová práce se zabývá virtuálními měnami. Detailně je popsána digitální měna Bitcoin. Teoretická část vysvětluje principy, funkce a použití virtuálních měn a porovnává je s fiat měnami. V teoretické části je dále věnována pozornost oběma transakčním systémům a rozdíly mezi nimi. V práci je vysvětlena legalita použití a regulace ve vybraných zemích. Dále se práce zabývá determinanty určujících hodnotu, využití, vliv a dopady v závislosti s použitím této digitální měny. Diplomová práce taktéž prezentuje vznik, vývoj, aktuální situaci a budoucí prognosy v digitálním světě z monetárního úhlu pohledu.

Praktická část je zaměřena na virtuální měnu Bitcoin z pohledu analýzy jeho hodnoty v daném časovém období. Je zde provedena komparativní analýza měny Bitcoin a Ethereum zahrnující jejich vlastnosti, použití a časový trend. Dále je v práci vysvětlena a zobrazena spotřeba elektrické energie spojená se vznikem nových virtuálních mincí. Praktická část se nejvíce věnována regresní a autoregresní analýze časové řady představující cenu Bitcoinu. Ta je závislá na vybraných nezávislých determinantech. Jsou zde vytyčeny a následně otestovány hypotézy pomocí open source softwaru. Analýza časové řady je zakončená dynamickou prognosou a evaluací získaných modelů ze spočítaných výsledků. Diskuse, vyhodnocení a doporučení jsou součástí závěru práce. Práce je zakončena shrnutím benefitů spolu s bezpečností a riziky spojenými s virtuálními měnami z objektivního i subjektivního úhlu pohledu.

Klíčová slova: Virtuální, digitální, krypto měna, Bitcoin, blockchain, hodnota, decentralizace, network, online transakce, anonymita

Table of content

List of figures

List of tables

1. Introduction

Invention of money and bond enable the expansion of trade in ancient times, establishment of banks with compound interest and double entry accounting have brought along the Renaissance firstly to Italy then to whole Europe. The boom of insurance companies and stocks stand behind the overseas discoveries and invention of bank reserves gave arise to a huge capital, which poured out into the industrial revolution. The expansion changes the contraction. Into the financial history it is unforgettably written two recent events, the crises from the year 2008 and rocket start of internet technologies. In conspicuous way, there is already taking place another revolution in banks, insurance companies and financial services. The revolution is called the fintech revolution. The world is very close to become free of banks, traditional currencies and even authorities. Such situation would result in totally digital verification of all transactions, instead of material cash there would become virtual money and if we believe in virtual reality, soon it become hologram.

In recent years there have emerged new methods of non-cash payments particularly in connection with internet. One of the methods represents the usage of probably the latest means of payment - crypto currency or in other words digital currency. In comparison with fiat currencies [1]these digital ones are still just marginal concept. Nevertheless, the popularity and so interconnected usage of digital currencies have grown up very sharply in recent months. Arrival of cryptocurrencies has brought not just another way of possible payment method but also revive debates concerning the influence of money by central authorities and banking systems generally. I choose in my thesis as a representative of digital currency the strongest and most known digital currency, which was also the first of its kind and it is called Bitcoin.

Bitcoin points out on several potentially problematic characteristics of fiat currencies which are described later-on in detail. On the other hand, there are of course disadvantages and risks connected with using digital currencies. I consider myself as independent spectator of this system. It is important to mention, I am not interested in my own profit

[1] Fiat currency: Conventional currencies issued by the central bank (Dollars, Euros, Crowns, etc.)

from mining or trading with cryptocurrencies. So, my point of view is supposed to be objective.

In analytical part, there are analysed and described regional legal regulation, frequency of use, security, risks. Special attention is paid to the comparison of selected factors that significantly influence the market value of digital currencies.

The conclusion is concentrated on both objective and subjective evaluation of results from practical part. Furthermore, there is discussed the prediction of further development of virtual currencies in contrast with development of banking sector.

Nowadays all these virtual currencies represent one huge experiment, because the history of their existence is too short. However, it is important to take into account, they are increasingly affecting the real economy. Financial and other state authorities are aware of that fact and they have started exploring this new phenomenon. Last but not least, authorities try to respond to the absence of a legal framework and related issues together with risks.

Selected topic of this thesis is so agile and rapidly changing, that it is probable there could have come up to some changes during the period of creating the thesis. I just would like to notify by this that some information or data may be inaccurate or no longer valid during the time.

2. Objectives and Methodology

2.1 Objectives

The main aim is to describe, explain and analyse the virtual currency as a means of payment. There are explained principles, functions and applicability of virtual currencies in comparison with fiat currencies. The diploma thesis is divided into two parts. The first one is theoretical which introduces the chosen topic and explains it on the basis of information from the scientific publications. The theory is followed by the practical part, which deals with calculating and testing collected data from the online statistics.

The thesis describes the origins, development, current situation and future prognosis in digital world from both economic and technical point of view. It is included the study of possible future situation when encountering the banking sector.
Special focus is paid to the detail study of two selected digital currencies representatives Bitcoin and Ethereum. There are presented the characteristics and properties of both digital currencies. Then, it is studied and presented consumption of electricity energy when creating new coins.
Another aim of the thesis is to explain the origin, substance, behaviour, utilization and reason of creation of digital currencies. Last but not least, the thesis is focused on economic impacts along with the likely future development and consequences in banking sector. Which is followed by the explanation of contrast between fiat and cryptocurrency characteristics.

Second part of the thesis is focused on virtual currency Bitcoin and its technical analysis explaining the price determinants. Analysis is based on dependent Bitcoin price and selected variable factors influencing the price of Bitcoin in analysed time horizon. There are stated and subsequently verified hypothesis from collected data representing Bitcoin price and its variable determinants. One of the main thesis objectives is to verify following analysis hypothesis:

1st: The higher the amount of transactions per day, the higher the price of Bitcoin.
2nd: The higher the cost per transaction, the higher the price of Bitcoin.
3rd: The higher the revenue for miners per block, the higher the price of Bitcoin.

4th: The higher the mining difficulty, the higher the price of Bitcoin.

5th: The price of Bitcoin fluctuates randomly without recognizable patterns and with high variance.

The analysis primarily serves to compare inconsistent characteristic, highly volatile trend and secondary to show, clarify risks in case of future investment into this digital currency. The goal is to determine the variable factor, that influence Bitcoin the most, therefore, it is significant or best in terms of reported results. Next, the thesis tries to reveal what other factors affect Bitcoin and looks at this popular digital currency from user behaviour point of view. And finally, the thesis evaluates the digital currency as a whole system of modern technologies. There is included simulating scenario of investing in Bitcoin in order to evaluate and recommend possible future investment. Furthermore, to show benefits of using digital currency in practise as well as associated risks and threads.

2.2 Methodology

The methodology of the thesis is divided into two main parts. The first one provides theoretical background within the literature review using descriptive and explanatory method. Theoretical part is concentrated on the description and explanation of theory, definition of individual terms and characterization of attributes in these problematics.

Practical part is directed to the analysis of selected cryptocurrency Bitcoin. There are collected time series daily data in time period 2016-2017. It is used in analysis time series data of secondary type from publicly accessible resources in order to obtain primary data.

It is used fundamental and technical analysis to evaluate and obtain results of both analyses.

Fundamental analysis compares digital currency transaction system with bank transaction using ratio, difference, frequency, electricity energy consumption and associated costs. Regional usage, conditions and legal regulation is depicted by following methods: observation, syntheses, description and explanation.

Fundamental analysis also includes both economic and non-economic indicators to evaluate collected data: such as inflation rate, exchange rate, user experience and subjective expert views. Observation of human psyche and behaviour of users belongs to

fundamental analysis. The future credibility is dependent on behaviour and psyche of users.

Technical analysis includes simulation of real-life investment. Explanation of Bitcoin value determinants is done by regression and autoregression analysis using open source software Gretl. As a tool of fundamental analysis, it is used statistical-mathematical and econometrics methods like: Ordinary Least Square Method, Autoregressive Integrated Moving Average including mean, median, mode, variance, standard deviation, correlation matrix and prognoses of time series. There are used econometric models and tests in order to prove and verify stated hypothesis. Asymptotic significance is measured by p-values and T-tests values in order to prove or deny mutual dependence of Bitcoin price on variable factors. There are also used prognostic forecasting methods for the probable future development. Results are processed into tables and figures with graphical representation and description of development in time to visualize determinants, progress development and comparison. Within the processing of all analysis, I relied on publicly accessible data, resources and information.

3. THEORETICAL PART

3.1 Characteristic of Virtual Currency

Most of the people think that our money is safe in banks. But have we ever thought about the situation when the system would collapse? For example, in the case of the state bankruptcy or the will of bank to block your funds and simply not to issue them back. These things have been happening quite often in recent time.

Bank sector is created from private organizations and such a bankrupt can be related to any of these organizations. Our deposits in banks have not been physically covered since 70's of the last century, when the bond between dollar and gold was cancelled. Today's money is covered only by the performance of economies and by the promise of central banks, they will not create too much new money. (Antonopoulos, A. 2015)

The whole risk comes from the fact that we entrust our money to the third party to keep it safe on the basis that there will be the possibility to take the money back, when we need to. But the fact to lose the money is possible whenever the bank refuses to or cannot issue it back. To sum it up I would say traditional banks are simply doubtful, expensive and logy.

In cryptocurrency system, everybody represents the bank to his/her own. This kind of system is like a holding cash or physical gold. But in comparison from that it differs by the much better protection from the theft or loss.

States all over the world lowers the freedom by sneaky way in all areas of life which means also finance. Governments restrict the free market, introduce electronics evidence of receipts, forbidden the cash and furthermore keep eye on citizens in large scale, censor the internet and even payments. (Stroukal, D. & Skalický, J. 2017). Billions of people still don't have access to financial services. In some countries, the situation is so bad, that people loose lifelong savings due to the state interventions and moreover die because of inaccessibility of essential food and medicaments. (Hubík, J. 2014)

Imagine the world in which the money is truly yours, without your permission nobody can take it away from you, devaluate it, or hinder in using it. I have in my mind the image of the world where there are financial services accessible to everybody without exception,

where the transactions of money take places immediately, without barriers, and with minimal fees. The world where only you decide, that just you buy. Where states cannot support anymore the wars through the printing new banknotes and where central banks cannot destroy your lifelong savings by imaginary push the button. That is how it would life and world look like if everybody would use digital currencies such as Bitcoin. “It is not just the first decentralized and truly free currency, which has no individual, corporation or state under its control. It is about the technological and social revolution”. (Nakamoto, S. 2009). We should let this new and young technology to develop freely. Listen. Learn. Do not call for fear on the grounds of unknown after all these regulations and prohibitions.

Encryption, anonymization and cryptocurrency enables not only the real protection privacy and property, but also the defence against censorship and discrimination. (Antonopoulos, A. 2015).

Everybody can join this decentralized and substantially uncontrollable economy, because money do not belong the state. (Hubík, J. 2014). Moreover, there is one of the strongest bitcoin communities on the world in Prague, which is explained more specifically later in practical part.

3.2 Bitcoin

Bitcoin is a form of cryptocurrency which is not owned, controlled or managed by any of the government, kings or any powerful organization. Bitcoin is not printed in banks and is not produced against gold. It is the most popular decentralized digital currency which is now used worldwide as a medium of exchange. Bitcoin represents a huge deal. (Antonopoulos, A. 2015).

In 2008 the world had to face one of the biggest crises in its history. The reality market, which was concerned as solid as a rock collapsed and unaware society was grasped in its own trap. The world economics was shaken in the grounds. The financial crises that started in 2007 caused the initiative of the group called Satoshi Nakamoto. Right after the crises this grouping came up with the new form of digital money, which has started the new revolution in fin-tech world. Bitcoin digital currency has been created in 2009, it is first and the strongest cryptocurrency which has been developed. It is the open source software

with peer-to-peer network that enables digital payment without the participation of the third party. The main uniqueness of Bitcoin represents its full decentralization; it is designed so that no one, neither the author or other individuals, groups or governments could not in any way affect the currency by destroying, falsifying, confiscating accounts, control cash flows or cause the inflation. In the network, there is no central point and nobody who could make decisions about the network. Bitcoin is in its essence deflationary currency. The total amount of money is finite and known in advance, and its release into the circulation is defined only by mathematical laws. Bank and governments cannot affect the frequency of bitcoin mining thanks to worldwide unchangeable rules. In the network, there are held payments for smaller or bigger cost. In contrast with bank transactions the Bitcoin ones are available 24/7, even in non-working days. (Frisby, D. 2017)

There has been made up many digital crypto currencies, however Bitcoin represents the most valuable medium in terms of value of "coins". Currently there are 15 billion of USD in the circle. (Stroukal, D. & Skalický, J., 2015). The reason why I decided to concern in this thesis on Bitcoin is that it is the first and strongest means of payment of its kind. Other digital currencies such as Monero, Zcash, Litecoin or Ethereum sums approximately only tenth of value of bitcoins. The reasons why it is so will be described later in the thesis.

Bitcoin (abb. BTC) is technically a type of network protocol with function to send and receive payment information. The unit of money on the Bitcoin protocol is the 'bitcoin' with a small 'b'. As the dollar is the unit of money on the US banking network, so the bitcoin is the unit of money on the Bitcoin system. Which means, Bitcoin is two things – a protocol and a unit of money. (Nakamoto, S. 2009)
The value is dependent not only on the confidence of users, but on the number of transaction and primarily on the stock where it is traded. In other words, the value subordinates the demand and supply on the market together with the trust of the future usage of this cryptocurrency. That is why the rate is then pretty much volatile relative to fiat currencies. The smallest part of bitcoin, also called 1 Satoshi, which can be separately manipulated is 0,00000001 BTC. (Nakamoto, S. 2009)

The finite amount of bitcoin in the circle is firmly given, currently there are app. 17mill. of BTC in circulation. The value of bitcoin is pretty much volatile, right now the current

value of 1 BTC equals app. 94 000 CZK/4200 USD/3700 EUR. Maximum amount of coins in the circulation counts 21 000 000 BTC which will be mined until the year 2140. Every 10 minute there are approximately 12.5 new coins. New coins mining and releasing into circulation is constantly slowing down. In fact, it is demonstrated through already mined amount of virtual money. There is mined almost 80% out of final amount of Bitcoin. The average number of daily Bitcoin transactions reached almost 224 000ths. in August 2017. Exactly one year ago in August 2016, it was around 206ths. of transactions. As we can see from the statistics, the daily volume of Bitcoin trades has risen rapidly over the past year. Together with this fact it also increased the average volume of transactions, which reached $ 86.7 million in August 2016, while this year it was already $ 2 billion during the same period. (Investing, 2017)

With expansion of Bitcoin it has come not just the interest of investors, customers and companies, but also state institutions. States of the EU regard cryptocurrencies suspiciously and consider them as appropriate means for black and grey economy, tax evasion or financing of illegal activities. To receive or send Bitcoins it is very simple, we just need to have installed the electronic wallet. The only identification is subsequently the unique address, where it is sent the amount of Bitcoin or other digital currency. Afterwards transaction is saved into blockchain. The blockchain technology is explained in the following paragraph.

Bitcoin represents not just potential new means of payment, but also alternative financial system based on so called blockchain. Blockchain stands for public, accessible string of all Bitcoin transactions. In other words, blockchain means the book of records where blocks are groups of transactions made through cryptographic hash. In Bitcoin system, everybody maintains its own ledger. The whole configuration does not give a chance to any central authority to control or regulate the system. (Stroukal, D. & Skalický, J., 2015)

The following chart shows the exchange rate development of Bitcoin (BTC) in comparison with US dollar (USD). The horizontal axis represents time, since November 2017 up to present. The vertical axis marks the amount of USD which correspondents to value of 1 BTC. At the turn of the year, there was a shock upwards, it was also the highest value nearly about 20,000 USD/BTC in the whole history of Bitcoin existence since the

launching in 2009. Actual price per Bitcoin fluctuates around 6,500 USD. (S.tradingview.com, 2017)

Figure 1: Exchange Rate BTC/USD

Source: S.tradingview.com (2017)

3.3 Blockchain System

Blockchain in other words means decentralized book of records – the public ledger. A block is a file with a record of recent transactions, like a page in a book of account. Each new block is then added to the chain. Currently its usage is the most often connected with cryptocurrency and its recording of transactions. Correctness of data guarantee every node in the system in which the blockchain is virtually meandered. Nodes are PC's of users connected into the network. There are strictly programmed conditions which all data undergo when entering into the system.

Every record is transaction between two parties – receiver and sender, no other party can enter the system, for example a bank, which would represent the third party as it is true in centralized system. (Stroukal, D. & Skalický, J. 2015)

Blockchain represents the future of transactions, the biggest advantage lies in quickness and decentralization of transactions on both national and multinational level. Transactions from one side of the globe to the other side can be proceeded within a minute. In comparison with centralized system, which represents one huge database with possibility

to be hacked one day by institutions, blockchain cannot delete any transaction because nobody can enter the system and change or manipulate recordings. Another advantage is to transact without costly intermediaries. Without the blockchain, Bitcoin is useless. Trust is based on crypto-proof and just blockchain provides that proof. Once the transaction is recorded, it cannot be deleted from blockchain. (Stroukal, D. & Skalický, J. 2015)

According to Nakamoto (2007) the system is based on Peer-to-Peer (P2P)[2] computing. Such architecture contains above mentioned nodes meaning individual computers that share resources amongst each other without the use of a centralized administrative system. All peers are equally privileged. They are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided.

Blockchain is the world's leading software platform for digital assets. The primary purpose is to build a better financial system in more simple, secured and seamless way. Currently there are powered over 100M transactions and empowered users in 140 countries across the world.

Following picture represents the network based on the client-server model, where individual clients request services and resources from centralized servers.

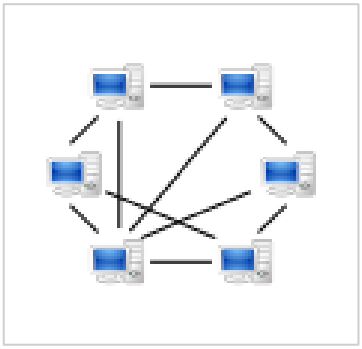
[2] P2P: decentralized communications model where each party has the same capabilities and either party can initiate a communication session. Unlike the client/server model, in which the client makes a service request and the server fulfils the request, the P2P network model allows each node to function as both a client and server.

Figure 2: Client – Side Network

Source: wikipedia.org/Client-server_model

A peer-to-peer (P2P) network contains interconnected nodes ("peers") and share resources amongst each other without the use of a centralized administrative system. (Parker, S. 1998)

Figure 3: P2P Network



Source: wikipedia.org/Peer-to-peer

3.4 Mining

At this moment, it is time to clarify, where and how there are Bitcoins produced. As I mentioned above, there is no material form of Bitcoin, therefore there do not exist any tangible coins or bank notes, it is just and only virtual currency in its digital form.

Bitcoin is gained through the process called mining. It is responsibility of miners who quest for new blocks. So, when we run a software – when we mine – what actually happens, is that we maintain the blockchain. Once a block is added, it is never changed. (Fillner, K. 2017)

According to (Nakamoto, S. 2009) the block is a processed group of transactions, that means the node takes transactions which are to be confirmed. Then it sorts them in a certain way and subsequently it processes them with encryption protocol. The result of encryption is so-called “hash”. The new block is logged into Blockchain and all nodes start searching for another. Blocks contain the data about all transactions, and as I have already mentioned above, that is why the blockchain is both the book of accounts and the account statement of all transactions that have ever occurred in the Bitcoin network.

In other words, it can be explained as confirmation of correctness of transactions in Bitcoin network. In normal system, this function is performed by banks. But there must be some control over the users of decentralized system, and the control means users themselves. “The whole proposal of Bitcoin counts with the fact, that most of the users will be honest, that is why it is always needed more than 50% of user's approval for sending the transaction. If there would be any fictional transaction sent into the system, potential invader would have got more than 50% of computing power of the network to confirm such transaction”. (Nakamoto, S. 2009)
Nevertheless, the power performance of network is currently so high, that possible attack is significantly improbable.

Original concept of Bitcoin counts that anybody could approve transactions on "home" PC. Thanks to that it was solved the question of distribution of Bitcoin amongst other users. Miners who quested for new Bitcoins this way got as a reward both fees from individual transactions and for emission of new Bitcoin into the network. Division of new Bitcoins is assigned to the user, who counts requested algorithm as a first. This algorithm is marked as a hash and serves as translator of entering data into the relatively small number. That is the reason why it is very important to have high-performance processor computer in order to increase the probability of primacy. However, soon it become clear that AMD or nVidia[3] graphic card with its architecture is able to calculate individual hashes many times faster than processor, therefore the high performance processor itself is nowadays no more effective.

[3] AMD and nVidia producers represent the best suitable types of graphic chips for mining of Bitcoin

The whole dynamics rests in maintaining the blockchain. People are incentivized to mine coins and verify transactions to keep the value up. [4]

3.4.1 Graphical Cards

Since the time Bitcoin has started to gain in its value, it become very interesting for producers of hardware, and for that reason it was manufactured special HW with simultaneously very high performance and low energy consumption. Production of these so called, ASIC chips is situated in China, where it is the world's largest focus on Bitcoin's mining.

Currently Bitcoin mining is being carried out in large quantities in special farms and exactly China represents ideal place for such activity due to various reasons: cheap electricity, high availability of HW, ASIC chips production, no need to pay custom duties or tariffs when shipping to the EU or US.[5]

3.4.2 Difficulty

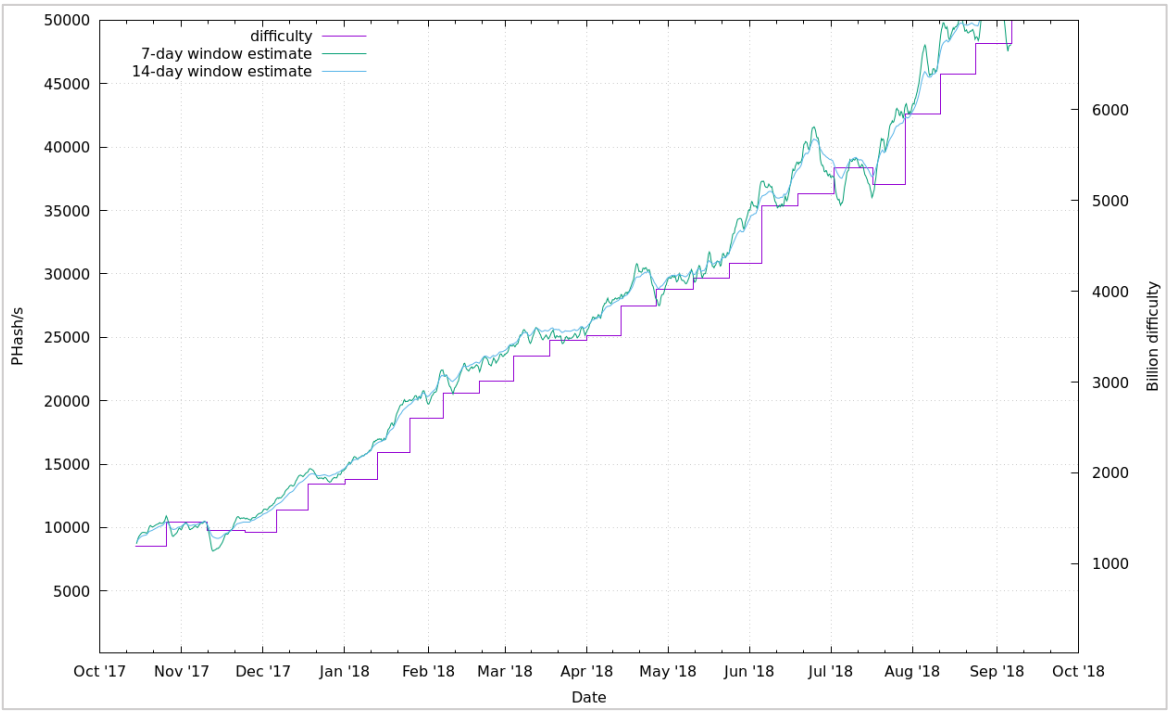
"It is needed to monitor the performance of the entire Bitcoin Network in order to solve new block approximately every 10 minutes. This time interval is fixed given and guarantee regular mining together with verifications of transactions". (Antonopoulos, A. 2015). If network performance doubles, the speed of finding a new block also increases. The network itself solves this problematic by increasing or decreasing the difficulty to find a new hash over the new block. The whole network mines one block just once in 10minutes. How many new Bitcoins and transactions are verified depends on hashing difficulty. Which is given by number of nulls in the beginning of every hash. The difficulty is checked every two weeks according to average number of transactions solved during 10-minute interval. (Stroukal, D. & Skalický, J. 2015).

If there are more nulls in the hash, it means the difficulty is higher together with power of network. Thanks to this autoregulation it is ensured that, blocks are solved in the same intervals and so new coins are mined after confirmation of a block. Moreover, every user is able to check how many coins is in circulation and if the issued number of coins corresponds. The whole trick is again in transparent blockchain. The following graph

[4] https://www.techradar.com/news/best-mining-gpu
[5] www.bitcoinmining.com

shows the development of the difficulty of mining. It can be seen the gradually increasing violet line showing the difficulty level. During one-year period, since October 2017 until October 2018, depicted in the graph the difficulty has increased approximately 5x. And will be still increasing trend until the last block will be mined.

Figure 4: BTC Network Total Computation Speed

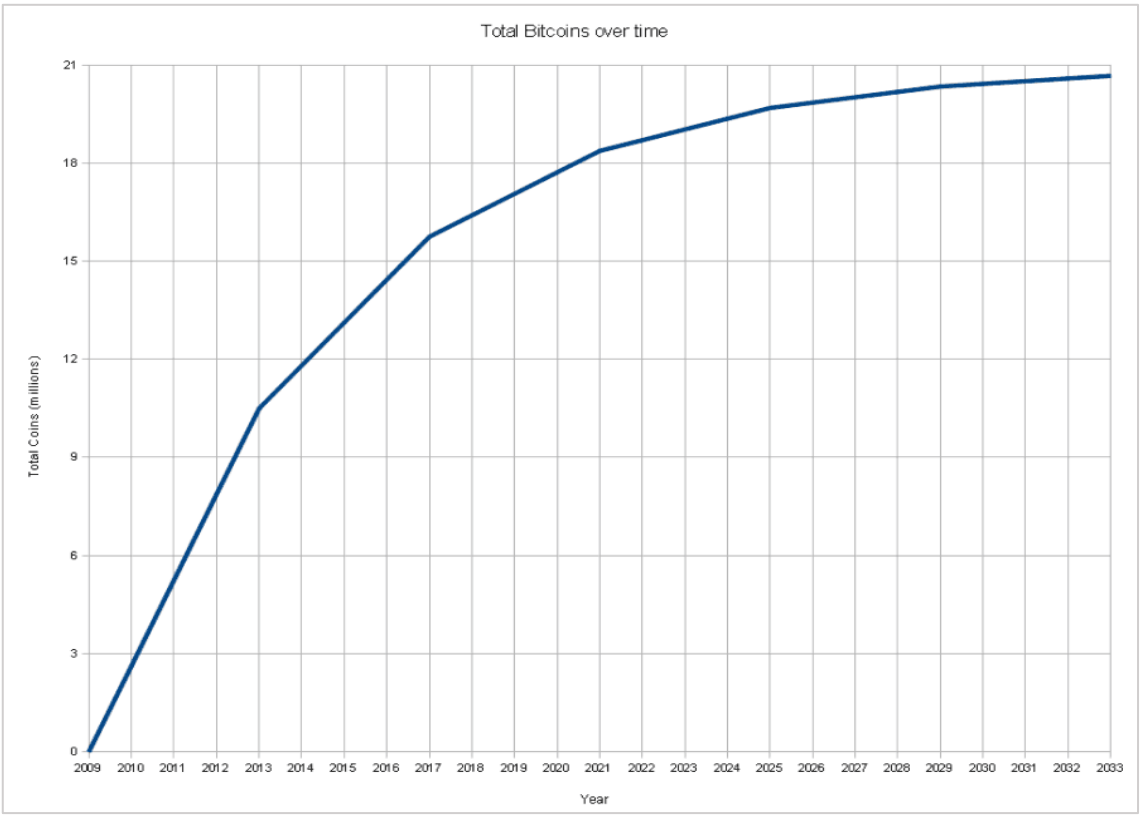


Source: Bitcoin-info.cz (2017)

3.4.3 Emission of New Coins

Bitcoin is designed to gradually reduce the number of new coins that are being added to the system. In 2009, when the Bitcoin network was launched, there were 50 new Bitcoins every 10 minutes. After 4 years, this figure has fallen by half, and since 2012 until 2016, there have been mined 25 new Bitcoins every 10 minutes. Since 2016 the network has been growing only by 12.5 Bitcoins /10 minutes. (Vigna, P. & Casey, M. 2015). Every 4-year in the future it will be divided in half. The subsequent reduction will last until 2140 when there will remain nothing to divide. However, the majority will be mined until 2030. The following chart shows how much Bitcoins will be harvested in what year. (Nakamoto, S. 2009)

Figure 5: Emission Curve of New Coins



Source: Bitcoin-info.cz (2017)

This graph illustrates the assumption of Bitcoin growth in the number of mined coins into the network. The starting year 2009 shows the releasing point of emergence and ending year 2033 depicts almost the final number of coins which will be mined until the year 2140.

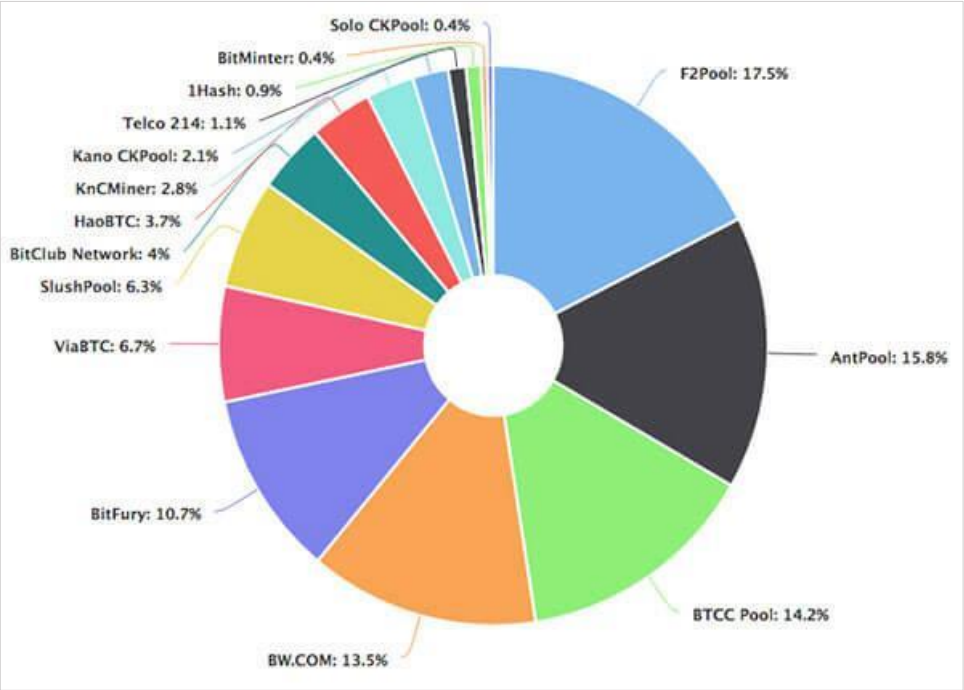
3.4.4 Pools

Due to the large number of miners in the network, the likelihood of finding the right hash above the block is minimized. Because of this reason, the miners began to join so-called mining pools where they are looking for the right hash collectively as one team. If someone finds a new Bitcoin's block, that individual shares it with other members from mining pool. The key role plays of course the performance of hardware used while mining, every member contributes with its hardware device to benefit within the pool as of team. This idea of association into mining pool was invented by with Czech programmer *Marek*

Palatinus (Slush)[6], who published this protocol as an open source. His own Czech pool is still running at *www.slushpool.com.*

According to Marek Palatinus the founder of mining pool. “There are several types of software used for mining, and for this reason it is recommended to find a pool, where individuals as part of a team can benefit, otherwise it is very tough to mine and gain some profit as an individual without the pool”. (Palatinus, M., 2010) Examples of the most powerful pools are showed below in the chart.

Figure 6: Mining Pool Examples



Source: Bitcoin-info.cz (2017)

3.4.5 Returnability

The mining problematics is closely related to returns. In these days, it is very tricky to earn by means of mining, however it is not impossible. We have to take into account initial investments into the high-performance hardware device and uncertain returns, therefore

[6] Marek Palatinus (Slush), creator of the first mining pool and TREZOR hardware wallet, architect in Satoshilabs, *www.slushpool.com.*

everybody interested in the mining should consider the possible zero profitability at least at the beginning. Generally, Bitcoin mining was widely profitable in first 4 years after its launching, even without being part of some mining pool community. Both fixed and variable costs were much less than it is nowadays. Fixed cost includes the purchase of device hardware, variable cost represents the electricity. The more difficult is to mine new coins, the more powerful hardware device is needed, and simultaneously more electricity is consumed. The most suitable locations for mining are places with low electricity tariffs and good cooling systems to protect from overheating. It is not surprising that most of the mining farms are situated in Iceland and China. (Fillner, K. 2017)

3.5 Energy Consumption

Bitcoin blockchain system employs the same protocols, like all other digital currencies. As I mentioned above the protocol runs on the energy-slurping proof-of-work algorithm. Due to still higher costs, there was created Bitcoin Energy Consumption index, which serves as an indicator to provide insight into this staggering consumption of energy amount. Another purpose of this index is to raise awareness on the unsustainability of the currently used proof-of-work algorithm (PoW). (Digicomist.com, 2017). Proof of Work system causes such costly verification, since there is no law enforcement and no control from the third party, it is needed to ensure the confidence in another way.

"PoW system consists of long benevolent nodes control (=PC's), which takes majority of computing power. This is what it makes mining so expensive. The verification algorithm PoW requires a lot of processing power thus electricity". (Nakamoto, S., White Paper, 2008)

The index is built on the premise that miner income and costs are related. Since electricity costs are a major component of the ongoing costs, it follows that the total electricity consumption of the Bitcoin network must be related to miner income as well.
After the calculating the total mining revenues, we can easily estimate how much is spent on electricity. (Digicomist.com, 2017).

Following formula explains consumption costs: W per GH/s = (price x BTC/day)/(price per kWh x 24hrday).[7]
Expenses are made in network primarily through mining (60% of overall expenses) and secondly through transactions (40% of overall expenses).

PoW system is also the part of blockchain which is being used by still increasing number of institutions namely banks. Therefore, it has been already made alternatives to PoW system to pretend such uneconomic spending and waste. (Digicomist.com, 2017).

One of the alternatives represents Proof of Stake (PoS) system. This algorithm requires miners to commit valuable resources (coins) instead of computing power (energy-hungry pc chips). PoS performs not just more reliable but mainly power saving system. Users – miners who own coins can generate new ones. In other words, the number of coins user mines depends on number of coins user possesses. Another advantage of PoS system is that it gives more price stability, since it gives users more incentive to keep the coin than to sell it. Proof of Stake system leads to higher trust between users. (Nakamoto, S., White Paper, 2008)

To sum up both systems, we can claim that PoW is based by computing power and PoS is based by coin ownership. Both systems have pros and cons, but it should be seriously considered the fact about energy consumption. There is clear distinction between effectiveness and efficiency to prevent global warming, green-house effect, power plants buy-outs, etc. PoS is not just as effective as PoW but also offers more practical conception for the future sustainability and so efficiency.

3.6 Other Digital Currencies

Bitcoin, of course, is not the only cryptocurrency in the world. Given that Bitcoin's source code is freely available, it is very easy to make a copy of it, rename it, edit a few rules, such as number of coins, mining speed, etc. Then it is just about releasing such clone into the digital world through internet.

[7] https://digiconomist.net/bitcoin-energy-consumption

Nowadays there are hundreds of currencies that have different names. We can find a list of these currencies at www.coinmarketcap.com. New currencies are created every day, but on the contrary, a lot of currencies expire each day. There are approximately around 1000 currencies in digital world, however there are just 166 “official” currencies in the real world. The biggest motivation to clone the currency is, of course, the vision of success to profit on new currency. There is a huge desire in the air to reiterate Bitcoin's success. (Coinmarketcap.com, 2017)

However, it is important to mention the fact that there are currencies that are trying to improve Bitcoin in certain ways. For example, I can mention: network acceleration, increased bandwidth, increased number of coins, increased anonymity, hash change, and so on. I picked up several currencies that are interesting the most in my opinion. They are briefly presented in the next paragraphs of the thesis.

3.6.1 Litecoin

Litecoin is one of the first alternatives to Bitcoin. The first block was mined in 2011. If we would consider Bitcoin as a gold, Litecoin could be easily compared to silver. It attempts to have faster confirmation of transaction than Bitcoin. Blocks in this case arise after every 2.5 minutes. Furthermore, the final number of coins was 4x increased from 21 to 84 million. However, the main reason for the creation of this alternative digital currency was to return the mining back to the processors of computers. The current value of Litecoin is app. **$75**, which is almost **60x** less than actual value of Bitcoin. (Investopedia, 2017)

3.6.2 Zcash

Zcash is the first open, permission-less cryptocurrency that can fully protect the privacy of transactions using zero-knowledge cryptography. A decentralized and open-source cryptocurrency provides strong privacy protections, which is the biggest advantage and differentiation from BTC. Shielded transactions hide the sender, recipient, and value recorded in the blockchain.

It can be explained the following way. Bitcoin behaves like **http**[8] for money, and Zcash represents **https**[9] to secure transport layer. Improvement over Bitcoin network is the addition of privacy. Zcash uses advanced cryptographic techniques, namely zero-knowledge proofs, to guarantee the validity of transactions without revealing additional information about them. 1 ZEC = **$245.70**, which is approximately **0.05494280** BTC. (Investopedia, 2017)

3.6.3 Ethereum

Ethereum is a cryptocurrency inspired by blockchain. Ethereum has a clearly defined creator who works permanently throughout the system. This virtual currency became public in 2015, it was introduced by Russian-Canadian programmer Vitalik Buterin. It is a shared computing platform that allows the operation with decentralized applications. It is virtual machine for running "smart contracts". (Investopedia.com, 2017)

"These smart contracts are controlled by transactions that hold information about the input data in the program. The result is then always written in a blockchain. Contracts can be replicated in order to create their own autonomous structure". (Buterin, V., 2015)

Currently the value of the currency has rocket speed of rise. The main difference from Bitcoin is the ability to create related chain applications. The Ethereum concept falls into the next generation of cryptocurrencies, sometimes referred to as "Bitcoin 2.0". (Buterin, V., 2015). 1 ETH = **$336.99**, which counts approximately **0.07490910** BTC. (Investopedia, 2017)

3.6.4 Dash

Dash is previously known as 'Darkcoin'. It is very popular currency among miners, because of used algorithm. Mining process does not overload graphic cards in such degree. The currency is also focused on anonymity. It supports the function Private Send, which mixes the same high inputs and outputs so that it is not possible to track from what place

[8] http: The Hypertext Transfer Protocol, the foundation of data communication for the World Wide Web, request–response protocol in the client–server computing model.

[9] https: The Hyper Text Transfer Protocol Secured creates a secure channel over an insecure network. It executes authentication of the visited website and protection of the privacy and integrity of the exchanged data.

and to where individual coins are sent. 1 DASH = **$307.82**, it counts approximately **0.07272290** BTC. (Investopedia, 2017)

3.6.5 Monero

Monero means coin or currency unit in Esperanto language. It was launched in 2014 and currently promises the highest possible user privacy. (Investing.com, 2017). Monero uses the technology of ring signatures. Simply, it is based on mixing the addresses of the sender in each transaction with several others, and for an external observer it is unidentifiable if the address in a particular transaction was actually used or it is only a mask. It also uses technology to hide both the amount sent and the recipient's address. All of these tools are mandatory within the network and used automatically.

In the future, developers plan to implement a tool that will hide the fact that you are using Monero currency money. This technology will send the data not through the common interface www but via decentralized I2P (Invisible Internet Project) protocol. (Investopedia.com, 2017). Nevertheless, the privacy has its price, that is why transaction fees are relatively high (around $ 10). 1 XMR = **$103.77**, it counts approximately **0.02451500** BTC. (Investopedia, 2017)

3.6.6 Ripple

The Ripple Network was established in 2012, the distinction from the most of cryptocurrencies is, that Ripple is not mined anymore. In the beginning Ripple creators have mined 100 billion coins, which have been gradually put into the circulation. Thus, it cannot be obtained by buying or donating. (Investopedia, 2017).

In contrast to Bitcoin, Ripple transactions are done by consensus. One of the advantages that Ripple has over Bitcoin is its speed. The consensus mechanism allows to carry out transactions in seconds - unlike Bitcoin transfers, which may take several minutes.

To get fiat currency into the Ripple network, we need to entrust real money to special users called Gateways. They work similarly just like PayPal[10] with the difference that PayPal is centralized entity and so less flexible in terms of supported virtual currencies. (99bitcoins.com, 2017) Because of its nature, Ripple does not have the tendency of replacing traditional currencies. However, the used payment network system has the potential to change the way of trading globally.
1XPR = **$0.197726**, which counts **0.00004696** BTC. (Investopedia, 2017)

3.7 Cryptocurrency Value Determinants

Neither banks nor governments cannot influence, whether the mining will be quicker or stopped, because digital currencies are created through worldwide network with unchangeable rules. Then there is guaranteed very low and predictable inflation, which is furthermore in constant decrease.

"Digital currencies are about the freedom and understanding the social substance of money and of course about IT. It should be noticed that the Czech Republic is strongly perceptive and influential in this problematic. The Czech Republic belong to one of the most active nation not just in comparison with the EU leading countries but also globally. The Czech Republic plays a key role in using and innovations concerting the Bitcoin". (Hubík, J., Paralelní Polis, 2016)

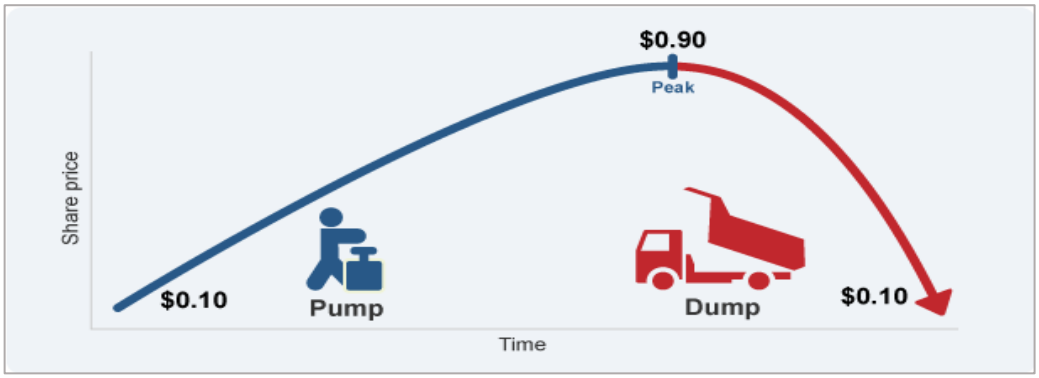
There are quite a lot of factors influencing cryptocurrencies, in this thesis I tried to achieve explanation of the most relevant drivers or determinants, which give cryptocurrency a value. Universally we can claim that all cryptocurrencies are volatile, behaving like a roller coaster, there are 3 main stages of progress: pump period, peak period, and dump period. (Bitcoin.com, 2017)

The following illustration shows the process of coin's value and its development in time. In the beginning of the graph the value of currency is optimal for the purchase, then it follows the pump period finished by the peak, where there is the highest price of currency and subsequently it falls during the dump period. These periods are repeating in cycles, but

[10] PayPal is the US company operating a worldwide online payments system that supports online money transfers and serves as an electronic alternative to traditional paper methods like cheques and money orders

generally we can claim that aggregate trend behaves like a roller coaster with incessant rising.

Figure 7: Course of Value



Source: Bitcoin.com (2017)

But what are the most significant agents, that determines the value of digital currencies in general? First of all, it is good to distinguish between objective and subjective valuation or in other words exogenous (outer) and endogenous (inner) properties. Between the built-in or dependent attributes, we can include: block reward, block times, difficulty target, mining effort, total number of coins to be mined, time since genesis the block, mining algorithm, etc. Among the relatively variable and independent variables it belongs: hash-power, market price, cost of energy, cost of production, volatility, etc. (Bitcoin.com, 2017).

On this basis, it can be implied that as mining becomes more energy efficient, the cost of production decreases and miners compete by offering lower prices in the market. Thus, the increase in difficulty counteract this tendency. When the block is mined, the reward is halved, and it also increases the cost of production. To sum up, we can claim that if the difficulty of mining increases, the cost increases as well, and the currency has a higher value.

The production includes following variables: block reward, hashing power employed by miner and the difficulty (mining effort). For example, in case of BTC, expected production per one day = **0.01076 BTC** (= $245), thus the cost of production per 1day = **$245/BTC**. According to micro economics formula, we can derive $/BTC = marginal cost/marginal product or marginal cost = marginal product = selling price. So, the price is dependent not just on the cost of production in terms of difficulty of mining but also on the cost of energy

which represent the cost of electricity. Both the mining difficulty cost and energy cost can be considered as variable costs, which are volatile in time trend. (Bitcoin.com, 2017)
There are also factors from another point of view, which have a significant share on the value of cryptocurrency. First of them and probably the most essential is limited supply.
If we want something to have a value, we must limit the supply and then the commodity can gain in its value. This would not work without the people, who drive demand and supply market forces. Willingness to pay for the coin at set price, gives the currency the value and without high demand coin loses its price.

Market forces are closely connected with usage or utility together with technology used. Assumptions to reach it include for example: the coin should be easily accepted in trade, ability to be used, stored and exchanged.
The rate of utility is connected, with the active community, the people that use it. If there are many people who have a trust into the given currency, then the coin has certain support, believe, brand loyalty and can go viral. Without the outer support, it would go nowhere. So, the bigger the community the better result in terms of valuation. Distrust into a currency is what ultimately kills it. A great community and capable developers are base stone for currency to succeed on the competitive market.

Unique features such as decentralization, anonymity, security, availability, social media platform, active admins, the whole infrastructure in general attract the interest of people to buy it against still stronger competition. This standpoint is closely related with speculation, which means the value in the future in terms of buying, selling, trading on stocks.
The rate of all digital currencies remains very volatile compared to fiat currencies, thus, speculative stock entails high degree of risk. Speculators give the liquidity on the stock market. In case of Bitcoin, the fundamental difference from fiat currencies it that trading with BTC never seizes. Bitcoin has been going on continuously for 9 years, since the network has been launched. And this network never stops it is online 24/7, in comparison with ordinary stocks. “Every 10-min there is an increment, it is like 10-min heartbeat of Bitcoin. No exchange is needed, and transactions are carried out constantly without a break, in addition there is no closing price of Bitcoin”. (Antonopoulos, A. 2015).

3.7.1 Cash or Digital

In late 1950's, a generation of computer geniuses was born. These game-changing creators include Tim Berners Lee, Bill Gates, Steve Jobs and a little know mathematician called David Chaum. It was he, the pioneer of early cryptography and the grandfather of digital cash. He proposed the idea of digital cash in 1982 as first. (Frisby, D., 2017)

The most famous digital money before Bitcoin was probably E-gold founded in 1996. The idea was about opening an account, buying some gold and then use that gold as means of payment to other E-gold account holders. The problem was that many of these accounts were operated by money-launderers and drug-dealers. It fell victim to hacking, fraud and identity theft. So, E-gold was under investigation of FBI since 2005 and by 2009, it had been shut down. (Frisby, D., 2017)

Previous systems of digital cash had in common central point of failure. They were dependent on the companies that ran them. Bitcoin is different. There is no single company that issues the coins or maintains the system. It is distributed network with no point of failure, without the presence so-called 'trusted third party'.

Since 1971, the US followed the path to fiat money, these government pieces of paper have been used less and less. In recent 10 years money in form of cash is on decline, in developed countries it has practically disappeared. Electronic banking began in early 1980's, money has become digital or electronic. Usage of electronic payment methods is not just more comfortable but also cheaper. In many countries cash represents less than 5% of money in circulation. (Hubík, J. 2017). If we have a look on developing countries and states with low trust into the finance system, we can claim that citizens still more and more tend to use digital currencies to get out of the control of state and banks. With digital era the influence and power of banks has grown. Typical features of authoritative centralized power include: absolute political and economic control over transactions, tax leakages, fraud, money laundering and other coherences connected with black economy. Cash has its good reason as a backup plan for solving in case of global disaster, but we are about to start the new era of digital banking. A Bitcoin transaction is direct, frictionless and private.

Possibilities are endless. In other words, unlike the dollars, the Bitcoin is digital cash. (Frisby, D., 2017)

4. Practical Part

4.1 Legislative Regulation

"The whole regulation should be aimed to secure cryptocurrencies and wallets on which they are stored". [11] (Charles Lee, founder of Litecoin, 2016)

From the essence of the matter we can claim that regulation typically develops much slower than innovation. The legislation cannot anticipate the technological development in advance. Thus, it responds to the newly-emerged facts subsequently with certain delay.

This is also the case of regulation of virtual currencies. In the beginning, trading with virtual currencies was like a marginal affair, but gradually as they gained in value, the circle of people who accepted them expanded. At the same time, virtual currencies became an object of interest for regulators, but unfortunately for organized crime as well.

Opinions on whether virtual currency regulation is needed and to what extent differ. Regulators claim that their uncontrolled development represents serious source of instability for the financial markets and worsening of the ability of states to operate on economic processes in the form of monetary policy. In contrast, the opponents hold the view it is necessary to act in such a way that there is no distortion of development. Since in their opinion, virtual currency has ability to change the imperfect functioning of financial markets in many ways. (Hujová, G. 2014)

Both views are possibly acceptable and future legal regulation will undoubtedly arise from a discussion between the two sides.

However, the fact is, that there is still much to be done if there is not enough or no regulation, it remains many unanswered questions together with legal statuses of entities very uncertain.

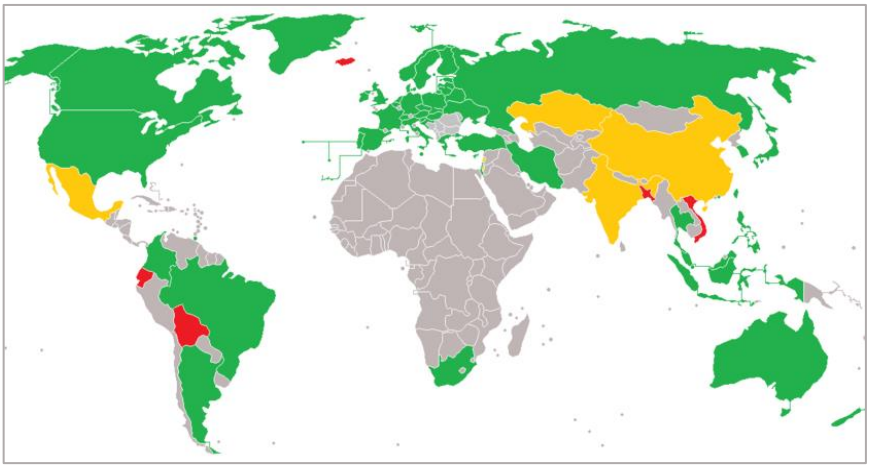
[11] Charlie Lee Litecoin Founder, 2016, https://www.investopedia.com/news/who-charlie-lee-litecoin-founder

This reality makes it difficult for virtual currencies to do any business activity, because it is not quite clear whether virtual currency usage is legal or not.

Following picture illustrates stance to virtual currency control in the world. Green colour is marked by states where virtual currency is **legal**. The yellow one marks certain **restrictions**, and the red states treat it as **illegal**. Namely countries where it is illegal to use virtual currency it belongs: **Bangladesh, Bolivia, Ecuador, Iceland** and **Kyrgyzstan**. Anybody using the virtual currency in these states can be prosecuted or even jailed. **China, Estonia, India, Indonesia, Jordan, Lebanon, Russia** and **Taiwan** represent countries where there are implemented certain restrictions while using the virtual currency. (Coindesk.com, 2017).

For example, in case of Estonia: "The Estonian Financial Intelligence Unit stated that every person who exchanges any amount of Bitcoin requires a license and that every person who trades more than 1000 Euro per months needs to be met in person, it is made and kept copy of ID of that person". (Coindesk.com, 2017). Other example denotes of situation in China: "Private parties can hold and trade Bitcoins in China, regulation prohibits financial firms like banks from doing the same". (Coindesk.com, 2017).

Figure 8: World Map of Legality/Illegality



Source: Coindesk.com (2017)

4.1.1 The EU

The European Central Bank was the first authority which started to deal with the virtual currencies in October 2012. The aim was to provide a structured point of view on virtual currencies that would remove the underlying uncertainty and created the basis for the

future discussion. The ECB has emphasized the fact that virtual currency has an impact on the financial system and therefore fall into the focus of central banks. (European Central Bank, 2017)[12]

Primary assumption of using crypto currency only within a certain virtual community however has significantly changed. With the development of a global internet network the wider groups were formed, through associated similar interests and objectives. Network gradually began to create and circulate virtual money that could be used by users from different countries and even continents.

Based on the information mentioned above, the ECB defined virtual currencies as *"type of unregulated digital money that is issued and controlled by their creators, used and accepted by members of a specific community."* (European Central Bank, 2017)[13]

Within a several years, virtual currencies, as I deal with them in this thesis with special focus on Bitcoin, have spread far beyond the given virtual community, due to its character and wider acceptance in real life. Nowadays, Bitcoin is accepted by many traders in stone stores and resemble to electronic money in certain way. For example, if the buyer makes a payment in form of bank transfer or by credit card.
The range of ideas about the nature and integration process of cryptocurrency is pretty wide. These facts together with often contrary interest of various countries still hinder to accept effective measures to regulate virtual currencies at the EU level.

The EU authorities have no doubt that the virtual currency itself is legal and regards it as a new generation of currency operated by users, but so far there have been issued documents that should serve only as a basis for the future regulation. Compared to the US, the development of virtual currency regulation in the European Union is slower due to a different political and legal environment. (Stroukal, D. & Skalický, J. 2015)

[12] https://www.ecb.europa.eu/
[13] ECB Legal Working Paper Series No 16

4.1.2 The USA

The United States of America is the most sophisticated country in the regulation of virtual currencies among all states on the world. The very first authority dealing with virtual currencies in the United States was FBI that issued a Bitcoin virtual currency report in April 2012. It expressed concerns about its potential abuse in connection with illegal activities.[14] These are later proved to be justified in case of Silk Road. Silk Road was anonymous online black market where illegal goods were freely offered. It included for example many kinds of drugs. Silk Road was launched in February 2011 and operated until October 2013, when the FBI closed its operations and arrested the owner. It was the first modern darknet market.[15] In 2014, the state Washington issued a document entitled "Virtual Currency Regulation", where it states that the virtual currencies are: "Money Transmission" in the Uniform Money Services Act.[16]

Money Transmission is understood as factual transfer of money. Thus, the state of Washington views virtual currencies as a unit for more efficient transmission money, not as a currency. Regulation in the US is under the patronage of the federal organization "Financial Crimes Enforcement Network[17] ", which regulates entities, especially exchanges that they accept or operates with virtual currencies. Above mentioned organization also regulates taxes for virtual currency, where, among other things, it is mentioned that payments in virtual currencies, stock exchange profits and operating with virtual currencies are subject to federal tax. The state that supports the most the blockchain technology in the US represents the state of Illinois, which in the year 2016 set up a group to help with the integration of blockchain technology into existing public sphere to operate more efficiently. (FinCen, 2016).

4.1.3 China

The economy of the People 's Republic of China is the world's largest in terms of absolute measure of GDP. Its specific feature is that the political and economic system is strongly

[14] Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity, 2017. https://www.fbi.gov/
[15] Maras, Marie-Helen, 2014. Inside Darknet: the takedown of Silk Road. Criminal Justice Matters.
[16] Money Services Act Summary, 2014. http://www.uniformlaws.org/
[17] FinCEN, 2016. https://www.fincen.gov/

influenced by the values from Confucianism (Kočenda, E. & Černý, A. 2015), which means it is located somewhere between centrally planned and market economy. The exchange rate of official currency yuan is permanently underestimated through the Chinese popular bank and fixed to the US dollar to favour exporters.
This situation appears to be economically advantageous in the short run. However, if there is a situation where any virtual currency gains on popularity in such an extent that traders accept it as a real currency and exchange it for goods and services, it starts to threaten the functioning of the economy. According to generally accepted opinion, exactly that was one of the main reasons why there was introduced the regulation of virtual currency in China.

China is also considered as one of the world's largest markets in cryptocurrencies. However, recently it has banned individuals and organizations from gaining funds through offering of coins. And this is probably related to the following decision of the largest Chinese stock exchange for virtual coins. The dramatic downturn from September 2017 is probably due to the announcement of the main Chinese Bitcoin stock exchange *BTCChina*[18]. It stopped all trading with Bitcoin cryptocurrency in September 2017. The central bank banned local exchanges from trading cryptocurrencies with the national fiat, the yuan. (Bitcoin.com, 2017).

4.1.4 Japan

In April 2017, Japanese lawmakers acknowledged Bitcoin as legal means of payment, and this step was also supported by large retailers in the country. It should be noted that Japan represents the second largest liquidity market for Bitcoin. (Bitcoin.com, 2017).
Japan represents the country that exceeds the majority of other states in terms of attitudes to the use of Bitcoin. In other words, if there is a country that is Bitcoin-friendly, it is just Japan.

In April 2017, Prime Minister Shinzó Abe legalized this cryptocurrency as a form of payment. At the same time there were also established special audit and security rules. In July, Japanese regulators allowed the removal of purchases via Bitcoins from 8% sales tax,

[18] BTCC, world's second largest bitcoin exchange and China's first, based in Shanghai. In September 2017 announced the suspending trading since 30 September 2017.

which got Bitcoin to the same "line" as financial products like stocks and bonds. (Cointelegraph.com, 2017).

In the country of the rising sun, the first bond denominated in Bitcoins was issued in 2017. It is a three-year bond, which is worth 200 BTC with an annual coupon of 3%. The instrument is designed as a classic corporate bond, and at the time of maturity, the owner will receive a repayment at BTC. It is concerned as the historically first deal of this character. (Roklen24.cz, 2017).

4.1.5 Russia

In the first quarter of 2017, after Japan's official acceptance of Bitcoin as a payment method, Russia has taken steps to regulate it as well. It is surprising support from Russian government, where the Deputy Minister of Finance, Alexey Moiseev, said the authorities are planning to recognize Bitcoin and other cryptocurrencies as legal financial instruments in the next year. According to Moisee, the motivation is to reduce the volume of money laundering in the country. (Cointelegraph.com, 2017).
Russian Finance Minister Anton Siluanov assured Russian users of Bitcoin and other cryptocurrencies that the government would not criminalize or penalize people for using it. It is a complete turnover of the stance of the Russian ministry after President Vladimir Putin has expressed his consensus towards cryptocurrencies. In the past, Putin encountered the founder of Ethereum, Vitalik Buterin (Cointelegraph.com, 2017), who contributed to the acceptance of blockchain technology in Russia, which creates the basis for Bitcoin.

The Russian Ministry of Finance previously rejected the use of cryptocurrencies and considered restricting them. Now, there is support from the side of Putin and the state realized that digital currencies are part of a new economic reality. Siluanov said: “There is no longer need to prohibit cryptocurrency. And as a next step it is to draw up a bill on regulating cryptocurrency sector”. (Arbolet.net, 2017).

4.1.6 Germany

Germany is probably the most important country of the European Union and thus the driving force of the EU policy, so its attitude to virtual currencies is important for the prognosis of future development. From the long-term point of view, we can claim that

Germany holds a liberal attitude towards alternative currencies. The virtual currency is in Germany defined as "Unit of account, not legal tender but a financial instrument", (BMF, 2017)[19]. According to the German Financial Market Authority (BaFin), the sale, purchase and mining of Bitcoin does not require a special license (ECB, 2017)[20]. An exception represents, for example, the commercial purchase and sale of bitcoins by own name on behalf of another person or running a trading platform. (Aschenbeck-Florange, T. 2014).[21]

According to the statement of the Federal Ministry of Finance from August 2013: "The virtual currency is not considered as electronic money or foreign currency, but private money. This financial instrument then falls under German bank rules. Private bitcoin transactions or their mediation is considered as dealing with receivables and therefore it is free from VAT". (BFM, 2013).

I would like to remain that in Germany, in comparison with other states, virtual currencies can be legally used thanks to already existing legal framework. So, the situation concerning legislative and regulation of virtual currencies is much clearer in Germany than in other the EU states

4.1.7 The Czech Republic

Trading with Bitcoins has not been legally regulated yet in the Czech Republic. No law or amendment to an already existing law has been adopted to respond to the phenomenon of crypto currency. According to statement of Chief Financial Officer and Payment Systems of the CNB: "Bitcoins do not have the character of money or electronic money in terms of medium of the exchange system". (Vodrážka, M. 2017).

According to the Czech National Bank vice governor Mojmír Hampl: Buying or selling of Bitcoins does not represent any of the payment services. The exchange of Bitcoins for the Czech crowns or other currencies is not subject to the law, exchange activities and Bitcoins also do not show the features of an investment instrument for doing business on the capital market. (Hampl, M. 2017)

[19] BMF: The Federal Ministry of Finance (German: Bundesministerium der Finanzen), http://www.bundesfinanzministerium.de

[20] ECB: European Central Bank, https://www.ecb.europa.eu/

[21] Aschenbeck-Florange, Tanja. Regulation of Bitcoins in Germany: First comprehensive statement on Bitcoins (BaFin), bitcoinmagazine.com, 2014

For the afore-mentioned reasons, trading with Bitcoin does not require permission from the CNB, it is not subject to its supervision. Furthermore, it is not obliged to inform the CNB in case of conducting of business. Trading with Bitcoin is therefore possible on the basis of a trade license falling under the activity of "Mediation of trade and services." (Arbolet.net, 2017).[22]

In January 2017, there was introduced new anti-money laundering law limiting Bitcoin. The proposed law requires the identification of customers by ID when transferring of virtual currency. Bitcoin users will no longer be able to "hide behind false names or nicknames." (Hampl, M. 2017)

Bitcoins are accepted in more than 80 places in Prague. (Vejvodová, E. 2017). Merchants who accept Bitcoins will need to register and require the customer to provide an ID card when paying in Bitcoins.

4.2 From Bear to Bull

Legislation therefore responds slowly to the dynamically evolving virtual currency industry. However, it is matter of time to be shown whether this very unstable cryptocurrency requires more detailed legal regulation.

Another country, or rather, the city that symbolizes the leadership in development and research area of blockchain technology and so cryptocurrency is Dubai. The Prince of Dubai has recently announced that he wants all government documents secured by blockchain technology until the year 2020. (Roklen24.cz, 2017).

It is obvious that this underlying blockchain technology has attracted number of states which are looking for a very safe way to store data while working with it. And this trend will most likely to continue.

"One of the things I've learned in the investing world is that very often the thing that's supposed to break an asset class is the thing that truly strengthens it."[23]

[22] https://arbolet.net/clanek/ceska-republika-predstavuje-zakon-upravujici-bitcoin

[23] Josh Brown, money manager and CEO of Ritholtz Wealth Management, www.cnbc.com, 2017

When an asset seems like it should die, but after years in the end it finds a market. Sometimes it depends not on what people need, but what they want and believe in, and still more users nowadays want just Bitcoin. Therefore, cryptocurrency enthusiasts have been fond of for years the following famous statement from Mahatma Ghandi.

"First, they ignore you, then they laugh at you, then they fight you, then you win." [24]

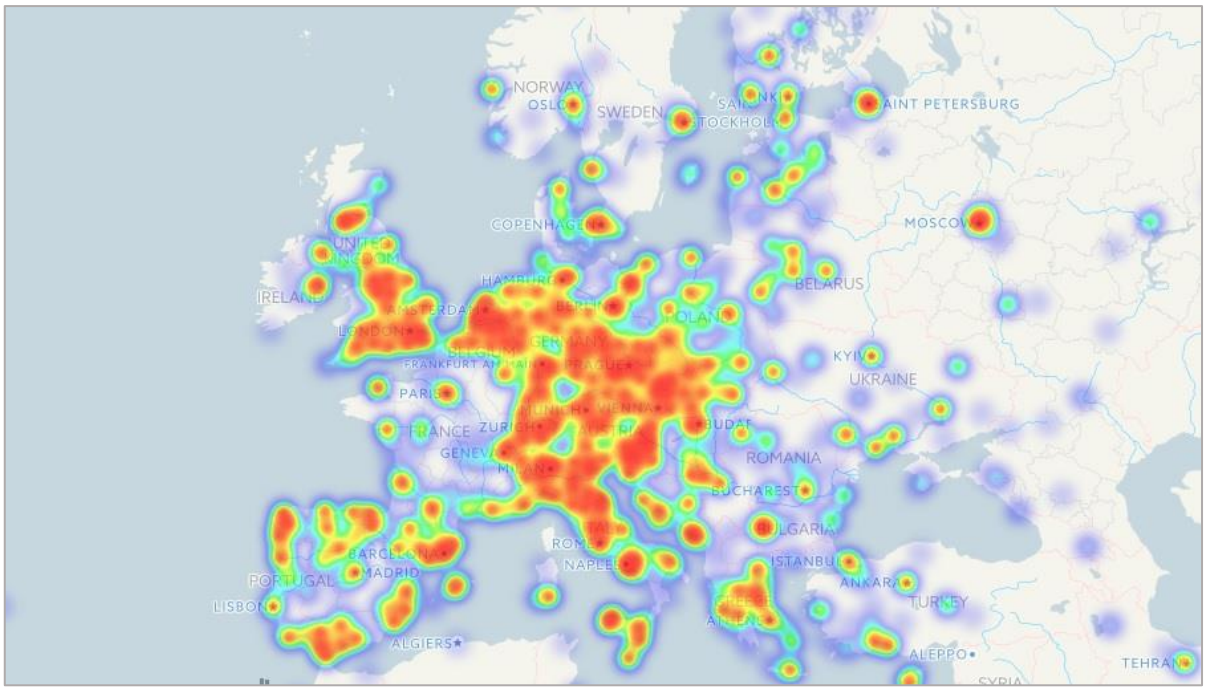
[24] Mahatma Ghandi, Indian politician, social activist, leader of the nationalist movement against the British rule of India, www.brainyquote.com, 2017

4.3 Bitcoin acceptance and distribution

The map of Europe demonstrates places where is it possible to pay with Bitcoin. The map includes Bitcoin accepting shops, ATM's & venues. All entries on CoinMap are crowdsourced: added either by users who are interested in populating the map, or by bitcoin merchants themselves. (Coindesk.com, 2018)

In my opinion CoinMap is very useful tool with minimalist interface. The navigation allows users to search and check the location they desire and to find a business that accepts Bitcoin. It is used as a kind of central map. Currently there are around 14 000 venues on all over the world.[25] (Coinmap.com, 2018).

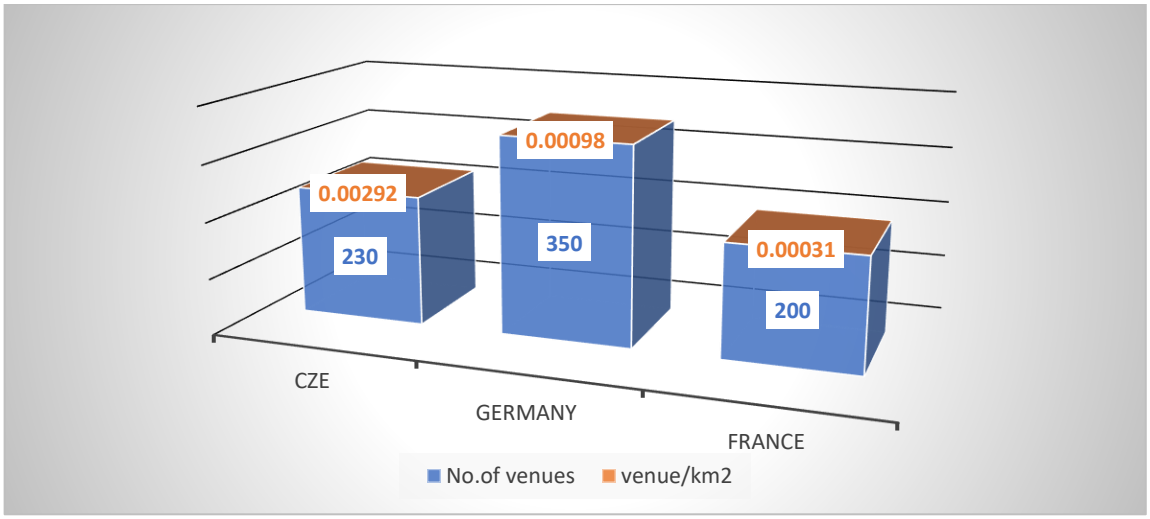
Figure 9: The EU Map of Bitcoin Accepting Venues



Source: Coinmap.org (2018)

[25] https://coinmap.org/#/world/37.89219555/17.31445313/4

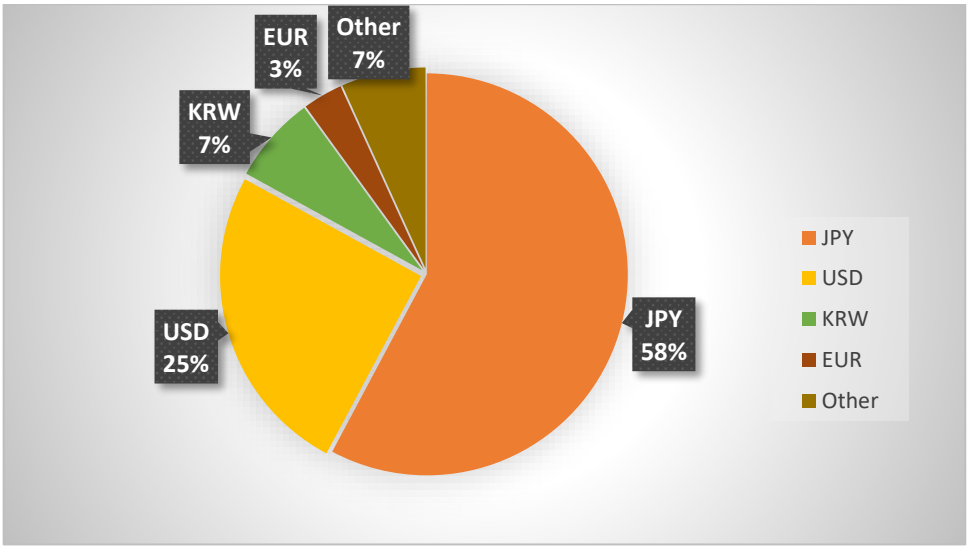
Figure 10: Number of Bitcoin Accepting Venues Related to Total Area (km^2)



Source: Own table based on data from Coindesk.com

The above shown graph illustrates the proportion of BTC venues/km^2. Despite the Czech Republic is the smallest country in terms of area, there are more venues in comparison with Germany and France. In the Czech Republic, there are currently around 230 places accepting BTC. ATM's are also included in the chart.

Figure 11: Bitcoin Volume Expressed by Fiat Currency



Source: Own table based on data from Coindesk.com

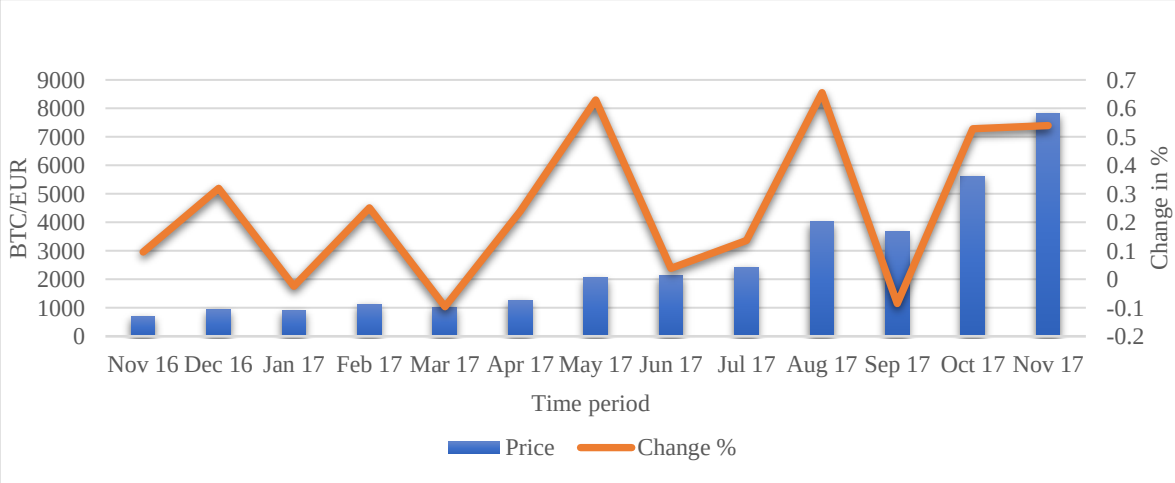
The graph shows the converting ratio between Bitcoin and selected fiat currencies. The highest share is converted from Japanese Yen (JPY). The second currency used for

purchasing of Bitcoin is the US Dollar (USD), the third biggest share represents South Korean Won (KRW) and only 3% of the total Bitcoin volume is converted from Euro (EUR). The rest app. 7% is converted from other world fiat currencies, no more specified.

4.4 Comparative Analysis of Bitcoin vs. Ethereum

The following part is focused on comparative analysis of Bitcoin and its younger brother called Ethereum, the second most spread and popular virtual cryptocurrency. Following two graphs illustrates the progress of Bitcoin and Ethereum currency during period 11/2016 – 11/2017. Vertical axis illustrates the time span and horizontal axis represents value of digital currency together with percentual change in time. Both currencies had progressive course, there is mutual correlation between them conditioned with behaviour of users.

Figure 12: BTC/EUR Price Development



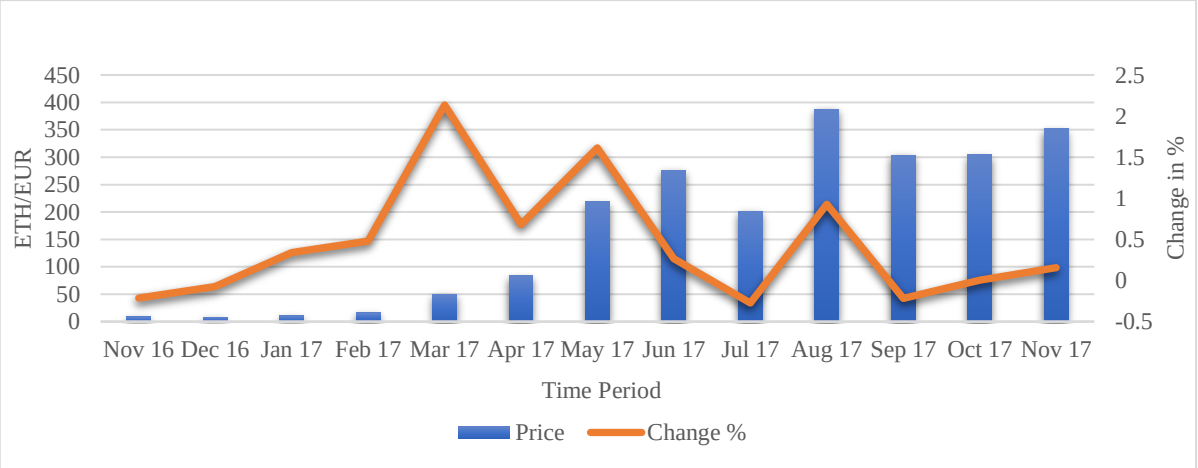
Source: Own table based on data from Investing.com

Avg. price 1 BTC = **2393.615 EUR**

Change %: **+721.1**

In 2017 Bitcoin price went through the most remarkable progress since its existence. The peak of the price showed up at the end of the year. In 2018 the price has fallen down and during the year behaves very stable in comparison with previous year. Actual rate fluctuates between 3350 EUR/BTC.

Figure 13: ETH/EUR Price Development



Source: Own table based on data from Investing.com

Avg. price 1 ETH = **170.71 EUR**

Change %: **+582.7**

Ethereum reacted with increase in value due the high demand of Bitcoin at the end of 2017. Progress was based on high credibility in the air and trigger virtual currency boom. Ethereum has got the highest rate at the same time, like Bitcoin at the end of 2017. This year it reaches generally lower values and currently it is around 200 EUR/ETH.

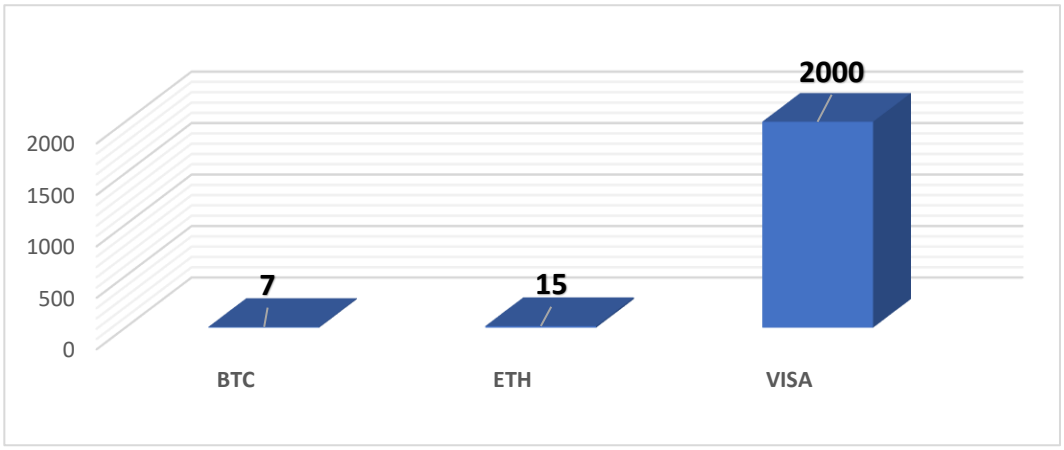
4.4.1 Transaction Costs

Virtual currency transactions have become popular due to many preferences that casual transaction does not have. Between these advantages it belongs: quickness, independency – no central authority, difficult to track the identity, which means partial anonymity, difficult to forge the transaction and last but not least irreversibility of transaction. However, there are certain negatives caused by using of virtual currency. In this chapter I focused on electricity energy consumption and related costs. I picked up three indicators as real means of worldwide daily transactions. They include transactions conducted via blockchain: Bitcoin and Ethereum and transactions via bank and Visa corporations as a mediator.

Figure 14: Number of Transactions per Second

The first graph describes number of transactions carried out every second on all over the world. It is obvious that Visa transactions are the leader. For the better understanding and seeing the difference I choose as complementary currecny Ethereum. As we can see from

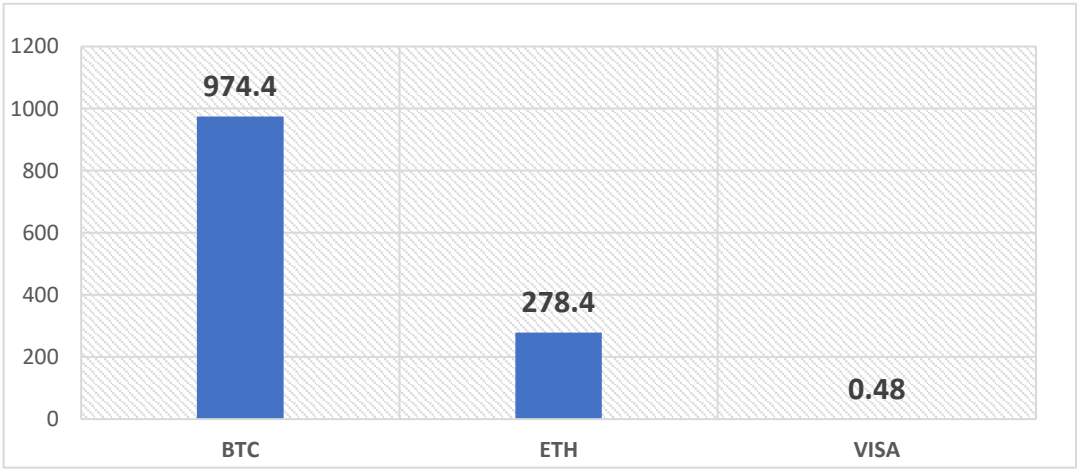
the chart below transactions of Ethereum are more frequent than Bitcoin ones. The explanation is that Ethereum transaction in blockchain is 50x times quicker than Bitcoin transaction.



Source: Own table based on data from Digiconomist.com

Figure 15: Cost per Unique Transaction (CZK)

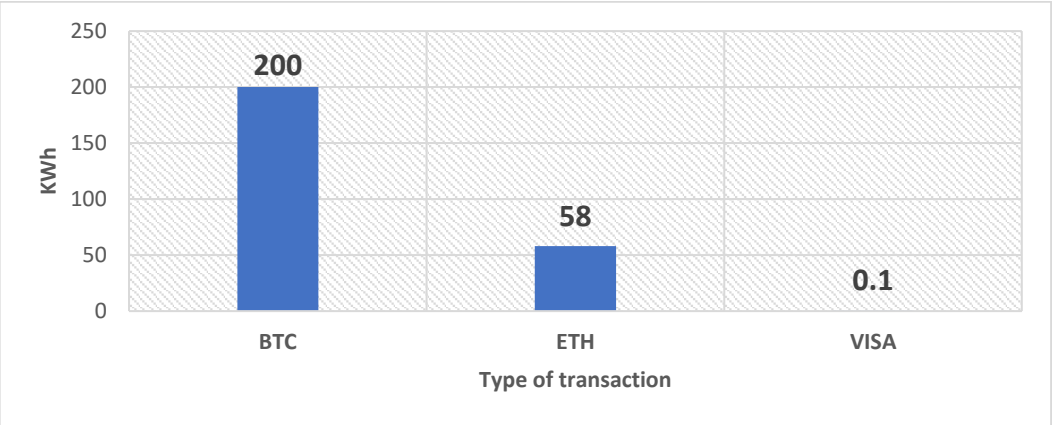
This graph shows average costs per single transaction expressed in CZK. As we can see, the Bitcoin is unambiguous leader concerning the cost per transaction. It is caused mainly by the high electricity consumption connected with running the whole blockchain.



Source: Own table based on data from Digiconomist.com

Figure 16: Estimated kWh Consumed per Transaction

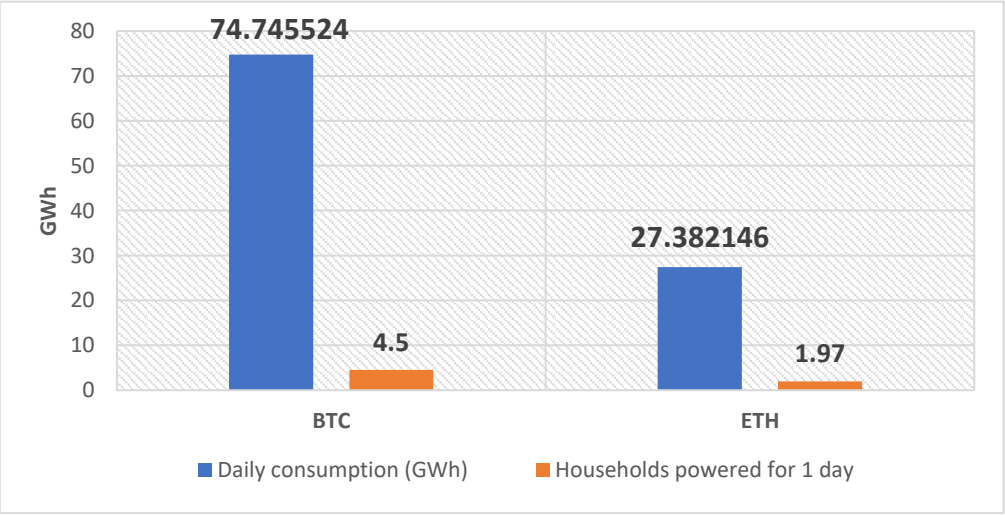
The following graph demonstrates estimated energy consumed while processing one transaction. The amount 200Wh is for better imagination such a kind of energy that modern electric cars have inbuilt in form of rechargeable battery to make a range 500miles.



Source: Own table based on data from Digiconomist.com

Figure 17: 1-Day Consumption Model

Average daily electricity consumption in 2017 makes 74.7GWh based on calculation one BTC transaction costs app. 200kWh. In 2017 the total network power consumption increased by almost 28% in comparison with previous year. The average energy consumption per unique transaction was up by around 6%. This is enough to power 1 U.S. household for almost 7 days or provide 220 washing cycles. Costs compared to revenues from mined coins are 4.5x lower, so mining is still profitable for users.



Source: Own table based on data from Digiconomist.com

Table 1: BTC Energy Consumption

Description	Value
Bitcoin's current estimated annual electricity consumption (TWh)	**27.28**
Annualized global mining revenues	**$6,209,156,808**
Annualized estimated global mining costs	**$1,364,105,812**
Country closest to Bitcoin in terms of electricity consumption	**Slovak Republic**
Estimated electricity used per day (KWh)	**74,745,524**
Implied Watts per GH/s	**0.261**
Total Network Hashrate in PH/s (1,000,000 GH/s)	**12,319**
Electricity consumed per transaction (KWh)	**203.00**
No. of U.S. households that could be powered by Bitcoin	**2,526,122**
No. of U.S. households powered for 1 day by the electricity consumed for a single transaction	**4.5**
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	**0.13%**

Source: Own table based on data from Digiconomist.com

Table 2: ETH Energy Consumption

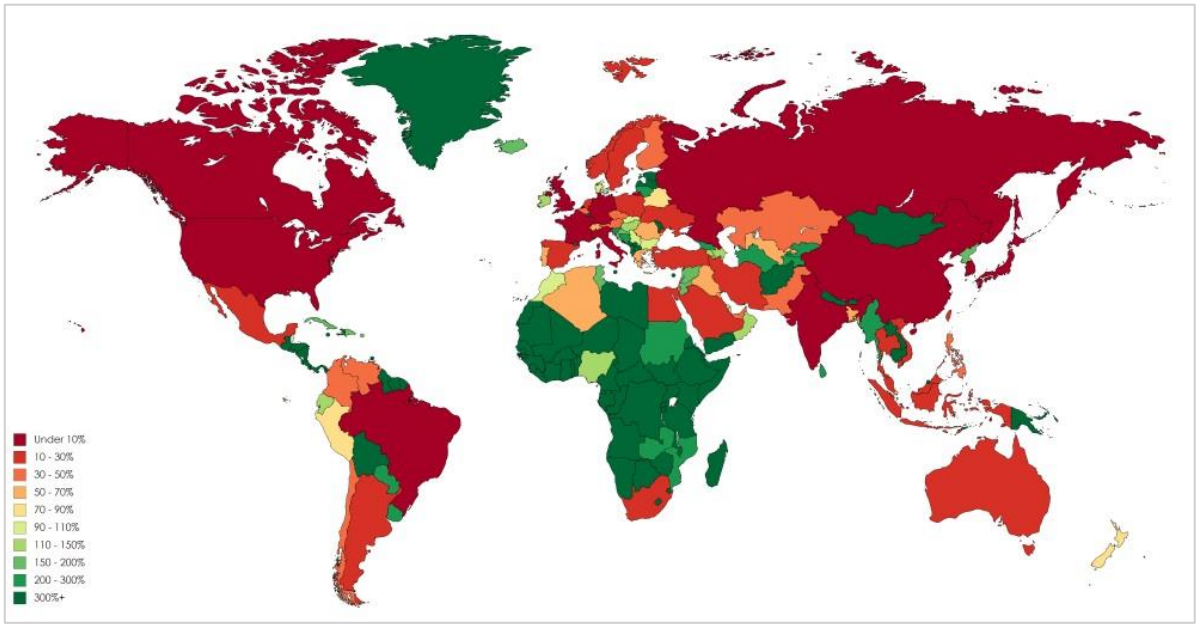
Description	Value
Ethereum's current estimated annual electricity consumption (TWh)	**9.99**
Annualized global mining revenues	**$3,588,802,930**
Annualized estimated global mining costs	**$1,199,337,998**
Country closest to Ethereum in terms of electricity consumption	**Georgia**
Estimated electricity used per day (KWh)	**27,382,146**
Implied Watts per MH/s	**10.353**
Break-even Watts per MH/s (based on 5 cents per KWh)	**30.98**
Electricity consumed per transaction (KWh)	**58.00**
No. of U.S. households that could be powered by Ethereum	**925,415**
No. of U.S. households powered for 1 day by the electricity consumed for a single transaction	**1.97**
Ethereum's electricity consumption as a percentage of the world's electricity consumption	**0.05%**

Source: Own table based on data from Digiconomist.com

These table numbers show that in 2017 Bitcoin has so far consumed as much energy as Slovak Republic. Bitcoin mining currently takes 27 times more energy than the entire global Visa network and 3 times more energy than the next largest cryptocurrency, Ethereum, which unlike Bitcoin, is actually taking steps to reduce its energy-sucking mining algorithm.

Although there are incredibly high costs while using bitcoins, still there are exceeding revenues over the losses. However, it is important to notice that these revenues go to primarily miners or mining pool communities, where there is the total profit furthermore distributed among all miners.

Figure 18: Global Bitcoin Mining Consumption Relative to Total Electricity Consumption



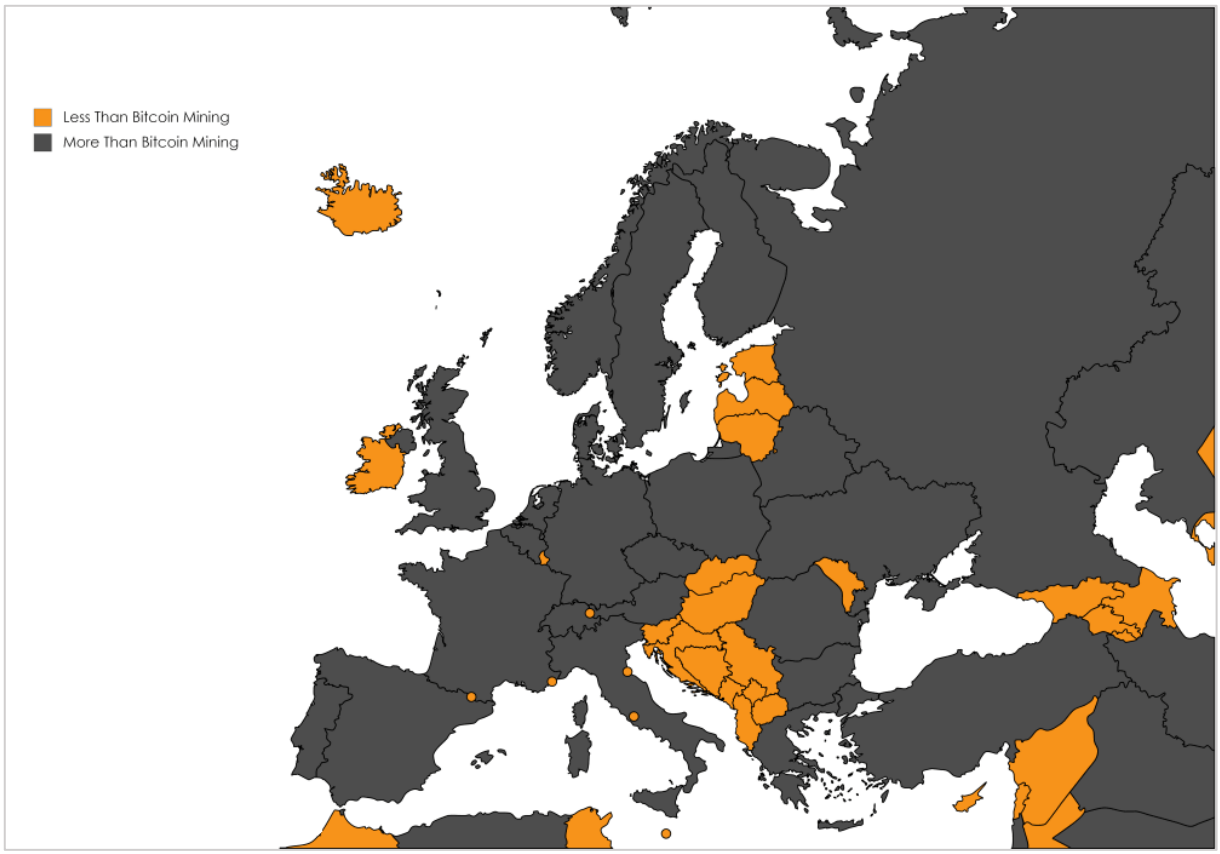
Source: Powercompare.co.uk (2017)

The map shows how much electricity countries currently consume while bitcoin mining – the computational process that keeps transactions on the blockchain relative to overall electricity consumption. If Bitcoin represented the autonomous state, it would rank 63rd place globally between Morocco and Serbia in terms of total electricity consumption.

The total volume of electricity required for mining is now using more electricity than 160 individual countries. (Powercompare.co.uk, 2017)

The map below illustrates which countries in Europe consume more or less electricity than Bitcoin network. It is indicated that this popular cryptocurrency now consumes more electricity than 20 countries in Europe. (Powercompare.co.uk, 2017)

Figure 19: European Bitcoin Mining Electricity Consumption



Source: Powercompare.co.uk (2017)

The map below shows which countries in Europe consume more/less electricity per year than the energy amount consumed by global Bitcoin mining for last 12months.

Bitcoin's energy consumption is determined by following steps: calculating total (USD) mining revenues, then estimating what part is spent on electricity, subsequently finding out how much miners pay per kWh, and finally costs are converted to consumption.

4.5 Investment Simulation

Table 3: Real Life Investment Simulation

Date	Price	Current Value when investing $1000	Bitcoins Owed	Increase/Decrease (USD/BTC)
01/12/2017	10859.56	$1,000.00	0.092084762	0
02/12/2017	10895.01	$1,003.26	0.092084762	$35.45
03/12/2017	11180.89	$1,029.59	0.092084762	$285.88
04/12/2017	11616.85	$1,069.73	0.092084762	$435.96
05/12/2017	11696.06	$1,077.03	0.092084762	$79.21
06/12/2017	13708.99	$1,262.39	0.092084762	$2,012.93
07/12/2017	16858.02	$1,552.37	0.092084762	$3,149.03
08/12/2017	16057.14	$1,478.62	0.092084762	$-800.88
09/12/2017	14913.4	$1,373.30	0.092084762	$-1,143.74
10/12/2017	15036.96	$1,384.67	0.092084762	$123.56
11/12/2017	16699.68	$1,537.79	0.092084762	$1,662.72
12/12/2017	17178.1	$1,581.84	0.092084762	$478.42
13/12/2017	16407.2	$1,510.85	0.092084762	$-770.90
14/12/2017	16531.08	$1,522.26	0.092084762	$123.88
15/12/2017	17601.94	$1,620.87	0.092084762	$1,070.86
16/12/2017	**19343.04**	**$1,781.20**	**0.092084762**	**$1,741.10**
17/12/2017	19086.64	$1,757.59	0.092084762	$-256.40
18/12/2017	18960.52	$1,745.97	0.092084762	$-126.12
19/12/2017	17608.35	$1,621.46	0.092084762	$-1,352.17
20/12/2017	16454.72	$1,515.23	0.092084762	$-1,153.63
21/12/2017	15561.05	$1,432.94	0.092084762	$-893.67
22/12/2017	13857.14	$1,276.03	0.092084762	$-1,703.91
23/12/2017	14548.71	$1,339.71	0.092084762	$691.57
24/12/2017	13975.44	$1,286.93	0.092084762	$-573.27
25/12/2017	13917.03	$1,281.55	0.092084762	$-58.41
26/12/2017	15745.26	$1,449.90	0.092084762	$1,828.23
27/12/2017	15378.28	$1,416.11	0.092084762	$-366.98

28/12/2017	14428.76	$1,328.67	0.092084762	$-949.52
29/12/2017	14427.87	$1,328.59	0.092084762	$-0.89
30/12/2017	12629.81	$1,163.01	0.092084762	$-1,798.06
31/12/2017	13860.14	$1,276.31	0.092084762	$1,230.33
01/01/2018	13412.44	$1,235.08	0.092084762	$-447.70
02/01/2018	14740.76	$1,357.40	0.092084762	$1,328.32
03/01/2018	15134.65	$1,393.67	0.092084762	$393.89
04/01/2018	15155.23	$1,395.57	0.092084762	$20.58
05/01/2018	16937.17	$1,559.66	0.092084762	$1,781.94
06/01/2018	17135.84	$1,577.95	0.092084762	$198.67
07/01/2018	16178.49	$1,489.79	0.092084762	$-957.35
08/01/2018	14970.36	$1,378.54	0.092084762	$-1,208.13
				Profit: $378.54

Source: Own table based on data from Coindesk (2018)

This table represents real life scenario simulation when investing $1000 during the time of the highest growth at the end of year 2017. In middle of December 2017 there was historically the highest value nearly $20,000 USD/BTC. The course of the price was the most remarkable during this time. The shock was caused due to future expectations of future contracts, sharp media attention and increase in number of new users, who has started investing on stock exchange. Investing $1000 in the beginning of the month would yield $378.54 profit one month later in January 2018**.**

4.6 Technical Analysis

4.6.1 Bitcoin Price Determinants

There are used time series data to analyse determinants influence on the price of Bitcoin. I collected daily data in time horizon: 09/2017 – 09/2018 of total sample size 364 observations. The data are collected from several webpage sources including Coindesk, Blockchain, and Investing. The regression analysis contains dependent variable - y and five independent variables – x_1, x_2, x_3, x_4, and x_5. All data are collected in one-year time horizon, without mathematical checking for outliers.

4.6.2 Spurious Regression

For further analysis of collected data I decided for two regression techniques: Ordinary Least Squares method (OLSM) and autoregressive integrated moving average (ARIMA) model. However, it is important to mention, that collected time series data are not stationary, which means, that variables are not casually related to each other and may provide misleading statistical evidence of linear relationship between explained and explaining variables. This kind of relationship is known as a spurious regression.

Analysis of non-stationary data can be carried out under certain transformation of data and then it can be manipulated with such data as with stationary ones. In this thesis I selected two above mentioned techniques to test the data.

4.6.3 Regression Model OLS

To estimate the relationship between the dependent and independent variables, I selected traditional regression techniques: standard OLS method using multiple linear regression together with minimizing the sum of the squared errors. Dependent explained variable represents average USD market price across major bitcoin exchanges. Independent explanatory variables include: X1: Unit Vector (constant), X2: Number of Daily Confirmed Bitcoin Transactions, X3: Miners Revenue Divided by the Number of Transactions, X4: Transaction Fees Paid to Miners, X5: Mining Difficulty (i.e. a relative measure of how difficult it is to find a new block). The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.

The analysis of relationship is presented in terms of a linear regression model. Which makes OLS assumptions to be: linear form of estimated parameters, homoscedastic - constant data variance, no autocorrelation - no covariance between error terms, no perfect multicollinearity - no correlation between explanatory variables, normal distribution of data, expected value of error term is zero and error term has finite variance, data must be independent.

Time series data are used for this analysis. Time series data is defined as one of three types of data that deals with trend analysis. Time series data means that data are in set of observations. These observations representing estimates have variable values in selected analysed time period.

Economic Model:

$y_{1t} = f(x_1, x_2, x_3, x_4, x_5)$

Econometric model:

$\beta_{11} y_{1t} = \gamma_{11} x_{1t} + \gamma_{12} x_{2t} + \gamma_{13} x_{3t} + \gamma_{14} x_{4t} + \gamma_{15} x_{5t} + u_{1t}$

Declaration of variables:

Dependent Variable:

y_{1t} …Market Price of Bitcoin USD/BTC

Independent Variables:

x_1 … Unit Vector (Constant)

x_2 … Transactions/Day

x_3 … Cost/Transaction

x_4 … Miners Revenue USD/BTC

X_5 …Mining Difficulty

Stochastic Variable: u_{1t} … Error Term

Matrix X = Constant, Number of Transactions per Day, Cost per Transaction, Revenue for Miners, Mining Difficulty. Matrix Y = Market Price of Bitcoin

Hypotheses

There are selected 4 hypotheses for testing the significance and to determine the probability if the statement is true or not. Accepting/rejecting the null hypothesis is done on basis of p-value and t-test of explanatory variable with significance level alpha 0.025 (5%). The confidence interval is 95% and it is used two-tailed test. If the p-value is smaller or equal to the alpha significance level, the null hypothesis is rejected, and alternative hypothesis accepted. This makes the phenomena statistically significant. In t-test there is compared t-value with t-table (alpha = 0.025). If t-value is higher than t-table value, it means the parameter is statistically significant.

Hypothesis 1.:

The higher the amount of transactions per day, the higher the price of Bitcoin.

Assumption: Positive sign

Reasoning: The more transactions is proceeded, the more users, attention and interest is paid, which makes cryptocurrency more valuable.

Hypothesis 2.:

The higher the costs per transaction, the higher the price of Bitcoin.

Assumption: Positive sign

Reasoning: The cost per transaction determines the order of payments in queue while processing transactions, the higher the cost per transaction, the higher priority and less time to process it. If there are lot of users which means lot of transactions in the network, there are higher costs per transaction. It is because of overloading the blockchain, that has limited capacity to verify certain number of transactions per second.

Hypothesis 3.:

The higher the revenue for miners per block, the higher the price of Bitcoin.

Assumption: Positive sign

Reasoning: If the revenue is higher for new coins, miners are motivated more to mine new ones and simultaneously keep the interest and so demand for the cryptocurrency higher.

Hypothesis 4.:

The higher the mining difficulty, the higher the price of Bitcoin.

Assumption: Positive sign

Reasoning: Increasing hash rate = difficulty makes the cryptocurrency more precious, therefore the value should have positive or at least stable trend.

Figure 20: Descriptive Statistics

	Mean	Median	S.D.	Min	Max
YMarketPriceUSDB~	8480	7688	3177	3320	19499
X1UV	1.000	1.000	0.000	1.000	1.000
X2Transactions	2.391e+005	2.159e+005	60836	1.702e+005	4.071e+005
X3CostTransaction	76.96	74.50	29.01	27.15	161.7
X4MinersRevenueU~	1.792e+007	1.506e+007	9.432e+006	6.147e+006	5.319e+007
X5MiningDifficul~	3.278e+012	3.291e+012	1.730e+012	9.227e+011	6.727e+012

Source: Gretl own computation

Descriptive Statistic processed by Gretl shows following values of data set: Mean, Median, Standard Deviation, Minimum and Maximum values of all regression variables.

Figure 21: Correlation Matrix

```
Correlation Coefficients, using the observations 1 - 364
5% critical value (two-tailed) = 0.1028 for n = 364

 YMarketPriceUS~  X2Transactions X3CostTransact~ X4MinersRevenu~                 X5MiningDiffic~
          1.0000          0.5408          0.8305          0.9619 YMarketPriceUS~  -0.2062 YMarketPriceUS~
                          1.0000          0.1292          0.6541 X2Transactions   -0.6174 X2Transactions
                                          1.0000          0.7741 X3CostTransact~  -0.0149 X3CostTransact~
                                                          1.0000 X4MinersRevenu~  -0.2925 X4MinersRevenu~
                                                                                   1.0000 X5MiningDiffic~
```

Source: Gretl own computation

Correlation matrix shows the relationship between explained and explanatory variables. It tests if there is a multicollinearity problem among explanatory variables. Multicollinearity is measured by correlation coefficient R. If there are no values higher than |0.8| respectively |0.9| between explanatory variables, there is no strong relationship between exogeneous variable and though no multicollinearity. Above calculated correlation matrix proves no correlation between X's variables.

Parameters Estimation using OLSM

Ordinary Least Squares Method (OLSM) is selected method for regression analysis while estimating the unknown parameters in a linear regression model. OLSM calculates two initial matrices: X and Y.

Matrix X = Constant, Number of Transactions per Day, Cost per Transaction, Revenue for Miners, Mining Difficulty. Matrix Y = Market Price of Bitcoin

Figure 22: Regression Outcome

```
Model 1: OLS, using observations 1-364
Dependent variable: YMarketPriceUSDBTC

                        coefficient      std. error    t-ratio   p-value
  ------------------------------------------------------------------------
  const                1571.88          456.576          3.443   0.0006    ***
  X2Transactions          0.000308481     0.00165734     0.1861   0.8524
  X3CostTransaction      21.8326          3.58222        6.095   2.83e-09  ***
  X4MinersRevenueU~       0.000274582     1.46519e-05   18.74    3.91e-055 ***
  X5MiningDifficul~       7.12560e-011    3.03070e-011   2.351   0.0193    **

Mean dependent var   8479.930   S.D. dependent var   3177.371
Sum squared resid    2.03e+08   S.E. of regression   751.3876
R-squared            0.944693   Adjusted R-squared   0.944077
F(4, 359)            1533.010   P-value(F)           3.6e-224
Log-likelihood      -2924.356   Akaike criterion     5858.712
Schwarz criterion    5878.197   Hannan-Quinn         5866.456

Excluding the constant, p-value was highest for variable 3 (X2Transactions)
```

Source: Gretl own computation

Econometric equation with parameters:

$Y_{1t} = 1571.88 + 0.000308481X_{2t} + 21.8326X_{3t} + 0.000274582X_{4t} + 7.12560e\text{-}011X_{5t} + u_{1t}$

Table 4: Regression Statistic

Multiple R	0.961975
R^2	0.944693
Adjusted R^2	0.944077
Standard Error	751,3876
Observations	364

Source: Own table based on Gretl computation

Verification of selected model

Verification of selected model answers the question whether the model is valid and representative. It is done through examination of the data and regression results. Verification is carried out by following tests and methods: the relationship between endogenous and exogenous variable, correlation matrix, t-statistic, p-value, R^2 and Durbin-Watson test.

Mathematical Verification

Mathematical verification checks the correctness of all data while estimating the parameter and during calculations. In this case the data were processed by Gretl software, so there is no need of check in mathematical calculations.

Economic Verification

Economic verification represents important part of the regression analysis.

In economic verification there are explained relations between variables together with estimated parameters. Signs in econometric equation describes positive or negative relationship between dependent and independent variables.

Table 5: Estimated Parameter Value

γ2	+ 0.000308481
γ3	+ 21.8326
γ4	+ 0.000274582
γ5	+ 7.12560e-011

Source: Own table based on Gretl computation

1. If the amount of Transactions per day increases by 1% then the price of Bitcoin increases by 0.000308481 %.
   Positive sign: **assumption confirmed**
2. If the costs per transaction increase by 1% then the price of Bitcoin will increase by 21.8326%. This is the same as the assumption.
   Positive sign: **assumption confirmed**
3. If the amount of miner revenue increase by 1% then the price of Bitcoin will increase by 0.000274582%. This is the same as the assumption.
   Positive sign: **assumption confirmed**
4. If the mining difficulty increases by 1% then the price of Bitcoin will increase by 7.12560e-011%.
   Positive sign: **assumption confirmed**

According to the regression analysis, it can be claimed that all four assumptions are fulfilled and confirmed. In other words, assumptions are in order with the economic theory

and simultaneously with calculated results. Estimated parameters fulfilled the theory requirements. The highest impact on Y_{1t} dependent variable Price of Bitcoin has X_{3t} explanatory variable Transaction Cost. The lowest impact on Price of Bitcoin has X_{5t} Mining difficulty.

Statistical Verification

Statistical significance of parameters is carried out by statistical verification. T-test outcome described in steps below is used to test the statistical significance of individual structural parameters. The F-test is used to test the statistical significance of the whole model.

Process of testing parameter significance:

1. Calculating the testing matrix
2. Calculating adjusted residual variance (adj. S_u^2)
3. Calculate the variance of estimated parameters (S_{ii})
4. Calculate standard errors of estimated parameters (S_{bi})
5. Calculate test criteria for estimated parameters based on t-values
6. Compare calculated t-values with tabulated values of t-test at a significance level of selected number of degrees of freedom

H_0: $\gamma = 0$ Parameter is statistically significant (SS)

H_1: $\gamma \neq 0$ Parameter is not statistically significant (SI)

Table 6: Testing for Statistical Significance

Variable	Coefficient	S.E.	t-ratio	p-value	95% lower bound	95% upper bound
Constant	1571.88	456.576	3.442	0.0006	673.978	2469.78
X2	0.000308481	0.001657	0.186	0.8524	-0.00295084	0.00356781
X3	21.8326	3.58222	6.095	2.83E-09	14.7879	28.8774
X4	0.000274582	1.47E-05	18.740	3.91E-55	0.000245768	3.03E-04
X5	7.13E-11	3.03E-11	2.351	0.0193	1.17E-11	1.31E-10

Source: Own table based on Gretl computation

Table 7: T-ratio vs. Critical T-table Value

t-value	3.442	0.186	6.095	18.740	2.351
t-tab (α = 0.05)	1.967	1.967	1.967	1.967	1.967
SS / SI *	**SS**	**SI**	**SS**	**SS**	**SS**

** SS - parameter statistically significant, SI - parameter statistically not significant.*

Source: Own table based on Gretl computation

Statistical verification is based on t-value at selected alpha level of 0.025 (5%). The t-table value is equal to 1.967. It can be claim that parameters X_1, X_3, X_4 and X_5 are statistically significant. Because the t-value of parameter is higher than selected t-table value. And simultaneously it means that parameters X_2 is statistically insignificant.

Figure 23: R^2 – Coefficient of Determination

```
R-squared          0.944693   Adjusted R-squared   0.944077
```

Source: Gretl own computation

Coefficient of determination or Goodness of Fit described how well the explanatory variable explains the variance of dependent variable. **R^2 = 0.944693** which means that the price of Bitcoin is described from 94.4693%. In other words, the explained value between observed and expected values is close to 1. This means, the discrepancy is very low, and theory matches the real data points, 94.4693% of variance of Y is explained by selected X variables. Adjusted R-squared = 0.944077 explains the price of Bitcoin, in case we would add another explanatory variable.

Testing for autocorrelation

Autocorrelation, a.k.a. serial correlation, which is the correlation of a series of data with its own lagged values. It is a violation of the independence assumptions that commonly occurs when data are taken over time. This tells us whether the observations are dependent on their lagged or future values. Autocorrelation is tested by Durbin-Watson test for 1st order autocorrelation. And by Breusch – Godfrey test for higher orders of autocorrelation.

Durbin-Watson Test statistic:

H0: $\rho \leq 0$, no autocorrelation in the model

H1: $\rho > 0$, autocorrelation in the model

DW statistic close to interval <1.8-2.2>: p = 0, no autocorrelation

DW statistic close to interval <0-1.8>: p > 0, positive autocorrelation

DW statistic close to interval <2.2 – 4>: p < 0, negative autocorrelation

Figure 24: DW Test

```
Durbin-Watson statistic = 1.08104
p-value = 1.21024e-016
```

Source: Gretl own computation

From the results calculated above it can be seen, that DW Statistic is not close to 2. So, there is present autocorrelation in the model. Number 1.08104 is in interval <0-1.8>, so there is positive autocorrelation detecting the first order autoregression.

Testing for heteroscedasticity

Heteroscedasticity means that the variance is not constant in time and so residues are greater in time. It is often caused due to structural changes in economy, dynamic change of external conditions, and so, higher inaccuracy in prediction the future data. Testing for heteroscedasticity is done using White Test – to test whether the estimated variance of residues is dependent on the values of the explanatory variables. It can be also used Breusch-Pagan Test to examine whether the square residues are dependent on the explanatory variables and constant in time.

White's Test statistic:

H_0: p >0.05, no heteroskedasticity in the model

H_1: p<0.05, heteroskedasticity in the model

Figure 25: White's test

```
White's test for heteroskedasticity (squares only)
OLS, using observations 2017-08-08:2018-08-06 (T = 364)
Dependent variable: uhat^2

                        coefficient       std. error     t-ratio  p-value
  ---------------------------------------------------------------------------
  const                  -3.23346e+06      1.93746e+06   -1.669   0.0960  *
  X2Transactions          18.5074          11.8044         1.568   0.1178
  X3CostTransaction    55837.4           19464.2           2.869   0.0044  ***
  X4MinersRevenueU~       -0.174154         0.0533059     -3.267   0.0012  ***
  X5MiningDifficul~        7.45353e-08      3.24891e-07    0.2294  0.8187
  sq_X2Transactions       -2.40463e-05      2.03757e-05   -1.180   0.2387
  sq_X3CostTransac~     -211.495           93.6734        -2.258   0.0246  **
  sq_X4MinersReven~        2.51369e-09      7.68357e-010   3.272   0.0012  ***
  sq_X5MiningDiffi~        0.00000          0.00000       -0.3190  0.7499

  Unadjusted R-squared = 0.085280

Test statistic: TR^2 = 31.041952,
with p-value = P(Chi-square(8) > 31.041952) = 0.000138
```

Source: Gretl own computation

Calculated results from White's test shows the p-value is lower than alpha value 0.05. Therefore, H_0 is rejected and H_1 accepted, which tells us the model is not homoscedastic, so there is present heteroscedasticity in the model.

Results from above calculated tests proved that parameter estimates do not fulfil the conditions for best linear unbiased estimates (BLUE).

Regression Model ARIMA

The second method for regression analysis I selected model of ARIMA. The abbreviation stands for Autoregressive Integrated Moving Average, it is appropriate model for time series analysis. The model represents a generalization of AR-MA model which means autoregressive moving average. Both models fit to time series in order to better understand the data and predict future points through forecasting. ARIMA consists of three parts: autoregressive (AR), integrational (I) and moving averages (MA). First part can be explained as linear combination of previous values, in other words regression on itself with p lags. So, it is denoted with letter ''p''. Second part represents the difference of time series before the application of the model AR and/or MA. Integer number of integration part is signed with letter ''d'' and means the level of differentiation. The third part expresses the time series residues and can be explained as linear combination of previous

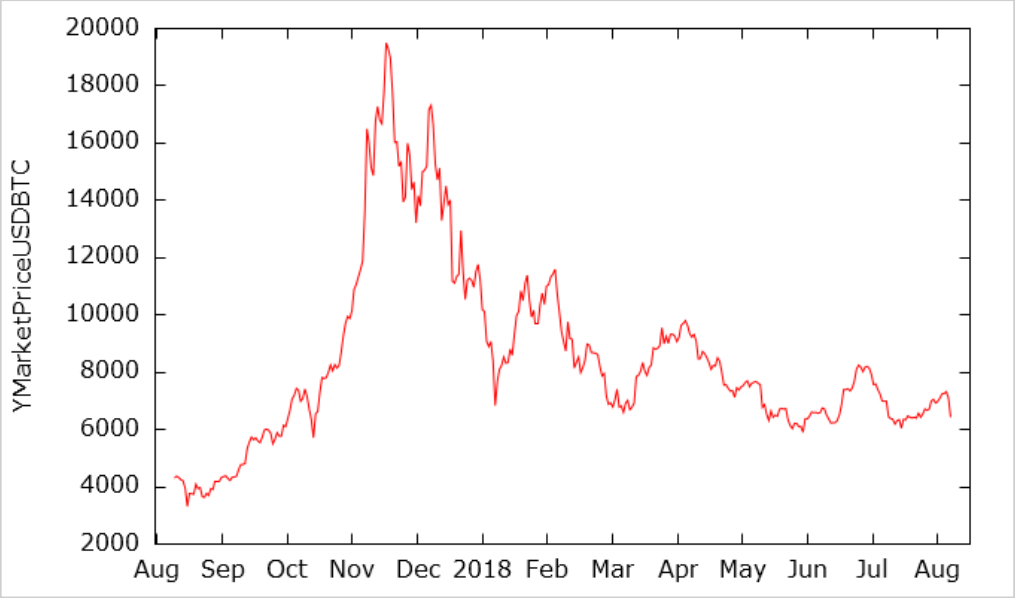
mistakes. Integer number of MA is signed with letter ‘’q’’ and tell us how many time series intervals from past will be used in the model.

All in all, the analysed time series model in this thesis contains all 3 parts (p, d, q), so it can be used the sign ARIMA.
Autoregressive models of time series are based on fact that every value in time series is in relation (dependency) with previous valued of the series. It is called stationarity of time series. In other words, the character of stationary time series is constant in the time and has constant statistical properties—mean, variance, autocorrelations, etc. Thus, it has also no trend and no heteroscedasticity. However, time series data in this cryptocurrency analysis is in non-stationary form. Time series data change non-systematically, with random character and create also White noise. The random process connected with dynamic behaviour of non-stationary data. White noise is caused by fluctuations which do not have recognizable character. It means that the probability distribution is not constant in time and changes randomly. Non-stationary data is difficult to estimate, they are hardly predictable.

ARIMA models are used for non-stational time series in forecasting, prediction of behaviour and trend analysis of selected dependent variable. ARIMA models recalculate non-stationary data into ‘stationarized’ regression models that use lags of the dependent variable as regressors. Models can be stationarized by transformations such as differencing, logging, and or deflating. All these processes are made by ARIMA modelling.

First of all, it is needed to identify the model. It is done by autocorrelation and partial autocorrelation function. The aim is to reveal existence of possible identification point k0. It is the value, in which autocorrelation function is zero. Or there is no such point and the value does not exist. Behaviour of autocorrelation function gives us clue, what type of model it is appropriate to use for selected time series.

Figure 26: Time Series Trend of Bitcoin Price



Source: own processing in Gretl

Trend is function of time, it reflects in long term changes in course of time series.
It is caused due to present forces having the impact on time series in one direction.
Time series plot shows, that the data fluctuate remarkably in time, so there is significant variance. It leads to conclusion that the null hypothesis will be accepted. In other words, alternative hypotheses will be rejected, which means it can be assumed there is a Unit Root.
To test and prove the null hypothesis with presence of Unit Root in this time series, it is used the Augmented Dickey Fuller Test, also signed as ‘’ADF’’.
Time series data in this case include constant and time trend, furthermore they are non-stational and non-seasonal type. This fact leads to conclusion that it is used ARIMA model p, d, q. Furthermore, it can be predicted there is a unit root present in analyses time series data. To test the prediction whether the null or alternative hypothesis will be accepted it is used already mentioned Augmented Dickey Fuller Test, Autocorrelation and Partial Autocorrelation Function.

The Unit Root test hypothesis:
H_0: Unit Root
H_1: No Unit Root

If there will be accepted null hypothesis, there is a unit root present, data fluctuate randomly without recognizable patterns, the variance is significant. They are not constant and non-stationary. If the null hypothesis will be rejected and alternative accepted, there is no unit root meaning that data are constant or stationary and variance is not so high.

Hypothesis is tested by calculating Augmented Dickey Fuller Test, Autocorrelation Function and Partial Autocorrelation Function.

Figure 27: Augmented Dickey Fuller Test

```
Augmented Dickey-Fuller test for YMarketPriceUSDBTC
testing down from 16 lags, criterion t-statistic
sample size 347
unit-root null hypothesis: a = 1

  test with constant
  including 16 lags of (1-L)YMarketPriceUSDBTC
  model: (1-L)y = b0 + (a-1)*y(-1) + ... + e
  estimated value of (a - 1): -0.0167302
  test statistic: tau_c(1) = -1.85416
  asymptotic p-value 0.3545
  1st-order autocorrelation coeff. for e: 0.011
  lagged differences: F(16, 329) = 4.093 [0.0000]

  with constant and trend
  including 16 lags of (1-L)YMarketPriceUSDBTC
  model: (1-L)y = b0 + b1*t + (a-1)*y(-1) + ... + e
  estimated value of (a - 1): -0.0195648
  test statistic: tau_ct(1) = -2.13857
  asymptotic p-value 0.5236
  1st-order autocorrelation coeff. for e: 0.011
  lagged differences: F(16, 328) = 4.069 [0.0000]
```

Source: own processing in Gretl

Table 8: Test Statistic of ADF

Test statistic	-1.854	-2.138
Critical t-table value	-3.43	-3.43
SS/IS	**IS**	**IS**

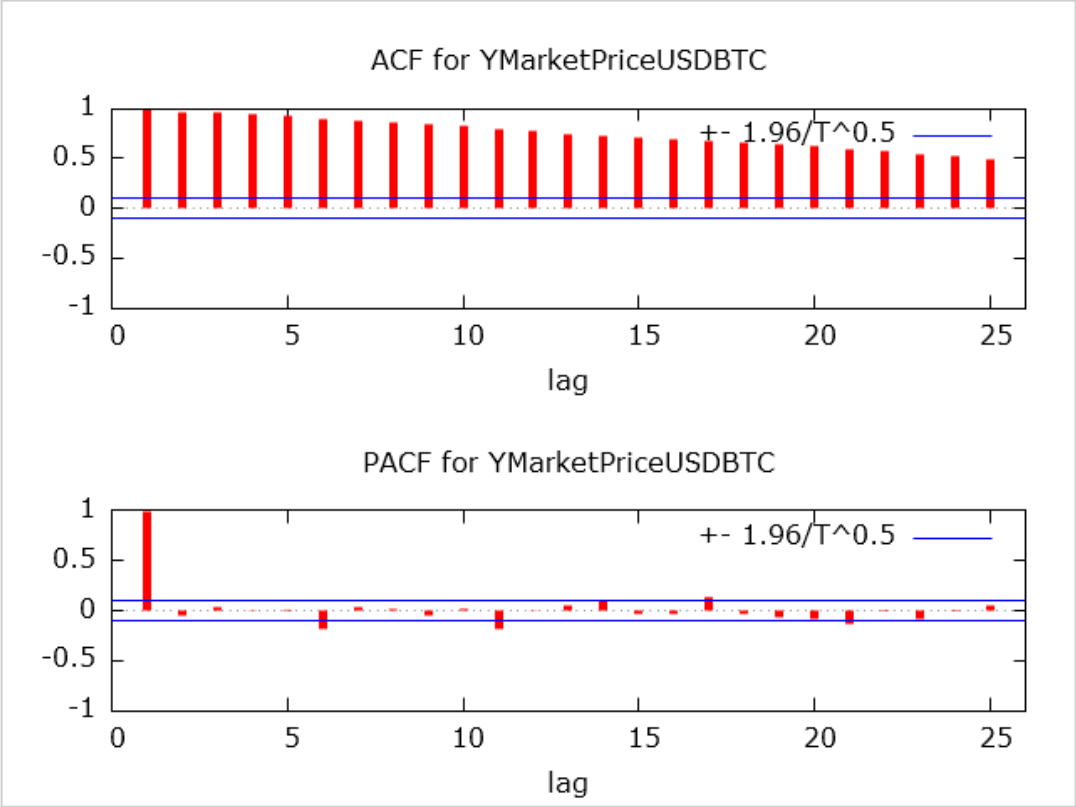
Source: Own table based on Gretl computation

Results of ADF test show test statistic values to be higher than critical values for Dickey-Fuller Unit Root t-Test Statistic at significance alpha level 0.05. Critical Values for the

Dickey-Fuller Unit Root T-test Statistics in 95% probability to the right of critical value equals 3.43. So, at the 95 per cent level the null hypothesis of a unit root will be accepted.

The Unit Root of time series proved to be present and parameter ‘’d’’ in ARIMA model needs to be transformed into first difference to solve problem of non-stationarity of the data.

Figure 28: Autocorrelation and Partial Autocorrelation Function



Source: own processing in Gretl

Choice of model structure is based on empirical comparison of autocorrelation function (ACF) and partial autocorrelation function (PACF) with their theoretical models, assuming comparison of random processes. There is certain coherence between the shape of ACF, PACF function and the identification of the model.

In ACF the exponential function is gradually decreasing and closing to zero. It signs model AR (p). In the determination of order for p it is used ACF, which equals to 1 in the first lag. In PACF there is just one peak and rest are insignificant or zero. It signs model MA (q) equals 1. The I for "integrated" determination of order for d, it responds the delay value,

since which the partial autocorrelation function is insignificant or zero. According the PACF graph, the order of d equals 2. So, the time series needs the data to be differenced second time. In other words, to obtain stationary time series properties it is desired second order differencing of data. All values besides the first peak in PACF are insignificant or close to zero, therefore we can assume it as random data which naturally generate White noise.

To sum up, by estimation of ACF and PACF it is obtained ARIMA 1-2-1 model.

Equation for ARIMA 1-2-1 model: $Y_t = rY_{(t-1)} + Y_t - 2Y_{t-1} + Y_{t-2} + ae_{(t-1)}$

r …… the autoregressive parameter

a ……the moving average parameter.

e_t ……the pure error term at time t.

$Y_t = rY_{(t-1)}$ …….. p = 1

$2Y_{t-1} + Y_{t-2}$ ……. d = 2 (second difference)

$ae_{(t-1)}$ ……. .q = 1

The goal of the construction of the p-d-q model is to find the simplest possible model, which suitably describes the dynamics. Because increasing of the orders does not usually lead to models with better results. Thus, simpler models are more reliable and desired than higher order ones.

Figure 29: ARIMA Time Series Model

```
Model 4: ARIMA, using observations 2017-08-10:2018-08-06 (T = 362)
Estimated using AS 197 (exact ML)
Dependent variable: (1-L)^2 YMarketPriceUSDBTC
Standard errors based on Hessian

             coefficient   std. error      z       p-value
  ---------------------------------------------------------
  const      -0.286039     0.277678       -1.030   0.3030
  phi_1       0.0705867    0.0525595       1.343   0.1793
  theta_1    -1.00000      0.00883015   -113.2     0.0000  ***

Mean dependent var  -2.056925   S.D. dependent var   705.8668
Mean of innovations  2.257171   S.D. of innovations  515.5635
Log-likelihood      -2777.317   Akaike criterion     5562.633
Schwarz criterion    5578.200   Hannan-Quinn         5568.822
```

Source: Gretl own computation

The above figure shows calculated ARIMA model for analysed Bitcoin time series Calculated results include following terms:

constant……...intercept parameter

phi_1……...the nonseasonal first-order autoregressive parameter

theta_1……the nonseasonal first-order moving average parameter

Table 9: Testing of Statistical Significance

Coefficient value	-0.2860	0.0705	-1.0000
p-value	0.3030	0.1793	0.0000
SS/SI*	**SI**	**SI**	**SS**

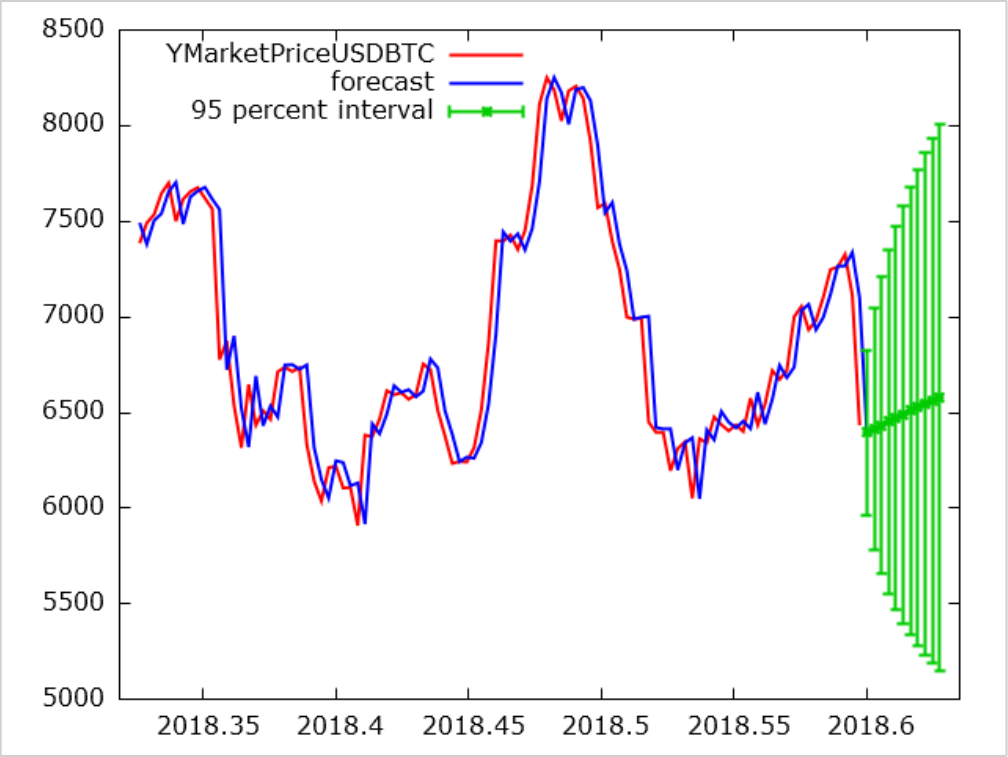
** SS - parameter statistically significant, SI - parameter statistically not significant*

Source: Own table based on Gretl computation

The table shows time series coefficient values and p-values. By comparing calculated p-value and significance level alpha 0.05 it is determined statistical significance of terms. If the calculated p-value equals less than 0.05, it means there is statistical significance and coefficient value is determined.

MA (q) term has a p-value that is less than the significance level of 0.05. It can be concluded that the coefficient for the moving average (MA) term is statistically significant, and it is recommended to keep it in the model.

Figure 30: Time Series Forecasting



Source: Gretl own computation

The graph above indicates forecasted 10-point period out of the sample. Prediction is based on alpha level 0.05 with 95% confidence interval. There are generated: forecast of time series in blue, actual values of dependent variable (Y_t - Price of Bitcoin) in red. The 95% confidence interval is shown in green. It can be supposed with high confidence that price value of Bitcoin is likely to be within the green range. The forecast is based on pre-forecast observations from collected data.

Figure 31: Real vs. Predicted Time Series Values

2018-07-29	7054.28	7032.76	
2018-07-30	6932.66	7065.56	
2018-07-31	6981.95	6932.65	
2018-08-01	7100.95	6996.72	
2018-08-02	7247.94	7118.56	
2018-08-03	7260.95	7265.42	
2018-08-04	7326.85	7266.82	
2018-08-05	7113.07	7337.21	
2018-08-06	6433.27	7102.49	
2018-08-07		6395.24	513.382
2018-08-08		6414.87	751.809
2018-08-09		6434.21	926.077
2018-08-10		6453.24	1068.20
2018-08-11		6471.97	1189.87
2018-08-12		6490.42	1296.96
2018-08-13		6508.58	1392.93
2018-08-14		6526.47	1480.02
2018-08-15		6544.07	1559.81
2018-08-16		6561.41	1633.44
2018-08-17		6578.47	1701.77

REAL **PREDICTED**

Source: Gretl own computation

The comparison table shows in the first column the time period, the second column represents real values, third one shows predicted values and the last one is calculated standard deviation. The amount of variation or dispersion in analysed set of data is increasing in time, so the confidence intervals are getting wider on the y-axis. The predicted values are less accurate with every next forecasted point. It is caused by the character of data, since they have random behaviour, non-stationary, no constant origin.

5. EVALUTION OF RESULTS AND DISSCUSION

5.1 Fundamental Analysis Evaluation

One of the biggest threads to Bitcoin is its regulation. The Czech Republic represents the country with stable and convenient conditions for accepting Bitcoin as a legal means of payment. There no remarkable changes and regulations against cryptocurrency. The situation quite opposite is in Mexico, India, South Korea, China and Japan. These countries have regulated market with cryptocurrencies and what is more transactions can be suspended and virtual accounts 'frozen'. The highest level of protection is in Bangladesh, Bolivia, Ecuador, Iceland and Kyrgyzstan. The cryptocurrency is recognized as illegal and its use can be prosecuted. The EU stance is quite positive, there have been issued changes in directives and regulations to prevent money laundering and financing of terrorism. From the side of virtual stock markets and electronic wallets it is required to identify suspicious activities.

Generally, it can be concluded that markets suffer from the regulations and react with the decline. This fact is important to consider when deciding the investment strategies.

Acceptance of Bitcoin is low in comparison with fiat currencies. Places where it is possible to pay in Bitcoin are slowly increasing worldwide. The main reason why it is so rests in users primarily the trust. Bitcoin is still more perceived as market commodity from society. The Czech Republic represents unique example of very rich network of places where it is possible to pay in Bitcoin. It is kind of Bitcoin heaven because of the strong local community. According to Coinmap.org Prague has even more places with Bitcoin acceptance than Paris or London. Bitcoin is accepted mainly in restaurants, cafe and bars. There are several examples of large companies and retail chains which accept Bitcoin as one of payment methods: Alza, Bloomberg, Foodler, KFC Canada, Microsoft, Playboy, Virgin Airline and Subway.

Two the most popular and frequently used digital currencies Ethereum and Bitcoin have closely related price. They mutually adjust their values. But without the very first and corner stone cryptocurrency Bitcoin it would be probably no other successful cryptocurrency yet. It also means that everything it dependents on Bitcoin.

Ethereum is not an exception. Even if it is technically more sophisticated. Bitcoin sets the pace and runs the stock market price.

Remarkable part associated with Bitcoin is its mining costs. In other words, electric electricity consumption in terms of running highly powerful devices designated to mine. In these days the most favourable country for mining is in Venezuela, because local government subsidizes the electricity and mining of 1 BTC equal the costs around 11 000 CZK. In comparison with the Czech Republic, where it counts approximately 140 000 CZK to cover costs to mine 1 BTC. Luckily the blockchain world network is quite small so the costs are still sustainable. If we compare it with bank online transaction processing and all activities associated it would be definitely more expensive.

5.2 Technical Analysis Evaluation

Technical analysis is performed by regression analysis. Bitcoin represents time series data of non-stationary type. So, it is not genuine regression but so called spurious. Because of this reason time series data are modified and then used in regression and autoregression analysis.

The results of the calculated models are following. Ordinary least square method proved the strongest influence on price of Bitcoin has the transaction cost, represented by variable x_3. Economic verification was positive in all cases and so initial assumptions were confirmed. Statistical significance was confirmed in all independent variables except variable x_2. Coefficient of determination explained the variation of the model from 94.46%. Which means that the model is explained with high accuracy. The model can be used for further simulation and investigation.

Another part of time series analysis deals with autoregressive integrated moving average. ARIMA model serves to forecast collected time series data. As mentioned above the analysis data are non-stationary which means dynamic and not constant in time. Arima transforms the data by differencing in conjunction with nonlinear transformations such logging into stationary character. Under these conditions statistical properties of data are constant in time.

ARIMA model is used as a filter separating the indication from the noise to obtain the forecast. Forecasting equation includes the predictors made of lags of the dependent variable, in this case the price of Bitcoin and simultaneously lags of the forecast errors. ARIMA model was classified as p-d-q model with value of terms 1-2-1. Number of

autoregressive terms representing letter p equals one. Number of nonseasonal differences needed for stationarity represented by letter d is two. Number of lagged forecast errors in the prediction equation signed with letter q equals one. The forecasting equation contains differenced second-order autoregressive model. There is used first-order difference in constant and simple exponential smoothing. In case of nonseasonal difference it is used second order difference. This is good result, because the goal is to construct the model with the lowest possible order.

Selected model proved the null hypothesis, in other words, the presence of unit root was verified. Statistical significance testing of ARIMA was confirmed in term q. The analysis has come to the conclusion that the coefficient of moving average is statistically significant and can be used for the prognoses.

It is a question whether Bitcoin should help to solve problems of fiat currencies, dependency on banks, governments or whether they rather should serve its mysterious founder Satoshi Nakamoto. Although, the basic idea seems to be brilliant, in my opinion the very first and original intention was not about to help the world economy, but rather to help the founder. It is like a magic at the expense of others. Though Bitcoin has independency and freedom compared to fiat currencies, the stability is still in the stars, so it is dependent more on its users and their mutual confidence.

6. CONCLUSION

Bitcoin remains very controversial topic. There are two opposite corners. One occupied by sworn enthusiasts admiring this virtual currency as digital gold and back-up plan in nowadays financial bank system. Against this group there are traditionalists defaming its sophisticated properties and claim that Bitcoin represents a thread for current financial system. To the first one group of Bitcoin fans belong for example the Winklevoss twins. Famous American brothers, former rowers and famous from Facebook authorship affair. Next one is John McAfee guru on internet security, Jim Cramer well-known host of CNBC, Tommy Lee the main analytic of company Fundstrat Global Advisors. Last but not least, Richard Branson, Bill Gates, Elon Musk, Warren Buffet expressed they feel confident particularly with the technology of blockchain. On the other side there are famous capacities in this branch like Joseph Stiglitz recipient of the Nobel Memorial Prize in Economic Sciences, Nouriel Roubini and Kenneth Rogoff one the world's most respected economists. They sharply criticise Bitcoin and claim it will be regulated until out of its existence.

In the end of 2017 it was a wild rally for Bitcoin price. This year 2018 is more stable the price fluctuates between six to eight thousand USD. So, Bitcoin is already nicknamed as ‘stablecoin’. Volatility is historically on minimum. There are created models and prognosis in order to make the reality simpler. My own calculated analysis cannot be considered as investment recommendation, because it contains many "deaf" spots, which are substituted by assumptions. Used ratios and rates do not consider lost coins, so the final amount of good and services paid in Bitcoin is not accurate.

To conclude this thesis, I tried to present and explain in depth for he readers Bitcoin properties, meaning and utilization. Fundamental and technical analysis contribute to understand the wide extend and guides the reader through this sophisticated technology.

7. BIBLIOGRAPHY

Literature

ANTONOPOULOS, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 1st ed., Sebastopol, CA: O'Reilly Media, 2014. 298 pages. ISBN: 1449374042.

FRISBY, Dominic. *Bitcoin: The Future of Money?* London: Unbound, 2014. 304 pages. ISBN: 1783520779.

HUJOVÁ, Gabriela, ed. Zkušenosti s virtuálními měnami - Bitcoin měna budoucnosti?: sborník z konference : Praha, 26. března 2014. Praha: Vysoká škola manažerské informatiky, ekonomiky a práva, 2014. ISBN 978-80-86847-71-9.

LEE, David a Robert DENG, ed. Handbook of blockchain, digital finance, and inclusion. London: Academic Press, [2018]. ISBN 978-0-12-810441-5.

LIEN, K. (2008). Day Trading and Swing Trading the Currency Market. Wiley; 2nd edition. ISBN 978-0470377369.

KELLY, Brian. The bitcoin big bang: how alternative currencies are about to change the world. Hoboken, New Jersey: Wiley, [2015].

KOČENDA, Evžen a Alexandr ČERNÝ. Elements of time series econometrics: an applied approach. Third edition. Prague: Charles University in Prague, Karolinum Press, 2015. ISBN 978-80-246-3199-8.

MORSE, Edward A. *Electronic payment systems: law and emerging technologies*. Chicago: American Bar Association, 2017. ISBN 9781634259620.

PAGLIERY, Jose. Bitcoin and the future of money. Chicago, Illinois: Triumph Books, [2014]. ISBN 9781629370361.

STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin: peníze budoucnosti: historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky. Praha: Ludwig von Mises Institut CZ&SK, 2015. ISBN 978-80-87733-26-4.

STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN 978-80-271-0742-1.
TAPSCOT

T, Don, Alex. LOWY, David. TICOLL a Natalie. KLYM. *Blueprint to the digital economy: creating wealth in the era of e-business*. New York: McGraw-Hill, c1998. ISBN 0070633495.

TŮMA, Jiří. *Složité systémy řízení*. Ostrava: VŠB-Technická univerzita, 1998. ISBN 80-7078-534-9.

VIGNA, Paul. a Michael J. CASEY. The age of cryptocurrency: how bitcoin and digital money are challenging the global economic order. New York: St. Martin's Press, 2015

Internet Sources

99bitcoins.com, 2018. 99bitcoins.com [online]. Sarasota, FL: 99bitcoins.com [cit. 2018-11-24]. Available at: www.99bitcoins.com
Blockchain. (2018). *Bitcoin Charts & Graphs - Blockchain*. [online] Available at: https://blockchain.info/charts [Accessed 21 Oct. 2018].

Blockchain.info. (2018). *Confirmed Transactions Per Day*. [online] Available at: https://blockchain.info/charts/n-transactions [Accessed 10 Jun. 2018].

Bitcoin Cash Price Nears $1,000 as Breakout Continues. www.coindesk.com [online]. Available at: https://www.coindesk.com/bitcoin-cash-price-nears-1000-breakout-continues/ [Accessed Nov.11 2017].

BitcoinOnline.cz. Sto nebo milion? [online]. Praha: Bitcoinonline.cz, 2018. Available at: http://bitcoinonline.cz/2018/11/06/sto-nebo-milion-odvazne-predpovedi-ceny-btc/ [cit. 2018-11-12].

Bitcoin Energy Consumption, 2017. Https://digiconomist.net [online]. New York: https://digiconomist.net [cit. 2018-11-17]. Available at: https://digiconomist.net/bitcoin-energy-consumption

Bitcoin.com: Value of digital currencies [online], 2018. Washington, DC: https://www.bitcoin.com/ [cit. 2018-11-17]. Available at: https://www.bitcoin.com/

Bitcoin [online], 2018. Praha: https://www.e15.cz/ [cit. 2018-11-17]. Available at: https ://www.e15.cz/tag/bitcoin/1

Best Mining Gpu, 2018. Www.techradar.com [online]. Barcelona: www.techradar.com [cit. 2018-11-17]. Available at: https://www.techradar.com/news/best-mining-gpu

Bitcoin mining hardware, 2018. Www.bitcoinmining.com [online]. Español: Hesiod Services [cit. 2018-11-17]. Available at: https://www.bitcoinmining.com/bitcoin-mining-hardware/

Brainyquote.com, 2018. Www.brainyquote.com [online]. Mercer Island: BrainyMedia [cit. 2018-11-24]. Available at: www.brainyquote.com

Croarkin, C., Tobias, P., Filliben, J., Hembree, B., Guthrie, W., Trutna, L., Prins, J.:e-Handbook of Statistical Methods. NIST/SEMATECH, [Online]. Available at: http://www.itl.nist.gov/div898/handbook [Accessed 20 Oct. 2018].

Digiconomist.net, 2018. Digiconomist.net [online]. Paris, FR: Digiconomist.net [cit. 2018-11-24]. Available at: https://digiconomist.net/

Charlie Lee Litecoin Founder, 2016. www.investopedia.com [online]. New York: www.investopedia.com [cit. 2018-11-17]. Available at: https://www.investopedia.com/news/who-charlie-lee-litecoin-founder/

Institut kryptoanarchie [online], 2018. Praha: https://www.paralelnipolis.cz/ [cit. 2018-11-17]. Availablee at: https://www.paralelnipolis.cz/koncepty/institut-kryptoanarchie/

Investing.com. (2018). *BTC USD | Bitcoin US Dollar Bitfinex - Investing.com*. [online] Available at: https://www.investing.com/currencies/btc-usd [Accessed 1 Nov. 2018].

Mining, 2018. http: //slushpool.com/blog/mining. [online], 2018. Praha: www.slushpool.com. [cit. 2018-11-17]. Available at: www.slushpool.com.

Mining Electricity Consumption, 2017. Powercompare.co.uk [online]. London: Powercompare.co.uk [cit. 2018-11-17]. Available at: Powercompare.co.uk/mining-electricity-consumption

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. (PDF). Available at: https://bitcoin.org/bitcoin.pdf. [Accessed 20 Apr. 2018].

Patria.cz (2017). CZK/EUR analytical tools. [online] Available at: https://www.patria.cz/kurzy/CZK/EUR/graf.html [Accessed 22 Oct. 2017].

Paypal.com, 2018. Paypal.com [online]. CA, USA: PayPal [cit. 2018-11-24]. Available at: https://www.paypal.com/

Proof of Work, 2017. Https://blockgeeks.com [online]. New York: https://blockgeeks.com [cit. 2018-11-17]. Available at: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

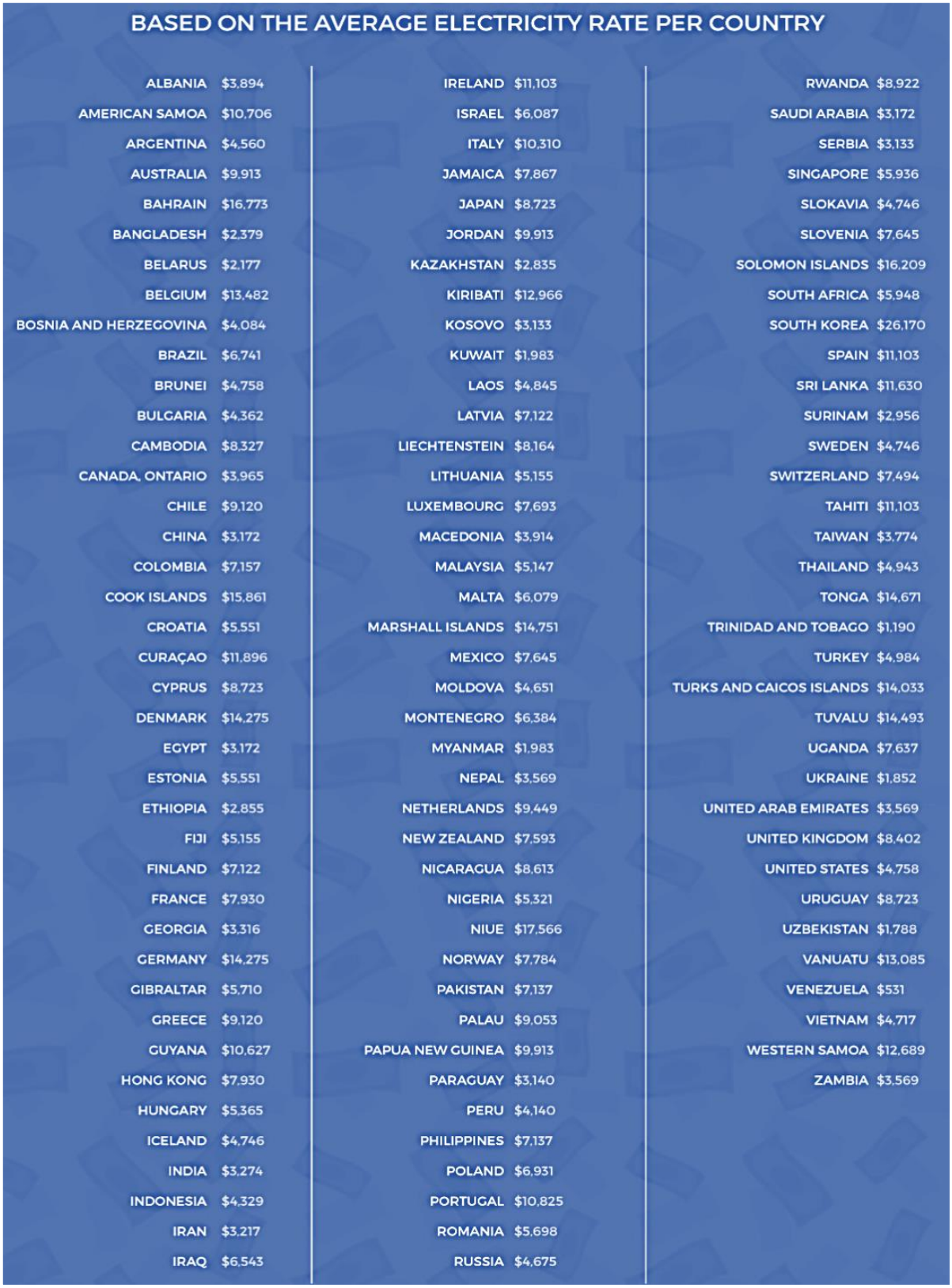
Stories of Slush Pool, 2018. https://cointelegraph.com [online]. London: https://cointelegraph.com [cit. 2018-11-17]. Available at: https ://cointelegraph.com/tags/marek-palatinus

The Czech Republic presents the law regulating Bitcoin, 2017. Arbolet.net [online]. Praha: www.arbolet.net [cit. 2018-11-17]. Available at: https://arbolet.net/clanek/ceska-republika-predstavuje-zakon-upravujici-bitcoin

Vitalik Buterin On The State Of Ethereum, 2018. Www.forbes.com [online]. San Francisco: www.forbes.com [cit. 2018-11-17]. Available at: https://www.forbes.com/sites/rachelwolfson/2018/08/15/vitalik-buterin-on-the-state-of-ethereum-the-future-of-blockchain-and-google-trying-to-hire-him/#26a3385758f0

APPENDIX

The cost to mine 1 Bitcoin in in selected countries



Source: CDR (2018)

Historical rates of Bitcoin/EUR from the end of 2016 to 2017.

Rate: BTC/€

Date	Price	Change %
Nov 2016	700	9.60%
Dec 2016	925	31.98%
Jan 2017	902	-2.44%
Feb 2017	1128	25.04%
Mar 2017	1019	-9.62%
Apr 2017	1263	23.85%
May 2017	2057	62.93%
Jun 2017	2136	3.82%
Jul 2017	2427	13.59%
Aug 2017	4017	65.53%
Sep 2017	3675	-8.52%
Oct 2017	5617	52.85%
Nov 2017	7821	53.95%

Source: own table based on data from Investopedia (2017)