Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Economics

Diploma Thesis

Economic analysis of Bitcoin

Bc. Kamen Kamenov

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Kamen Kamenov

Economics and Management

Thesis title

Economic Analysis of Bitcoin

Objectives of thesis

The main objective of the thesis is to give a brief overview to the reader what Bitcoin is and how Bitcoin work and to analyze the Bitcoin currency from fundamental, psychological and technical perspective.

Methodology

In the theoretical part data collection is being used. As for the practical part, fundamental macroeconomic analysis of the Bitcoin currency is being used. Psychological analysis including mass psychology of the market is used.

In the technical analysis is used graph analysis as well as analysis of technical indicators such as moving average and trend line analysis.

Programs used in the thesis are: Microsoft Excel, Microsoft Word, Statistical internet programs

---

The proposed extent of the thesis
60 pages

Keywords
money, bitcoin, exchange, price, fundamental and technical analysis

---

Recommended information sources
Bitcoin: How Can a Virtual Currency Attain Real Market Value?, D.N. Salter
Bitcoins: Mining, Transaction, Security Challenges and Future of This Currency, M. Zahid
Mastering Bitcoin, A. Atnopolous
Relationship Investing: Stock Market Therapy for Your Money, J. Weiss
Stock Market Efficiency, Insider Dealing and Market Abuse, P. Barnes

---

Expected date of thesis defence
2016/17 SS – FEM

The Diploma Thesis Supervisor
Ing. Petr Procházka, Ph.D., MSc

Supervising department
Department of Economics

Electronic approval: 28. 3. 2017
prof. Ing. Miroslav Svatoš, CSc.
Head of department

Electronic approval: 28. 3. 2017
Ing. Martin Pelikán, Ph.D.
Dean

Prague on 29. 03. 2017

Declaration

I declare that I have worked on my diploma thesis titled "Economic analysis 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 their person.

In Prague on 31.3.2017 _____

Acknowledgement

I would like to thank Ing. Petr Procházka, MSc, Ph.D. and all other persons, for their advice and support during my work on this thesis.

Economic Analysis of Bitcoin

The thesis highlights the currency of Bitcoin which starts to play bigger and more important role in today's economic and technical world. From the very beginning of the Bitcoin in 2009 until the time this work has been finished (2017) the Bitcoin has suffered many downfalls and rises and has become stable good on the stock markets when it comes to investments. The Bicoin has become more and more popular as a currency and the number of merchandises and retailers who accept it as a payment system still grows. This work depicts Bitcoin from theoretical perspective – the creation of Bitcoin, how the whole Bitcoin system works (including the Bitcoin transactions, how Bitcoin is being generated – mined, how the miners are rewarded and how the security system of Bitcoin works). The practical part of the thesis analyzes the Bitcoin from psychological, fundamental and technical perspective including analyzing the currency's volatility and price development in the years Bitcoin has existed as well as analyzing moving averages and other technical indicators of the currency.

Keywords: money, Bitcoin, exchange, price, fundamental, technical, psychological analysis

Ekonomická analýza Bitcoinu

Tato práce poukazuje na problematiku Bitcoinu, který hraje čím dále větší roli v dnešním ekonomickém světě. Od roku 2009 zažil Bitcoin mnoho výstupů a pádů a zařadil se mezi stabilní možnosti investice. Měna se stala o to populárnější, když ji začalo stále větší množství lidi akceptovat jako platební systém. Práce vysvětluje Bitcoin z teoretického hlediska – založení Bitcoinu, jak celý Bitcoin systém funguje (Bitcoin transakce, jakým způsobem je Bitcoin generován a jak funguje bezpečnostní systém kolem Bitcoinu).
V praktické části je Bitcoin analyzován pomocí fundamentálních, technických i psychologických metod včetně analýzy volatility, vývoje ceny Bitcoinu od jeho počátcích atd. Použity jsou mimo jiné metody klouzavých proměn i další technické indikátory.

Klíčová slova: peníze, Bitcoin, kurs, cena, fundamentální, technická, psychologická analýza

Contents

1. Introduction 9

2. Objectives and Methodology 10

2.1 Objectives 10

2.2 Methodology 10

2.3 Hypothesis 11

2.4 Research question 11

3. Theoretical part 12

3.1 Cryptography 12

3.2 Bitcoin 15

3.2.1 What is bitcoin? 15

3.2.2 How does Bitcoin work 18

3.3 Crypto-currencies based on Bitcoin 23

3.3.1 Litecoin 23

3.3.2 PPCoin 24

3.3.3 Namecoin 24

3.4 Practical usage of Bitcoin 24

3.4.1 Bitcoin as a payment system 25

3.4.2 Bitcoin as an investment 25

4. Practical part 26

4.1 Analysis of the Bitcoin 26
4.1.1 General fundamental analysis 31
4.1.2 General technical analysis..... 33
4.1.3 General psychological analysis 39
4.1.4 Own analysis..... 41
5. Conclusion 61
6. References.....62

1. Introduction

The thesis highlights the currency of Bitcoin which starts to play bigger and more important role in today's economic and technical world. From the very beginning of the Bitcoin in 2009 until the time this work has been finished (2017) the Bitcoin has suffered many downfalls and rises and has become stable good on the stock markets when it comes to investments. The Bicoin has become more and more popular as a currency and the number of merchandises and retailers who accept it as a payment system still grows. This work depicts Bitcoin from theoretical perspective – the creation of Bitcoin, how the whole Bitcoin system works (including the Bitcoin transactions, how Bitcoin is being generated – mined, how the miners are rewarded and how the security system of Bitcoin works).

The practical part of the thesis analyzes the Bitcoin from psychological, fundamental and technical perspective including analyzing the currency's volatility and price development in the years Bitcoin has existed as well as analyzing moving averages and other technical indicators of the currency.

2. Objectives and Methodology

2.1 Objectives

The main objective of the thesis is to give the reader brief overview what Bitcoin is and how Bitcoin works and to analyze Bitcoin from fundamental, psychological and technical perspective.

2.2 Methodology

In the theoretical part data collection is being used. As for the practical part, fundamental macroeconomic analysis is being used. Psychological analysis including mass psychology of the market is being used.

In the technical analysis graph analysis is being used as well as analysis of technical indicators such as moving averages and oscillators.

Programs used in the thesis are: Microsoft Word, Excel, Statistical internet programs

2.3 Hypothesis

"The price of the Bitcoin is due to high volatility and many unexpected rises/falls very hard to predict in long term periods"

2.4 Research question

"What is the best analyzing method for the Bitcoin currency?"

3. Theoretical part

3.1 Cryptography

To understand the main principles of bitcoin we have to know few terms from the arena of cryptography. Cryptography is a technique or a method which is being used for a safe communication between two users along with the assumption that there is a third user with whom we do not want to share the information. In general, cryptography is about constructing and analyzing protocols which do not allow the third side to participate in the communication and to extract the information. These protocols have to assure safety of the information and have to meet certain requirements such as authenticity, integrity of the data etc.

- Authenticity – It has to be possible for the receiver to provably discover the origin of the information (so the potential sender cannot pass off someone else.
- Integrity – It has to be possible for the receiver to find out whether the information/message has not been change on the "route" between the sender and the receiver. On other words the information should not be manipulated with.
- Indisputableness – The sender should not be able to decline that he/she is the real author and sender of the information.

Encryption has many devices in order to achieve the above mentioned principles. This thesis aims on ones which are needed for the understanding of Bitcoin(Frisby, 2014). If two parties want to share information together, they can encrypt the content – hide the real real content and transfer it to no readable format so that no other party can read the information. Than the party of the receiver can execute decrypting process to restore the original information. More or less most of the encryption and decryption algorithms are widely accessible on the internet, however the decryption keys (which are created by the author) are confidential. If both of the parties use the same encryption and decryption key they use symmetric encryption algorithm. Symmetric algorithms can assure intimacy of the information on their own, however to accomplish the authenticity, integrity and indisputableness other techniques are being used such as hash function.

Hash is mathematical function transforming the input data (pre-image) and converts the data to output hash value with fixed number of characters. Hash is shorter than the original

input chain and even a minimal chain in the output generates completely different hash value. One-way hash function is function which operates only in one direction. It is relatively easy to compute the hash value; however it is harder to do it the other way – to compute the input data out of the hash value.

As an example of the hash function SHA256:

Input: *Hello how are you*

Output: *2953d33828c3095aebe8225236ba4e23fa75e60f13bd881b9056a3295cbd64d3*

By simply changing the capital "H" with "h" we get completely different output.

Input: *hello how are you*

Output: *2cb097b2a305d0047aed9af1015bb5542fbd6d16a40705bcd17048db9265060b*

In the second example we can observe the variable length of the input and the fixed length of the output.

Input: *hello*

Output: *2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824*

Input: *hello my name is Michael and i live in Czech Republic however i am originally from Belgium*

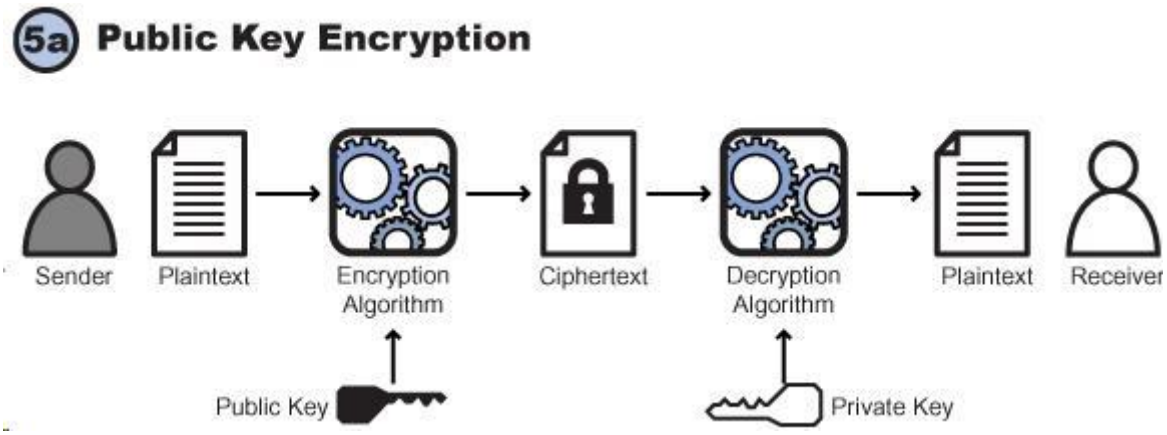
Output: *6074c339d94dce20718d01824873907e91bb31ce33f1efca8e50948322a7a206*

The output of the hash function is not dependent on the input in any recognizable way. These attributes allow us to use hash functions for verifications of the integrity of the message – the receiver can find out whether the message was not manipulated with or not damaged in any way. This method is being used in the BitTorrent protocol. The torrent client divides the data on few parts (which has its own hash value) and after downloading each part it verifies whether the hash value is the same as it was before. If the hash value of the downloaded part it not the same as the hash value of the torrent file, it is automatically restricted and downloaded later from someone else. This process prevents replacing the required data for other data (Frisby, 2014).

If the digital message provides authenticity, integrity and indisputableness we can state that it has signature similar to the one that is written in a piece of paper on an invoice for example. It is possible to create digital signatures with the help of symmetric algorithms, hash functions or with the help of reliable third party – however these methods may be still ineffective - not like the cryptography of public keys. This method creates a whole new way in encrypting, decoding and digital signing. In order to be possible to encrypt and decode a message we create two different keys – one public and one private.

We can safely publish the public key because it is technically almost impossible to extract the private key from the public one. If anyone would like to send this person an encrypted message he/she will simply use this public key. Everyone with the public key can send a message however only the private key can be able to decode it and subsequently read it.

Picture 1 - Public Key Encryption



Source: http://www.infosectoday.com/Articles/Intro_to_Cryptography/Introduction_Encryption_Algorithms.htm

The cryptography of the public keys can be also used for digital signing – we create a hash message and encrypt it with private key. If anyone with public key receives message with digital signature he/she can verify the integrity and authenticity by decoding the message using the public key and comparing the result with the hash value of the message. The signed message has also indisputableness – the sender cannot deny the sending of the message.

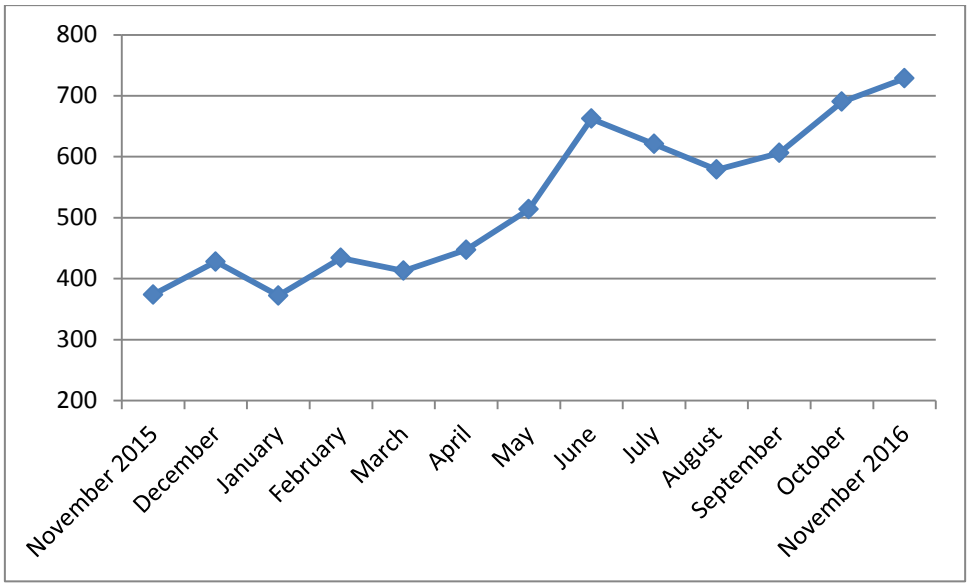
3.2 Bitcoin

3.2.1 What is bitcoin?

Bitcoin is decentralized digital currency which is not dependent on any central authority – no one is taking care of the administration and operation of the currency. Operation of the currency means essential operations such as validation of the transactions or emission of the monetary units of the currency. Bitcoin is an open source project – all source codes, documentations are freely accessible on the internet.

Unlike the ordinary payment methods the Bitcoin transactions are nearly instant and it is possible to send them all across the globe – Bitcoin does not distinguish to which country the transaction is being sent or in which country was the account created. All transactions are non-refundable and due to the absence of an central authority is not even possible freezing of the account. The transactions themselves are free, the fee for transactions is mostly voluntary. In case of paying the voluntary fee your transaction may be processed a bit faster. All transactions and account balances are freely available on the internet including IP addresses from which the individual transactions had been sent. Bitcoin is not anonymous as many people would think.

Table 1 - the evolution of the price of Bitcoin in USD in the past year



Source: Excel computations, http://www.investing.com/currencies/btc-usd-historical-data

The creation of Bitcoin account is very simple and fast – may take few minutes and no personal data or email address are required. The user received assigned address (public key) – to which can other users sent him/her Bitcoins (the addresses are unlimited). In the process of the sending of Bitcoins a transaction is created which is signed by the user's private key. Each transaction subsequently refers to the previous transaction in order to prevent the "creation" of Bitcoins and the fact that one Bitcoin can not be used twice. Each transaction has to be broadcasted trough the Bitcoin web in order to be valid and to verify it's authenticity. Broadcast is an informatics method in which the message is transmitted to all connected to the web.

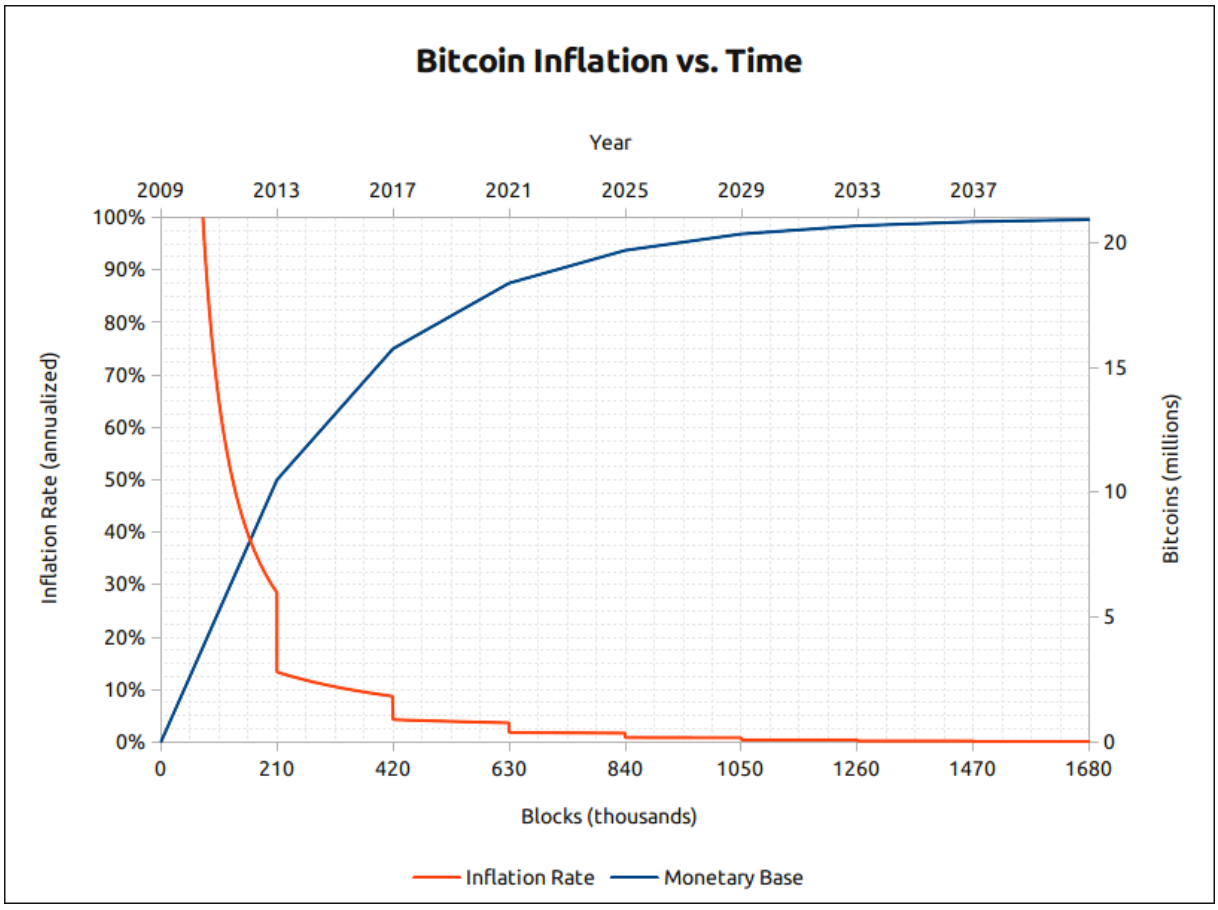
Every 10 minutes all transactions are assembled in the Bitcoin block (Franco, 2014). As soon as the transaction is a part of the Bitcoin block we can say that the Bitcoins which participated in that transaction are "safe to spend". The blocks are very hard to create and almost impossible to falsify. All blocks are connected together into the blockchain. Blockchain is considered as the open accountancy book of the Bitcoin – all time transactions are recorded there and definitely delimits how many Bitcoins are attached to each Bitcoin address. The blockchain is secured by cryptographic algorithms which prevent modifying of any part.

Bitcoins are created by solving cryptographic task which is connected with the creation of the block and the provision of the "proof of work". This process requires a lot of

calculation output and is simply programmed to create blocks every 10 minutes. As a reward for the creation of a valid block the creator (miner) receives a certain amount of freshly created Bitcoins. The amount of the freshly created Bitcoins is simply predicted by the fact that every 10 minutes a new are created. Currently in circulation there are about 16 million Bitcoins and about 25 new Bitcoins are mined every 10 minutes (Logan, 2016).

On the picture No. 3 we can observe the assumed Bitcoin reserves evolution in the next years among with the inflation. The term inflation here means only the increase in the monetary supplies – the Austrian school.

Picture 2 - Bitcoin inflation vs. Time



Source: bitcointalk.org

3.2.2 How does Bitcoin work

In 2008 Bitcoin was introduced as the first concept ever of decentralized currency (Felten, 2016). The first proposal had been signed by the pseudonym Satoshi Nakamoto however the real identity of the person is still unknown. The first official version of the client was introduced in January 2009.

Adresses

As soon as the user installs the Bitcoin client he/she receives a pair of ECDSA keys. If the user wants to send Bitcoins from one address to another he/she creates a special message (transaction) and subsequently signs it with the private key of the user. Afterwards the public key is used by anyone who wants to find out whether the user has privacy rights over those Bitcoins.

An example of a Bitcoin address is seen bellow.

1HceWtheh1yfeCN85GfXG84hYJjDz1JPsQ

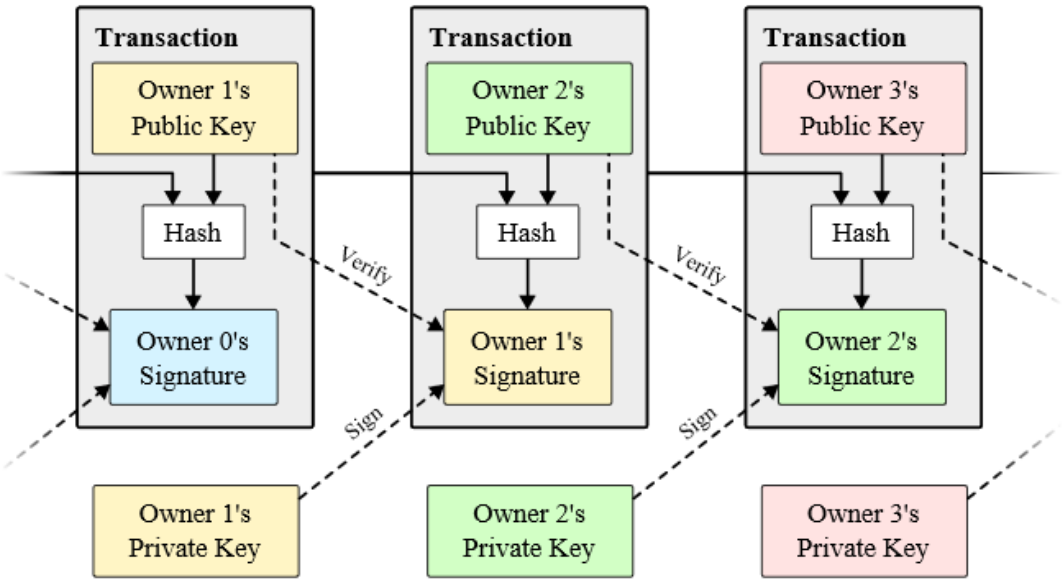
The Bitcoin adress is (with very few exceptions) 34 characters in lenght and it starts with 1 or in extreme situations with 3. The adress must not contain „0“ ; „O“ ; „l“ and „I“ due to this characters can be mixed up very easily. The adress itself contains the following information:

- Information about the web which the address is used for
- Hash of the public key owned by the user
- A sum for ensuring the integrity of the data

Transactions

Bitcoins themselves can be defined as a chain of digital signatures as shown on the next picture. Every Bitcoin user can send Bitcoins by simply signing the hash of the previous transaction and the public key of the receiver. The receiver can verify the signatures as well as the whole chain of the previous Bitcoin owners (Antonopoulos, 2014).

Picture 3 - Bitcoin transactions



Source: Satoshi Nakamoto Institute, http://nakamotoinstitute.org/

In the ordinary payment systems the payment operation is verified by a third party, most of the times by the operator who checks up whether the sender has enough money in the account for the transaction operation and whether the money had not been spent before (double spending). As is mentioned above in the thesis – the Bitcoin has all transactions public so everyone can verify the chain of the ownership of the coins – the double spending attempts are not possible. This theoretical concept was introduced for the very first time by Wei Dai in his essay "B-money".

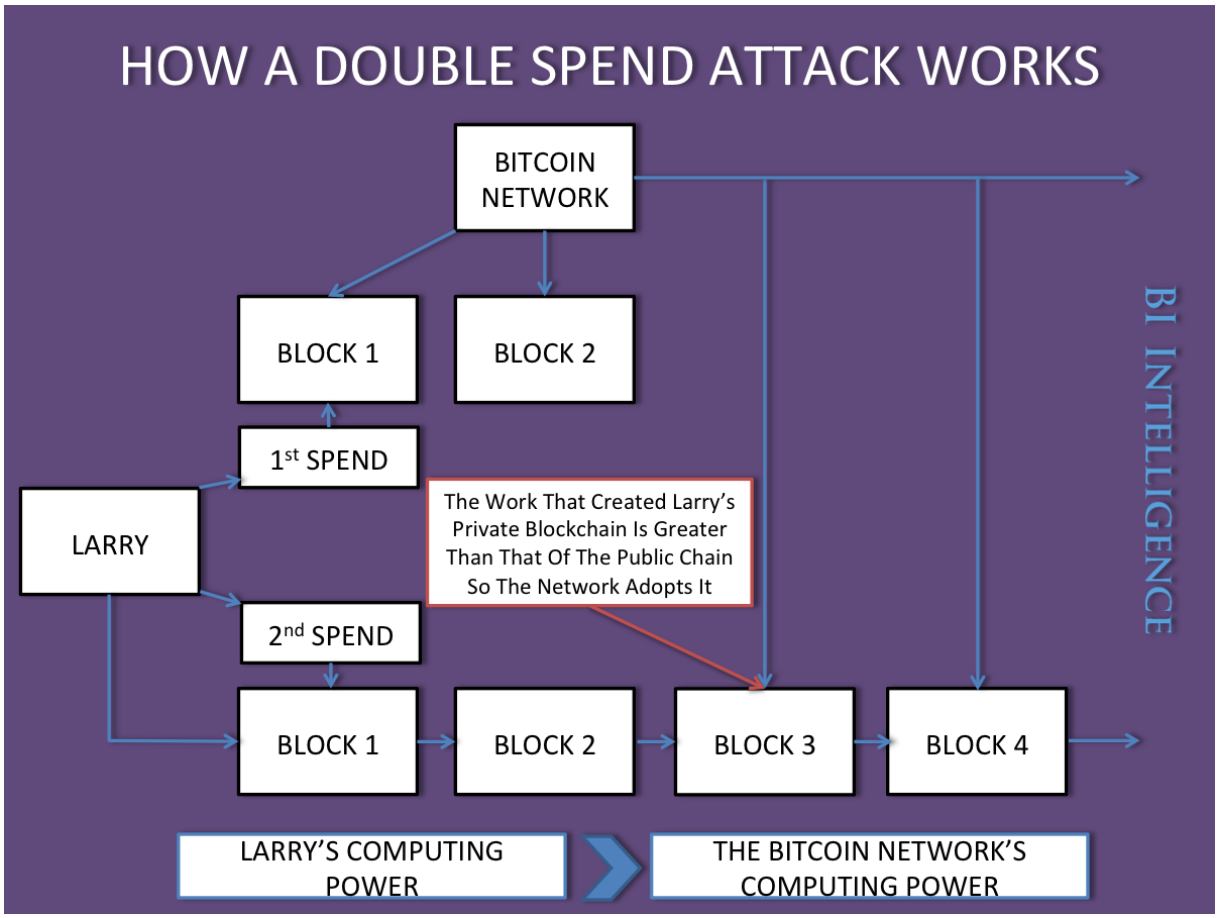
Bitcoin relies on a peer-to-peer web which communicates with the individual users by the internet. Peer-to-peer, also known as the architecture client-client, is appellation for computer webs where the users communicate directly (with the absence of a third party or a central server). Peer-to-peer systems are distributed systems being comprised of connected intersections who have the ability to individually organize for the purpose of sharing sources such as content or computational performance. The peer-to-peer system is

capable of adapting to faults and to ensure communication among the intersections while they maintain good connection and performance and without any central server or authority.

The Bitcoin web provides communication channel which sends transactions and other information among the intersections (users) of the web.

A unique characteristic of the Bitcoin is a method for receiving and declining a transaction and a method of agreeing on unified history of the transactions in the web. Considering the delay which occurs while broadcasting the transactions into the Bitcoin network, it is not possible for every user to track every single transaction. This fact could be abused in order to "double spend" – spend the same Bitcoins more than once – before the first transaction has spread far enough in the Bitcoin web. Next picture illustrates the fact how one Bitcoin can be spend more times (however there is a cryptographic method which does not allow it).

Picture 4 - How double spend attack works



Source: Emily Adler, https://www.businessinsider.com.au/the-latest-attack-on-bitcoin

Proof of work

The "proof of work" was originally designed by Adam Black in the "Hashcash" as a measure against email spam. For many cryptographic hash functions can be the number of attempts for finding the input stochastically predicted because the most effective way how to find such input is the "brute force method". Solving a problem with the brute force method requires systematic testing of all possible combinations or a subset of all possible combinations until finally the result is found. This method is widely used for breaking through passwords. There is an example of the brute force method for cracking passwords.

Password: Kamen

Progress of the crack: "A" "B" "C"…… "K" ; "KA" ; "KAB" "KAC" KAD" … "KAM" ;

"KAMA" "KAMB" "KAMC" … "KAME" …. "KAMEN"

The input creating the hash stating on certain chain is called "partial hash collision" and the process of the searching for the appropriate input is called "mining". For example if we need 32bit chain in a binary hash, the expected number if inputs which we have to try is 2^{32}. In the Bitcoin terminology the proof of work means that these attempts were actually made in order to find out the partial hash collision.

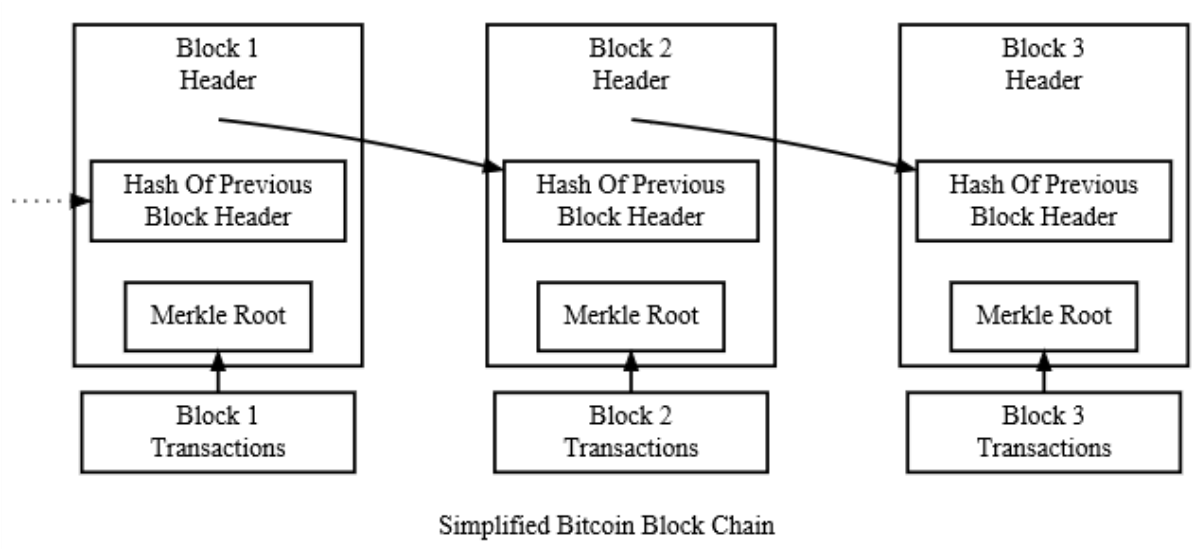
The proof of work is used for 2 reasons. The first one is that proof of work serves as a voting device about the transaction history – the more the person performs, the bigger voting right he/she has. The second reason is creating the currency.

Anybody can create the money by simply broadcasting the solution of previously not solved computational problem. The only condition is that it has to be easily defined how computationally hard was the problem and the solution of the problem must not have any value, neither practical nor intellectual.

As for the partial hash collision – it meets the requirements. It is easy to find out how much computational power had been used and the computation has no other value. The partial hash collision serves as a "vote" for the transactions to be included into the transaction history and the "miner" is rewarded with Bitoins (Frisby, 2014).

The next important concept of the Bitoin is that every proof of work is based on the previous one. The hash from the previous proof of work is contained in the input of the actual one – a block chain is created.

Picture 5 - Block chain



Source: Bitcoin.org, Developer's guide

Block

Each block consists of its own content – the transaction and the head of the block. The head of the block consists of the following information:

- Version – version of the protocol
- Previous hash – SHA hash of the previous head of the block
- Merkle root – hash verifying the integrity of the transactions in the block
- Time stamp – time when the block was created
- Bits – value connected with the difficulty of the proof of work
- Nonce – variable value during the mining which helps finding the partial hash collision

Instead of saving the transactions themselves in the head of the block we use the Merkle root – the root hash merkle tree computed from all transactions of the current block. The Merkle root is computed as follows. Firstly, hash for every transaction in the block is being computed. These hashes are being paired and subsequently a new hash is computed based

on the pair – a new hash is produced which is half the original one. This step is repeated as many times as we have generated only one hash. This hash is called root (merkle) hash and is placed in the head of the block. Afterwards every head of each block has stable size of 80 bytes and the transactions can be verified without needing the whole block chain. Only the head of the block is enough for the verification. This process is called "Simplified Payment Verification" and is used in the most Bitcoin clients – the user does not have to download the whole block chain (which might be several gigabytes) but only the head of the block (few megabytes).

Block Chain

If the is a hash included in every block from the previous one we can state that every block is "build" on the top of the previous one. The voting itself is at the moment when the "miners" choose which block to expand and link the following block. The choice of a certain block means that the miner agrees with all transactions within the block and with all transactions within the blocks preceded the current one. If a group of miners work on a different block than the other miners the block chain branches. In this situation two or more chains appear which compete with each other. The chain in which more computational performance is being put into is getting longer and the Bitcoin intersections always prefer the longest one – the other chains perish. As a result of this, block chain consists only of transactions with whom most of the computational performance agree. Block chain should not be mistaken with the Bitcoins which are chains of digital signatures. Block chain links the blocks while the transactions are linked by the signatures. The intersection is considered "honest" if all rules are observed. The condition of the successful operating of the Bitcoin is that the "honest" intersections must have higher computational performance than any other "attacker".

3.3 Crypto-currencies based on Bitcoin

3.3.1 Litecoin

Litecoin is the second most popular virtual currency after Bitcoin. It is based on the source codes of Bitcoin and it is open source project (as Bitcoin). The main difference with

Bitcoin is the reduced time interval between the creation of different blocks from 10 minutes to 2,5 minutes. The consequence is faster confirmation of the transactions and 4 times higher amount of created Litecoins – 84 million. Litecoin addresses start with capital "L" in order to be easily distinguished from the Bitcoin addresses. Otherwise are generated the same way. The Litecoin price is approximately $ 4,2 (17th March 2017).

3.3.2 PPCoin

PPCoin is a project based on the same principles as Bitcoin, however it tries to mitigate the energy consumption of the mining and in the same time to keep the same safety and other positive aspects of the Bitcoin. In order to achieve the above mentioned facts PPCoin substitutes the proof of work with so called proof of stake. This system is based on the "age" of the single coins – for example having 10 coins which were not manipulated with for 50 days; these coins automatically gain value of 500 coin-days. After any transaction of these coins this value is annulled. In the creation of the blocks the block with the largest volume of annulled coins becomes part of the main block chain.

3.3.3 Namecoin

Out of all cryptographic currencies based on the Bitcoin the Namecoin shares the third position as of a popularity, however the share in the market is approximately 90% less than on the Litecoin. Namecoin is more of an alternate domain name system than a currency. It expands the original software so the transactions support registration, update and transfer of the privacy rights of the domains.

3.4 Practical usage of Bitcoin

After a brief description how does the Bitcoin work the work proceeds to the practical use of the Bitcoin. After one has already obtained a Bitcoin he/she can do this things:

- By any service/goods from a merchandise which accepts Bitcoin as a payment system
- Trade with the Bitcoin in the stock market

3.4.1 Bitcoin as a payment system

As for the use of Bitcoin as a payment system an interesting fact is that the first thing ever paid with Bitcoin was pizza. Since then the application of Bitcoin has considerably expanded. There are certain theories which address that Bitcoin has been primarily developed in order to pay for illegal activities and goods such as drugs, however todays use is rather wider. Nowadays exist shops in which there is possibility to pay with Bicoin, even in Europe. The number of the merchants accepting in is rather small however is expands very fast and there is such high potential in the next years.

3.4.2 Bitcoin as an investment

Another use of the Bitcoin is as an investment. Nowadays there are countless opportunities and possibilities how and in what to invest his/her financial resources. One chooses the types of the assets he/she wants to trade with, on which markets, when, how long and what risk is willing to take. In the investments we always need to consider the ratio between the risk, profit and the liquidity. There are many assets in which we can choose to invest such as stocks, bonds, commodities and properties. The investments into stocks and bonds are made in the stock markets while in the financial markets we trade with commodities such as gold, silver, platinum and other precious metals or even oil, cocoa or wheat. The trade with the Bicoin can be beneficial if the trader look at the Bitcoin as an investment, not as a currency. On the one hand it might be a great deal in a short period of time, on the other hand there is a high risk (due to the high volatility).

4. Practical part

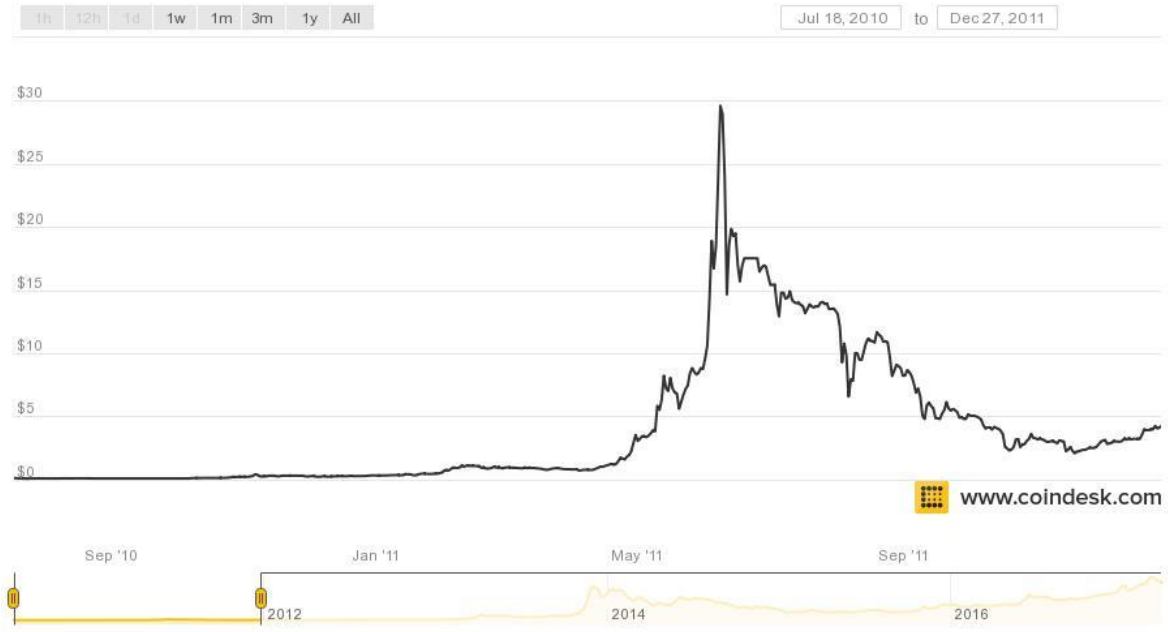
4.1 Analysis of the Bitcoin

Analysis can be really complicated process. There are two main methods for analyzing a currency and its values – technical analysis and fundamental analysis. There is also a psychological analysis however this type of analysis is not as valued as the two mentioned above. More detailed description of the analyses will be depicted in the next chapters.

The Bitcoin has no base assets – its value is only based on the willingness of the clients to buy and sell it for a certain price. The evolution of the Bitcoin price was very irregular. From the very beginning (2009) until nowadays there had been so many fluctuations, no regular rotation of the cycles. The Bitcoin price can vary in the different stocks markets – therefore the price in the stock coindesk.com is used.

Since this work describes the evolution of the price if this virtual currency in its whole existence, we need to state that the price had no significant changes in the first 2 year of its existence. The price moved around $0 for a Bitcoin from January 2009 until the beginning of 2011. In January 2011 it started to grow from $0,3 to $3 in April and then the first rapid increase occurred in June 2011 – the price jumped to $30 and then subsequently decrease to $16. Until the end of 2011 the price descended to $3 - $4. After the rapid growth in June 2011 the Bitcoin trades had significally increased. The currency exchange rate did not had higher volatility and until the summer of 2012 it stabilized at around $2 - $6.

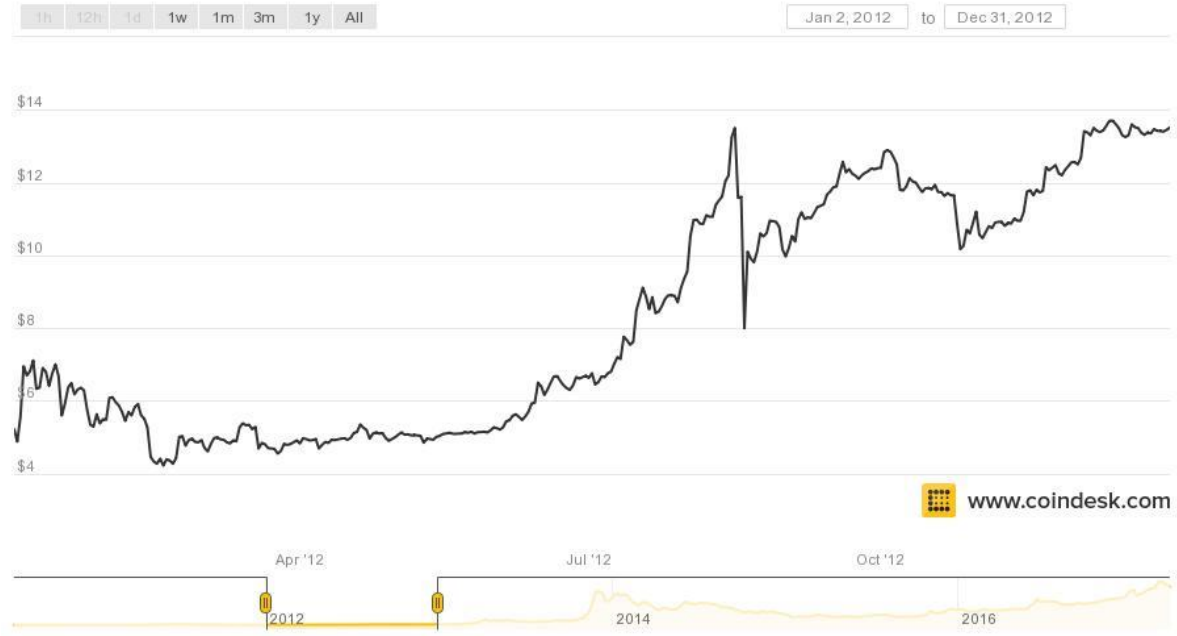
Chart 1 – Evolution of the Bitcoin Price in 2010-2011



Source: Coindesk.com, 2016

After the summer of 2011 when the currency reached its peak at that time there were no great fluctuations. In January 2012 the exchange rate was $6, then in the summer of 2012 increased to $15, then rapidly decreased and afterwards stabilized around $10 - $14 until the end of 2012.

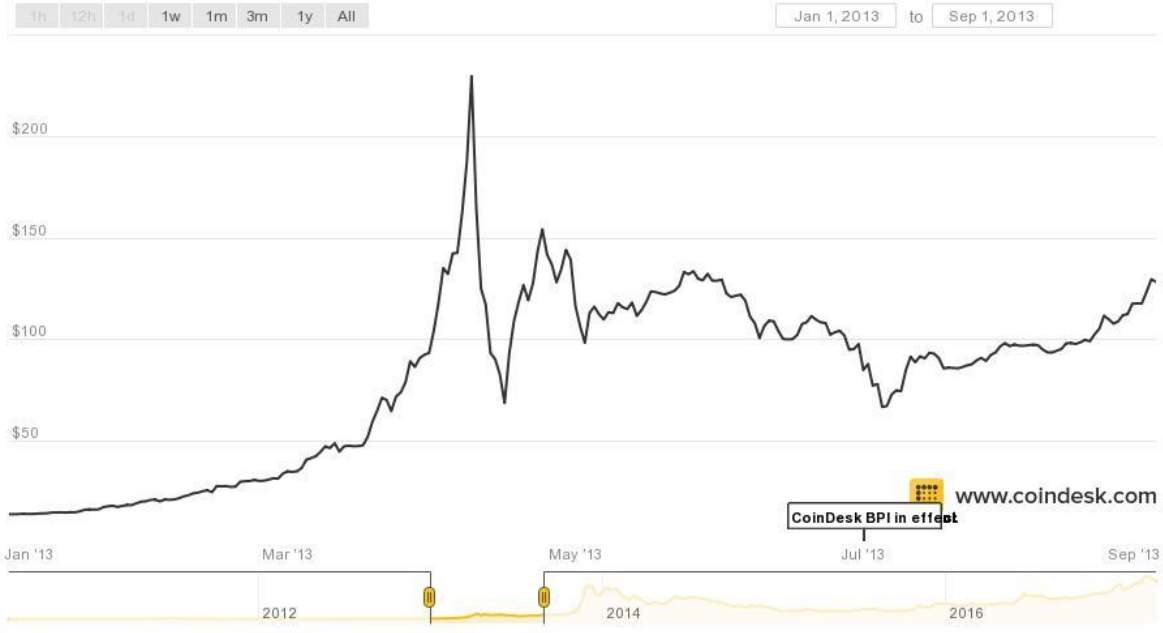
Chart 2 - The price of Bitcoin in 2012



Source: Coindesk.com, 2016

In January 2013 the rate rapidly increased again and reach its peak at $238 in April 2013. One of the main reasons was the expand of the market – still more and more people knew already about the Bitcoin. At that time a lot of articles about the Bitcoin were published and the trade capacity of the Bitcoin increased. The price maintained at the peak for a very short period of time and yet in the same month the price declined to $75. Than it oscillated in the range of $70 - $150 from April to October 2013.

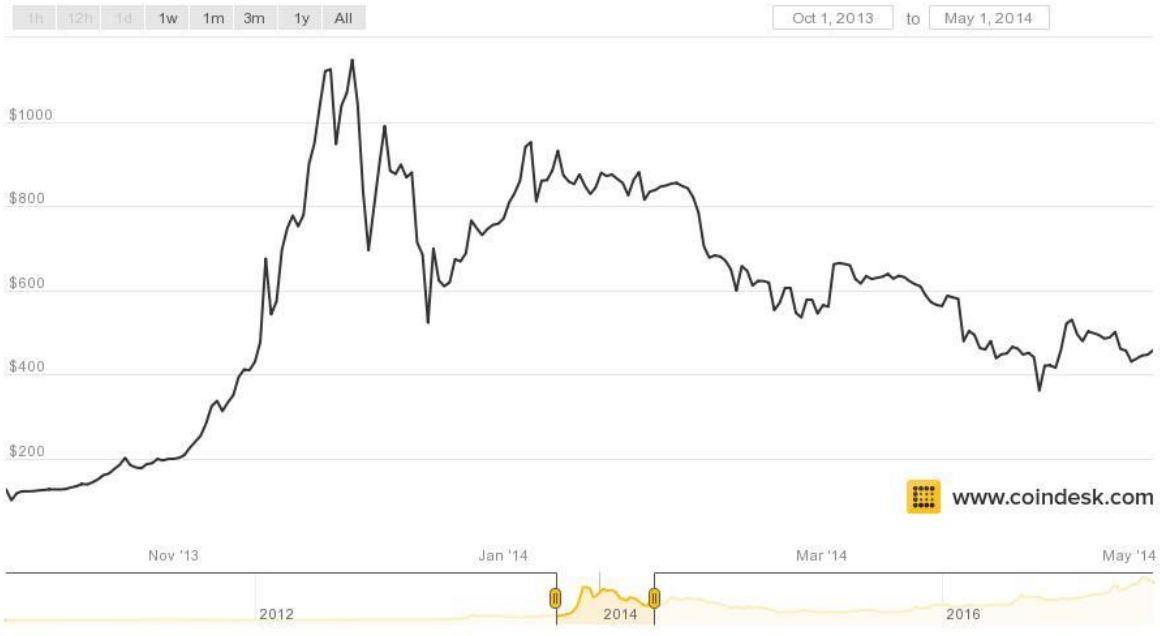
Chart 3 - Bitcoin price from January 2013 to September 2013



Source: Coindesk.com, 2016

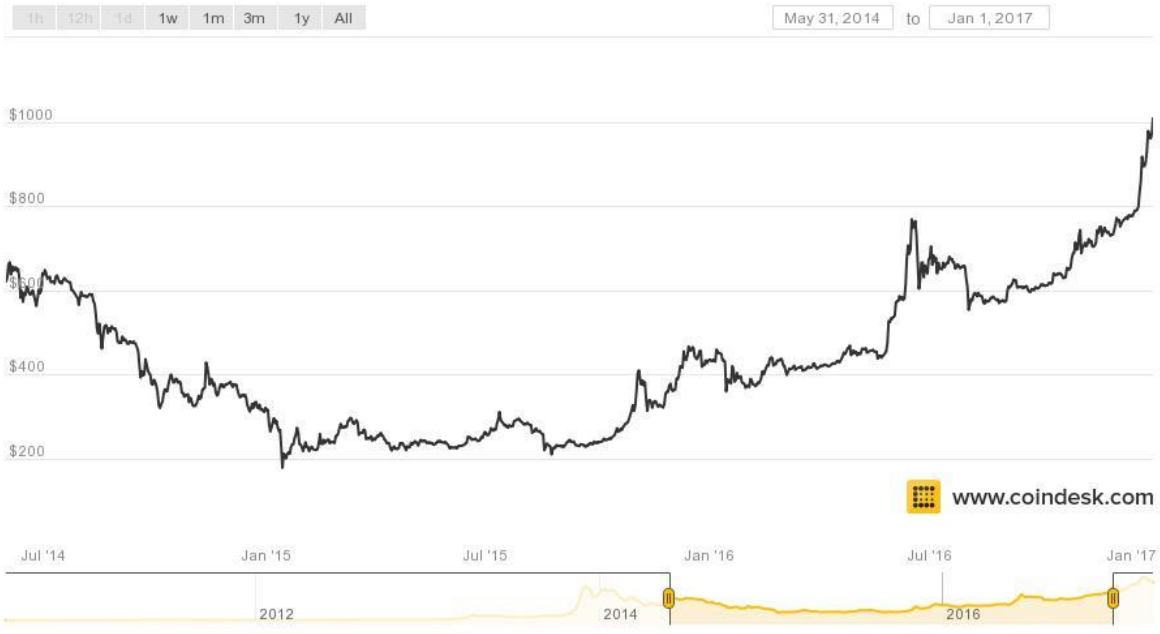
In October 2013 the price started to rapidly increase from $120 and the maximum value of Bitcoin was $1150 in December 2013. Again the phenomenon was for a very short period of time and before the end of 2013 the price rapidly decreased to $550. In January 2014 the price jumped to $950 and then slowly diminished from $800 to $400 as shown in the chart 4.

Chart 4 - Bitcoin price from October 2013 until May 2014



Source: Coindesk.com, 2016

Chart 5 - Evolution of the Bitcoin price from May 2014 until January 2017

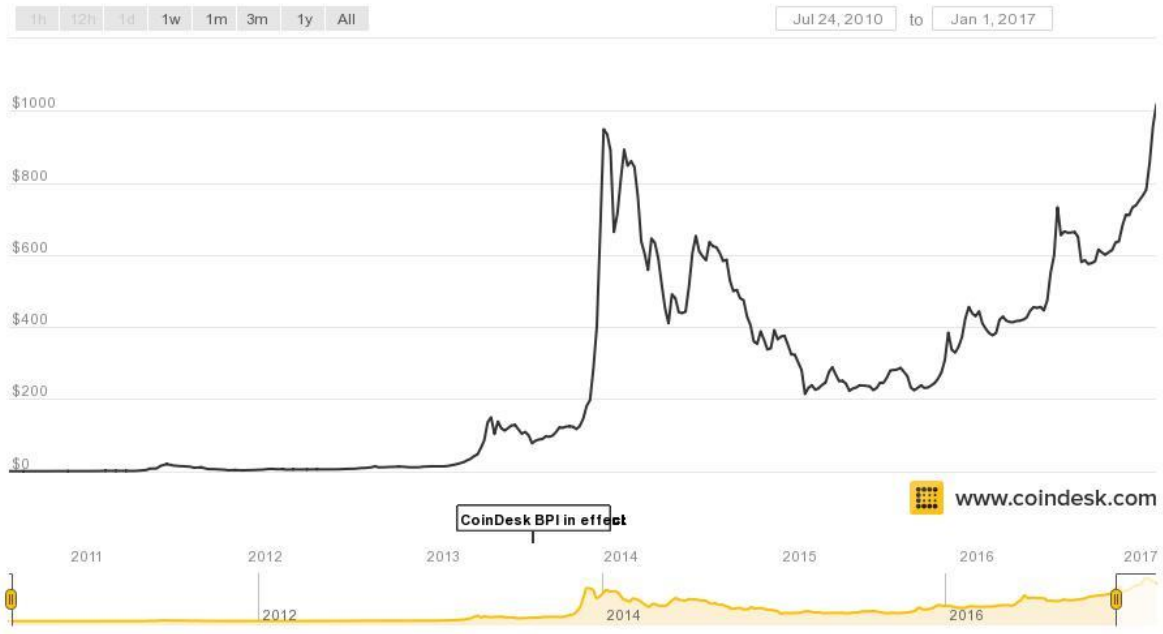


Source: Coindesk.com, 2017

During the overall existence of Bitcoin (around 7 years) there were several larger "peaks" and a one less significant. We can observe that after every peak that is significant decrease

(around 40%-50% of the peak value). However after every "correction" the Bitcoin maintained of higher value than one before the last peak. These periods of high increase and subsequent decrease can be explained most of the times only by psychological analysis where people most likely succumb to mass psychosis based on some kind of information and start to buy as many Bitcoins as they can and subsequently start to sell them. In the next chart we observe the overall evolution of the Bicoin price.

Chart 6 - Overall Bitcoin evolution price



Source: Coindesk.com, 2017

From the graphs above we observe that the Bitcoin is very volatile currency. Volatility is defined as instability, fluctuation of the prices of assets on the financial markets. Volatility models and predictions are in the centre of interest of many financial analyses – theoretical and practical. It is not surprise because the volatility – used as decisive deviation for indicators of profitability – is the base measure for riskiness.

Even the volatility is not directly observable; there are certain usual characteristics when observing the profitability of financial activities. The methods which help us to predict and estimate the volatility are (Cipra, 2008):

- The volatility can be high in some periods and low in other ones
- Volatility reacts differently on a price growth and price decline
- Volatility does not jump to "extra high" values, its shape can be stationary in a certain period

We can state that the development of the exchange rate of the Bitcoin confirms these facts about the volatility of the Bitcoin – in certain periods of time was very low, in other it was quite high, differently developed when there was price increase and differently when there was a decrease. However there were no extreme "jumps" and most of the time in did not approximate to extreme values.

4.1.1 General fundamental analysis

Fundamental analysis is an important aspect of understanding the main principles of the market. It aims at estimating the "fundaments". Speaking very generally – these are the events which can affect the value of the assets. Fundamental analysis gives us the possibility to reveal the motion of the trend and to create prediction and forecasts for the future.

Fundamental analysis is based on the assumption that the theoretical prices of the assets are different from the actual market prices (for which they are traded on the public markets). In very general way we can say that the fundamental analysis researches whether the market price of the asset corresponds with its theoretical price. Fundamental analysis is the most complex analysis of assets – in is used when we want to invest. If the theoretical value of the asset is higher than its market value, than we can state that the asset is undervalued and if the theoretical value is lower, than the asset is overvalued. In order to clearly understand the fundamental analysis we need to define the "theoretical value". This can be defined as an individual opinion of any market's participant what the impartial exchange rate should be (the value of the exchange rate is considered "constant" in the short period of time therefore we can compare it with the variable actual rate of the asset.

Fundamental analysis searches and analyses factors which influence the theoretical value of the asset. Generally speaking about Bitcoin this can be a bit harder because it is hard to define it's theoretical value – there is no real work, no material inputs etc. (in comparison to other market assets).

Investors and financial analysts use different methods in order to compute the theoretical value of the asset. The individual investors dispose of different information and figure – that's why they may use different methods. This is the fact that even if many analysts use the same analytical method they can achieve a different result. It follows that in a single moment there may be several theoretical values of an asset or commodity. It follows that since the theoretical values change – the exchange rates will change also.

Fundamental analysis examines many factors. From the point of view of the examined factors we can divide it into several branches:

- Macroeconomic analysis – analyses the economy as a whole and researches the relations among the global macroeconomic aggregates and the exchange rate
- Branch analysis – analyses the single branches and predicts their future development
- Microeconomic analysis – estimates the inside parameters of a company – retrospective, present day and perspective

It is really hard to analyze the Bitcoin with the branch analysis with the microeconomic analysis by these simple facts:

- Bitcoin is not a branch of the economy which development we can try to predict to the future (in terms of economy market structure of the branch etc.)
- Is not generated as a stocks of a certain company. Not a single method is useful because most if the input parameters which are used simply miss
    - Dividend models
    - Profit models
    - Balance models
    - Financial analysis

The only category from the fundamental analysis that is acceptable when analyzing Bitcoin is the global macroeconomic analysis.

General macroeconomic analysis

Fundamental analysis from macroeconomic perspective aims at observation of economic indicators, social factors and international politics. It is a method which predicts the real value of the investment. It proceeds from the theory that the market value of the assets recurs to its theoretical (real) value. It uses the database of all past and present (public) information and aims at answering the question: what and why will happen in the future. Among the most important factors which affect the development of the market with assets from macroeconomic point of view are: development of the economy, fiscal policy (administration of the incomes, debts etc.), the amount of financial supply, the amount and changes in the interest rates, inflation, foreign capital, the quality of the investment environment, legal aspect.. Among other factors which we can analyze in the macroeconomic analyses belong unemployment, GDP growth, taxes, monetary policy.

4.1.2 General technical analysis

Technical analysis has many forms and methods of usage. It is used to analyze the development of the stock market, commodity market or for example or foreign exchange market. It works on the presumption of public information such as exchange rates, amount of trades. The technical analysis "assumes" that the human factor is basically constant. The fact that the history of the exchange rate changes is constantly repeating, the technical analysis with the help of time series identifies the trends from which it predicts the future development of the currencies. Technical analysis is based on the confidence that the crucial factors are market supply and demand. Based on these two aspects the exchange rates are created in which all available information (fundamental information) is stored – even potential pessimism or optimism of the participants of the trade. In the technical

analysis we are not interested that much in the price level or the concrete exchange rate changes – technical analysis aims at the prediction of these changes and on the estimation when these changes will occur. So the fundamental analysis basically aims on what to buy or trade with, the technical analysis determines the right time of buying and selling – estimates when to trade.

The technical analysis uses two main indicators. The technical analysts concentrates all his attention on the graph, its shape and the indicators derived from the prices of the assets and from the amount of the trades. During the technical analysis we observe two main parts: patterns and indicators.

Graphical analysis

Graphical analysis can be characterized as follows:

1. Creation of graphs based on time series and exchange rates
2. Analysis of these increasing and decreasing trends
3. Analysis of the graphic formations which has arisen for the purpose of the prediction

The graphical analysis uses very wide spectrum of graphs and charts – the most common one is the line graph and the column graph. The main advantage of the line chart is its simplicity – on the horizontal axe displays the time, on the vertical one the evolution of the exchange rate. It is used at short term as long term trends. The column graphs are a bit more complex since they display at a time 4 different information: open prices, low prices, high prices and close prices.

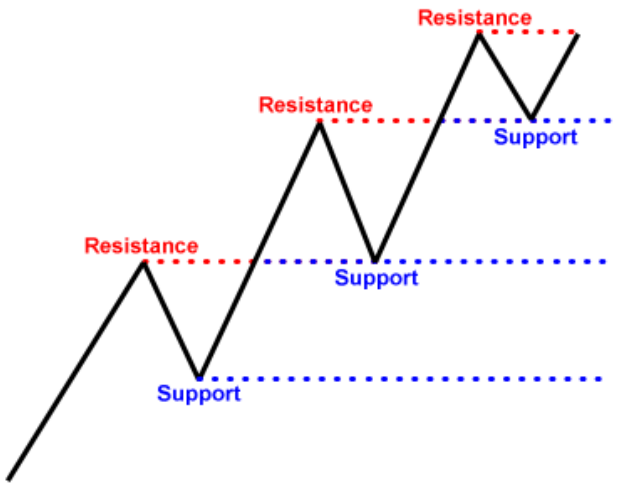
There are many other types of graphs such as point graph, candle volume graph, figure graph etc.

Trend analysis

In the technical analysis is important to define whether the trend is increasing or decreasing – in the increasing trend the maximums and minimums of the exchange rates increases while in the decreasing they decrease. In the prediction of the future development of the trend there is another factor which plays big role – the amount of trade. This was defined by Charles Dow – If the amount of the trade increases, the current trend should continue the same way. If the amount of the trade starts to decrease, we should expect a change in the trend.

The supply and demand in the technical analysis have to do with two terms – level of support and level of resistance. The support is the exchange rate which most of the traders consider as a minimal and are not willing to sell for a lower price. Oppositely the resistance is the maximum rate for which the trader is willing to buy. The levels of support and resistance are sometimes drawn in the graphs used in trades. They are just temporary psychological factors – however they should not be underestimated. On the next picture we can see the theoretical levels of support and resistance.

Picture 6 - Graph showing what support and resistance levels are in the exchange rate



Source: http://electrofx.com/forex-trading-basics/support-resistance/; Theo Pastios

Another term used in the technical analysis are the trend lines – straight lines which connect the minimal values of the exchange rate (local minimums – increasing trend lines) or the maximum values (local maximums – decreasing trend lines) during a period of time. The longer the line is, the more points in connects on the graph and the more dependable and significant it is.

Analysts and investor have to recognize when the current trend ends and changes to inverse one. All exchange rates after a certain periods of growth or decline have tendency to get back the other way – a correction of the exchange rates. The theory of "percent of changes" states that if the rate falls about 1/3 – 2/3 of the current value, it is a short term correction and will continue with the original trend. If the rate falls more than 2/3 of the value – it will most likely change its trend.

Fibonacci retracement

One of the best tools of the technical analysis is the Fibonacci retracement based on the Fibonacci sequence (1, 1, 2, 3, 5, 8, 13, 21, 34. . .) where every number is the sum of the two numbers before. The proportion of the 2 numbers next to each other is always close to 1,618. As from the economic point of view the strongest Fibonacci values are 38,2%, 50% and 61,8%. They are basically very strong support and resistance levels from which the market reflects or the trend changes.

Analysis based on technical indicators

Technical indicators are formulas based on which we count and subsequently receive information whether current asset's price has rapidly increased therefore a correction is expected or oppositely the price is very low and is expected to increase. The technical indicators also provides us with the information whether the price has changed or is expected to change soon, or whether there will be a new trend – increasing or decreasing. The technical indicators can be characterized as a mathematical functions which serves us as an analysis of the future development of the rates as well as for the prediction of the future development of the whole market. As for the main technical indicators, the most commonly used are:

- Moving averages
- Oscillators
- Price volume indicators
- Zone analysis

The moving averages are most commonly used implements of the technical analysis as well as most probable in the investment analysis. There are simple, exponential and other moving averages. The most commonly used is the simple moving average even it indicates many "false" signals. Weighed moving average is being used the same way as the simple moving average with the exception that the oldest entry has the least significance while the newest has the highest significance. The exponential moving average is a category of the weighed; however the weights are assigned to the exchange rates exponentially. Practical usage of the moving averages is a combination of:

- Moving average with the exchange rate of the asset
- Mutual combination of two or more moving averages

The origin of the buying and selling signal comes where the intersections of the curves are. The moment where the curve of the exchange rate intersects the moving average one from the bottom is the buying one, while the intersection is the other way we consider it as a selling moment.

The zone analysis is a method which also uses the moving averages. It works with three curves where the middle one is the curve of the moving average while the other two are the boundaries of the so called "envelope" which surrounds the moving average. This way comes in existence a zone where its upper border is the line of resistance while the lower border is the line of support. There are three main categories of zones:

- Percentual zone
- Bollinger zone
- Moving averages zone

The percentual zones are the simplest method of zone analysis, the upper and lower borders are distant from the moving average by a stable value; for example 5%-10%. We observe the approaching to the borders, however this signal is considered

relatively unreliable. The buying and selling signals are indicated in the moment where there is an intersection and subsequently the rate starts to go back to the zone. When the lower border has been intersected we consider it as a buying signal while the upper border is intersected it indicates the selling signal. In the Bollinger zones the width of the envelope changes depending on the volatility of the simple moving average curve (the more volatile curve, the wider envelope). The evaluation is the same way as is in the first method.

Oscillators are technical indicators measuring the long term change in the exchange rate and they need enough input indicators. They are suitable for a market which is neither increasing neither decreasing. The shorter is the time measured the more signals they indicate. There is relatively large amount of oscillators, among the most used ones are:

- Momentum
- Rate of Change (ROT)
- Relative Strength Index (RSI)
- Moving Average Convergence Divergence (MACD)

Momentum is the simplest type of oscillator measuring the acceleration or deceleration of the trend based on the comparison of the exchange rates in the closing term with the beginning of the observed period (usually 10-12 days). An absolute and relative Momentum can be calculated. If the momentum is positive, the trend is increasing while if the momentum is negative, we observe decreasing trend. If the momentum is strong, the trend is also getting stronger and if the momentum is weaker, the same applies for the trend.

Among other commonly used technical indicators we have Slow Stochastic Oscillator (SSO), Average Directional Index (ADX) and Commodity Channel Index (CCI).

Limitations of the technical analysis

Even the technical analysis has many defenders; there are also many objectors who point out that it is dubious. Among the most common imperfections of the technical analysis are:

- The statement that the history of the price changes is constantly repeating. This statement is not supported by any empirical evidence.
- Many people doubt that reasons of the constant repetition of the price changes exist.
- Many economists think that the advanced stock exchange markets are managed well themselves and not by the trend management of the exchange rates.
- The empirical studies have not proved that by using technical analysis we contract better and above-average results.

Despite the above mentioned facts we can state that the technical analysis has many indicators and tools that are completely safe and can be used successfully. The main point of the technical analysis is not finding the right investment but finding the right time for buying and selling.

4.1.3 General psychological analysis

The psychological analysis is based on the fact that the stock exchange markets are under a strong influence of a mass psychology of the stock audience which affects the stock participants and subsequently the exchange rates. It indicates that the future development of the exchange rate is dependent on the impulses which affect the behavior of the audience – which subsequently sides with either buying or selling the asset. The psychological analysis consists of many theoretical concepts dealing with mass psychology in the stock market. Among the most common are (Caes, 2011):

- Keynes speculative hypothesis
- Bubble theory of speculative markets
- Kostolany stock market psychology
- Drasnar psychological analysis

The mass psychology significance is supported by Kaynese statement: There is no point at paying 25 “money” for an investment which from a perspective point of view has the value

of 30, however you assume that in three months the value will be 20. With that being said the investor has to focus the attention on the predicting of the future changes in the psychological atmosphere of the market and the estimations wisely.

Keynes promoted a theory that any individual without the ability to predict the future and stepping in the market automatically contributes to the mass psychology of the market which consists of large amount of ignorant people (Keynes, 2014).

The Keynes speculative hypothesis is based on the constant increase in the share of the traded asset in the hands of inexperienced investor which leads to other phenomena:

- The markets often react exaggeratedly on insignificant situation – they become more volatile for no reason
- The influence of the mass psychology is constantly increasing
- Investors try to achieve profit in very short period of time – they concentrate on estimation of the behavior of the audience rather than fundaments

The Kostolany stock market psychology states that in a short period of time (max 1 year) the exchange rates are affected by the psychology and the reaction of the market audience while in a long period (1 year +) the prices are affected by the fundamental factors. Kostolany separates the stock audience on two main parts:

- Players – 90% of the market audience, they try to achieve fast profits, no fundamental thinking, they keep going with the "crowd"
- Speculates – they implement long term transactions, they don't have emotional behavior and their thinking is based on fundamental analysis. Most of the times the speculates are a lot more successful than the players.

Bubble theory of speculative markets discusses situations where the exchange rate (price level) increases or decreases without any rational explanation based on a fundamental fact.

After a certain period of time this move stops and goes the other direction until the price level stabilizes. The less experienced investors often suffer critical losses.

Drasnar psychological analysis is based on two human attributes – greed and fear. If the greed is prevailing the people buy, the demand and the price level increases. If they start to fear of losses they start to sell, the supply increases and the price levels decrease. The fear can evolve into panic and stock decrease of the value arises (Rejnus, 2010).

Since the psychological analysis affects the exchange rate / price level mostly in short periods, we can state that the psychological analysis is a short term analysis.

4.1.4 Own analysis

Base on the theoretical aspects from the previous chapter this chapter will present practical specific example of the Bitcoin price evolution. The virtual currency Bitcoin will be analyzed from fundamental, technical and psychological point of view.

Fundamental analysis - Macroeconomic analysis of the Bitcoin

Fundamental analysis not only researches the economic factors but also social, international politics etc. from the most commonly considered factors the one that have the biggest impact on the Bitcoin development are: economic development and monetary policy, the size of the interest rates, the quality of the investment environment, economic and political decision with an impact on Bitcoin, economic crime rate, law system, tax policy. The deductions are clear – the worse it is in the classic economic, political, tax and monetary world, the more people tend to look around "alternative methods". The larger demand there is (even the Bitcoins are restricted and not "endless" as explained in the theoretical part of this work) the more the price is being pushed upwards – unless no political, economic or other boundaries emerge. The Bitcoin price is not affected by all

factors that affect the stock market price level, however there are certain factors which might affect Bitcoin's price crucially.

Since Bitcoin is something highly specific and as an alternate payment system it still looks for its place in the modern world – the fundamental analysis of this currency is rather complicated. Since it is nearly impossible to gather all input parameters (factors) affecting the price of Bitcoin there is no relevance in trying to predict its future development from fundamental perspective – only one either politic, or economic or technical event can crucially influence the Bitcoin's development the one or other way. If we want to at least briefly look into factors that might impact the development of the Bitcoin exchange rate we can state few factors:

- Countries opinion on Bitcoin, legislative changes
- Incidents in the stocks where Bitcoin trade is participating
- There might emerge something "more interesting, even safer and larger" than Bitcoin – however this is not likely to happen in the next years
- Possible worldwide conflict
- A disaster which can generate large energy failures so that technically it won't be able to be worked with Bitcoin – as we know from the previous chapters high capacity computers and webs are important

All this factors can render Bitcoin from day to day completely worthless. On the other hand there can be significant increases connected with the devaluation of other currencies. In this case there can be a mass psychosis and its price might jump about hundreds of % in a single week. At the time of its existence the bitcoin has suffered a few very high jumps and 4 times its price has jumped by very high percentual increase in extremely short period of time. Subsequently in a very short period of time the price level "corrected" (in a matter of days). Base on the facts above we can state that fundamental qualitative analysis is not significant and prediction for the future development of the currency from this perspective is irrelevant. In order to create a solid fundamental analysis we lack of input indicators and information (in comparison to stocks) and on the other hand there is too many variable indicators that might change its development from day to day.

If we still want to make a gross fundamental estimation of the prediction of Bitcoin price it could be as follows:

If more people think that the inflation and the monetary system prevents us from saving more money, the Bitcoin demand will rise – however in case that more appropriate conditions for its spending arise. The higher demand on the Bitcoin, the higher prices of Bitcoin we can expect. The most probable scenario is that the price will continue to have large jumps and subsequent corrections, however the gaps between the jump and the correction will decline – the price will become more stabilized and loss volatile. Only an extreme politic, economic or geographic situation might change the price development.

In the prediction of the future development of the Bitcoin the technical analysis should be more suitable, however the large volatility of the currency can still prevents us from obtaining enough reliable information.

Technical analysis

Graph analysis

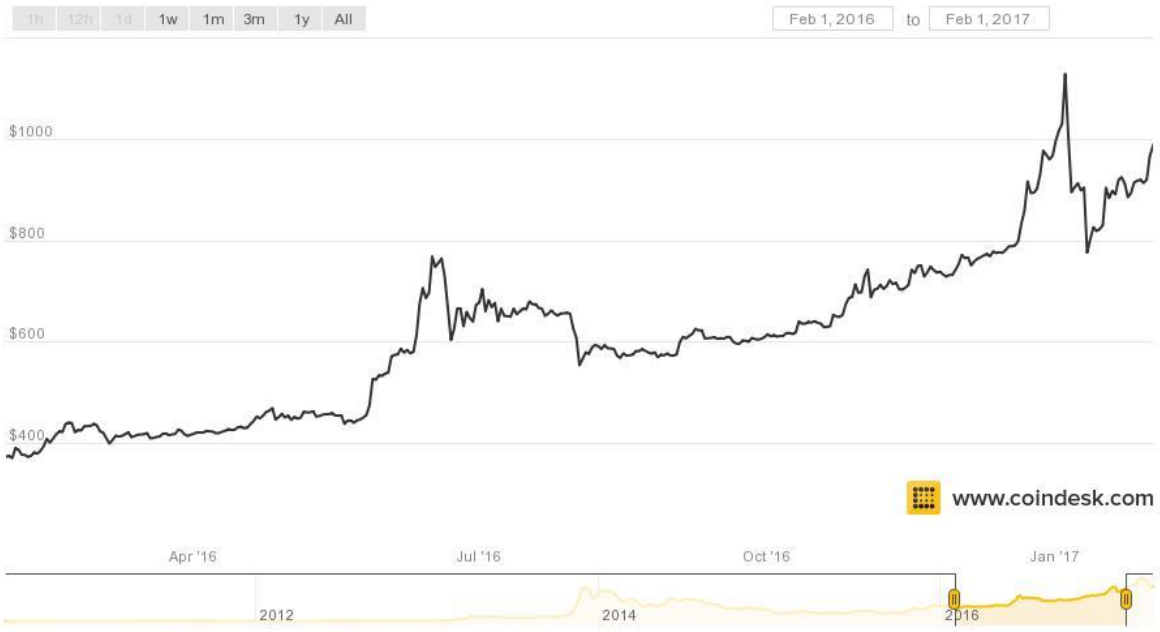
Within the scope of the graph analysis graphs derived from the exchange rates or capacity of the trades are being investigated and analyzed. Some methods are simpler other more complex however in all cases we need computer technology in order to process the input data into charts.

Analysis of the increasing and decreasing trends

In this part of the analysis we use the support and resistance values, trend lines and trend channels.

One of the main functions of the technical analysis is identifying whether the trend in increasing or decreasing – in the increasing trend the maximum and minimum values are increasing while in the decreasing these values are declining. In the prediction of the future development of the currency another factor is rather important – the capacity of the trades. If the capacity of the trades increases, then the current trend should continue. If the capacity of the trades decreases, then we should be expecting a change in the current trend. As for the capacity of the Bitcoin trades – in view of the fact that it is very specific currency – it is a lot harder to predict the trade capacities for a period of time (than in the stocks for example). The capacity of the Bitcoin trade is the same as the exchange rate – very volatile.

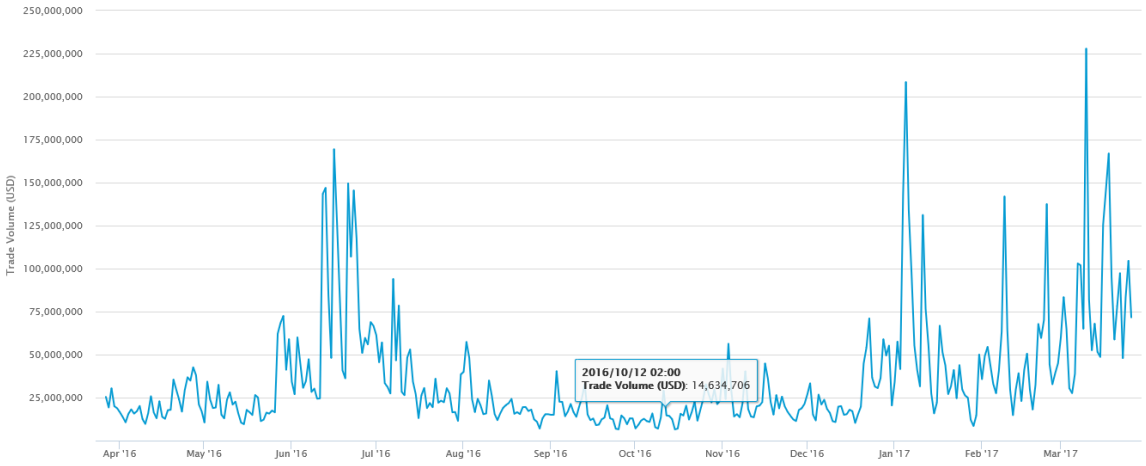
Chart 7 - Bitcoin price in USD from February 2016 to February 2017



Source: Coindesk.com

We can state that if the trade volume increases it means the current trend will strengthen. The price also increases – Dows theory. We can observe that by comparing the two charts, the trade volume in USD and the evolution of the Bitcoin price in USD in the past year.

Chart 8 - Bitcoin trade volume in USD from April 2016 to March 2017



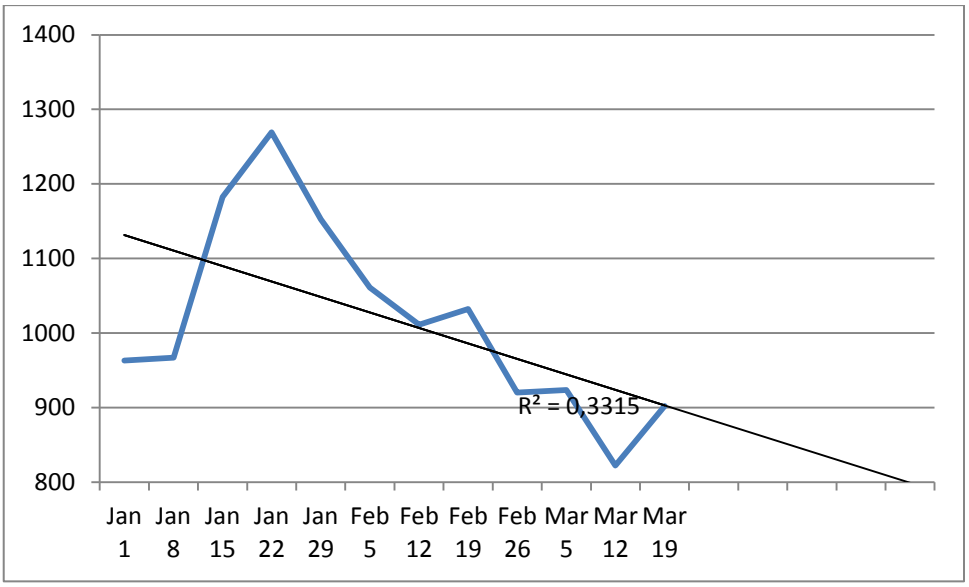
Source: Blockchain.info

Looking at chart 7 we can observe that the trend of the Bitcoin price was increasing the whole year.

As for the support and resistance levels, since the Bitcoin is relatively young currency and is too volatile, we can't speak about these levels in its all development. By the time this part of the work has written, the support level of the Bitcoin was stable around $ 900.

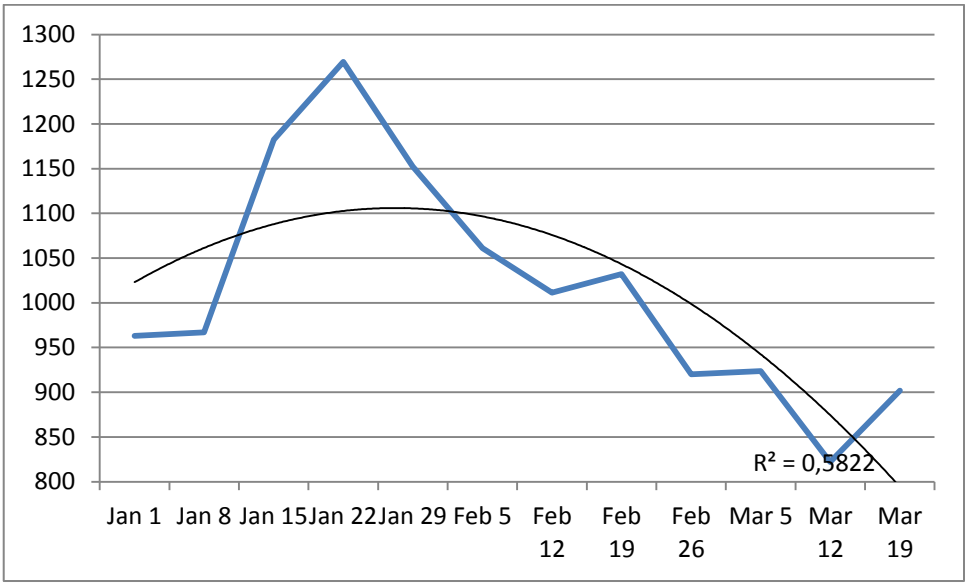
Another term used in the technical analysis are the trend lines – lines connecting the minimums of the increasing trend or maximum of the decreasing trend. The longer the line is, the more dots it connects and the lesser angle it has with the horizontal axe, the more the information is reliable.

Chart 9 - Trendline of the evolution of the Bitcoin Price in USD in the past 3 months



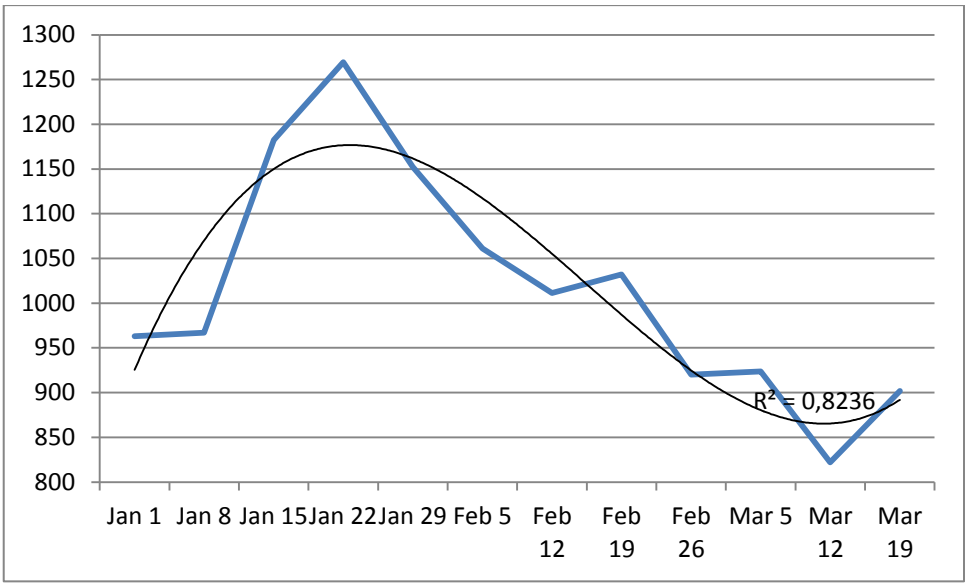
Source: Cointask.com, Own Computation done in Microsoft Excel

Chart 10 - Squared trend line of the Bitcoin price in USD



Source: Coindesk.com, Own Computation done in Microsoft Excel

Chart 11 - Cubic trend line of the Bitcoin price in USD



Source: Coindesk.com, Own Computations done in Microsoft Excel

Analysis based on technical indicators

Most of the technical indicators require complex mathematical computations for which software is being used. Since Bitcoin is very young currency it is hard to use many of the indicators and the computations will not be accurate. In the technical analysis this work depicts one of the most common indicators of the technical analysis: the moving averages. Moving averages are the most significant and important tool of the technical analysis. Better overview of the method itself is depicted in the previous chapters of the thesis. The practical part of the work verifies the theory that the buying signal is being indicated by the intersection of the moving average curve and the exchange rate curve is from the bottom of the moving average one and the selling signal is the other way.

In this work simple and exponential moving averages had been used – 14 day moving averages.

Chart 12 - Simple 14-day moving average of the bitcoin price in the past 3 months

Source: Coincharts.com, 2017

Chart 13 - Exponential 14-day moving average of the Bitcoin price in the past 3 months

Source: Coincharts.com, 2017

We can state that the theory in which we generate profit if we consider that the buying signal is when the moving average curve intersects the exchange rate curve from the bottom while the selling signal is when it intersects it from the top – the theory is applicable in Bitcoin.

Comparing the exponential moving average with the simple one we observe that the exponential provides better output – assigns higher importance on the newer information rather than the old one.

In the next step there is comparison of moving averages of different length, 7-day and 30-day.

Chart 14 - 7-day exponential moving average of the Bitcoin price in the past 3 months

Source: Bitcoincharts.com,2017

Chart 15 - 30-day exponential moving average of the Bitcoin price in the past 3 months

Source: Bitcoincharts.com, 2017

Comparing the 14-day and the 7-day exponential moving averages the 14-day showed the buying and selling points correctly while in the 7-day there were a bit misleading. The 7-day moving average indicated more signals however it might indicate a wrong one as well. On the other hand the 30-day moving average indicated the least amount of buying/selling signals. To summarize all graphs indicated buying and selling points relatively good, the interval between the buying and selling points were in most cases short and the difference between the buying and selling price was relatively small with the exceptions of the high growth of the price in February. The 7 and more day moving average method does not have crucial impact for the "big" investors. The 10+ day moving average method might be recommended to smaller careful investors who want to prevent losses and have a small, secure profit.

The moving average method should be recommended to the investor not from maximizing profit point of view but from minimalizing losses point of view. It can't be used for confident prediction either.

The method might be efficiently used when predicting the direction of the price of the asset, however not when predicting the actual price nor the time how long the price will

rise/fall. Since a 7-day moving average tended to be the best method, it is only good for short term information – no long term predictions can be safely done with this method.

Chart 16 - 7-day and 14-day moving average comparison

Source: Bitcoincharts.com, 2017

Chart 17 - 14-day and 30-day moving average comparison

Source: Bitcoincharts.com, 2017

The indicators for safe buying and selling the Bitcoin tend to be where the both moving averages intersect. The graphical results confirmed the validity of the 7-day and 14-day theory. The 14-day and 30-day moving average intersections did not have the proper

amount of intersections – the buy/sell signals. For the prediction of the currency is the trade volume important for the investors so in chart 18 is trade volume and the currency development in the past 6 months.

Chart 18 - Bitcoin price vs Bitcoin trade volume from October 2016 until March 2017

Source: Bitcoinity.org/markets, 2017

Another technical indicator is the Aaron Oscillator which show us the current trend and whether it will most likely continue or not. Readings above zero indicate that increasing trend is present while lower that zero indicate that decreasing trend is present. The indicator can be seen in chart 19.

Chart 19 - Evolution of the Bitcoin price and Aaron oscillator

Source: Bitcoincharts.com

Chart 20 - Moving average convergence-divergence

Source: Bitcoincharts.com, 2017

The moving average convergence-divergence indicator shows the reader the correct time to sell – when the curve is dropping to the signal line, we should sell the currency while it emerges from the negative values it is time to buy.

Bitcoin and Litecoin correlation

Since from its launch in 2011 Litecoin is the main competitor of the Bitcoin, this work depicts the correlation betwee those two currencies (in the past 3 months). Correlation is the dependence between two or more variables – the correlation coefficient "r" (Pearson's coefficient) measures the strength and the direction of the linear relationship among the variables. The correlation coefficient is calculated as follows:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{(n-1)s_x s_y} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}},$$

Where "n" is the number of measurements, x and y are the values of the measured units, s is the standard deviation and $\bar{x}$ and $\bar{y}$ are the sample means.

The correlation coefficient values range from -1 to 1 where 1 is total positive correlation, 0 is no correlation and -1 total negative correlation.

Table 2 - Weekly Bitcoin price in the past 3 months

Date	Bitcoin Price in USD
Jan 1	963,1
Jan 8	966,86
Jan 15	1182,5
Jan 22	1269,41
Jan 29	1152,2
Feb 5	1061,07
Feb 12	1011,27
Feb 19	1032,24
Feb 26	920,02
Mar 5	923,63
Mar 12	821,97
Mar 19	901,99

Source: Cointask.com

Table 3 - Weekly Litecoin Price in the past 3 months

Date	Litecoin Price in USD
Jan 1	4,5
Jan 8	3,99
Jan 15	3,906
Jan 22	3,83
Jan 29	3,82
Feb 5	3,955
Feb 12	3,79
Feb 19	3,807
Feb 26	3,9255
Mar 5	4,0009
Mar 12	3,973
Mar 19	3,93

Source: coingecko.com

After substituting the measurements to the main formula we receive the Pearson coefficient r= -0.34385. This is weak negative correlation – the more one price rises the other one does not and reverse way. We have to keep in mind that the more measurements we have, the bigger significance we have on the measurement.

Table 4 Gold prices in the past 3 months

Date	Gold Price in USD per Ounce
Jan 1	1150
Jan 8	1178
Jan 15	1999,8
Jan 22	1204,3
Jan 29	1191,78
Feb 5	1223,1
Feb 12	1224,9
Feb 19	1238,74
Feb 26	1257,66
Mar 5	1231,4
Mar 12	1203,53
Mar 19	1232,7

Source: www.kitko.com

The gold price is taken from the British server www.kitko.com which has the closest overall prices to the major stock markets.

After substituting the measurements to the main formula we receive the Pearson coefficient r= 0.37923. This is positive relationship however not very strong. It still indicates us that the price of Bitcoin and gold on the world's largest stock markets tend to increase and decrease together.

Psychological analysis

The psychological analysis analyzes the mass psychology of the market participants. Based on that the traders act, buy or sell – these actions affect the changes in the currency.

The current situation of the Bitcoin market is closely confirmed by the Keynes speculative hypothesis theory – the still increasing share of a trading active in the hands of inexperienced investors. In 2011 people learned about the extreme increase in the Bitcoin price almost 100x in 7 months – this ended up attracting a lot of new investors. The market become too volatile and started to succumb more and more to mass psychology. All investors wanted the highest profit as they can possibly generate in a small period of time. It happened what Keynes consider rather dangerous – speculations charged bigger scope than the hesitation based on fundamental analysis.

The development of the Bitcoin is also confirmed by the Kostolany stock market psychology – 90% of the stock participants are inexperienced and want high profit as soon as possible. Another evidence for the volatility of the exchange rate.

Drasnar psychological analysis was proven also – the two human characteristics – greed and fear decided about the faith if the currency. When the greed prevailed, people bought more, the exchange rates rose rapidly. When the people started to fear of losses, they started to sell and the rate rapidly decreased.

Prediction model

The creation of a prediction model in a long term is due to lack of input information almost impossible (from the fundamental analysis point of view). We can work on the presumption – hypothesis what would probably occur.

The technical analysis serves us as a short term predictor – based on the actual trade volume and certain conditions. We can predict with the technical analysis for a few days, maybe weeks. For a long term investors the technical analysis might serve as a source for minimalizing losses and for generating small amounts of profit.

The psychological analysis is quite effective when it comes to Bitcoin due to the facts mentioned above. It starts to play major role when the stock market is occupied with inexperienced audience.

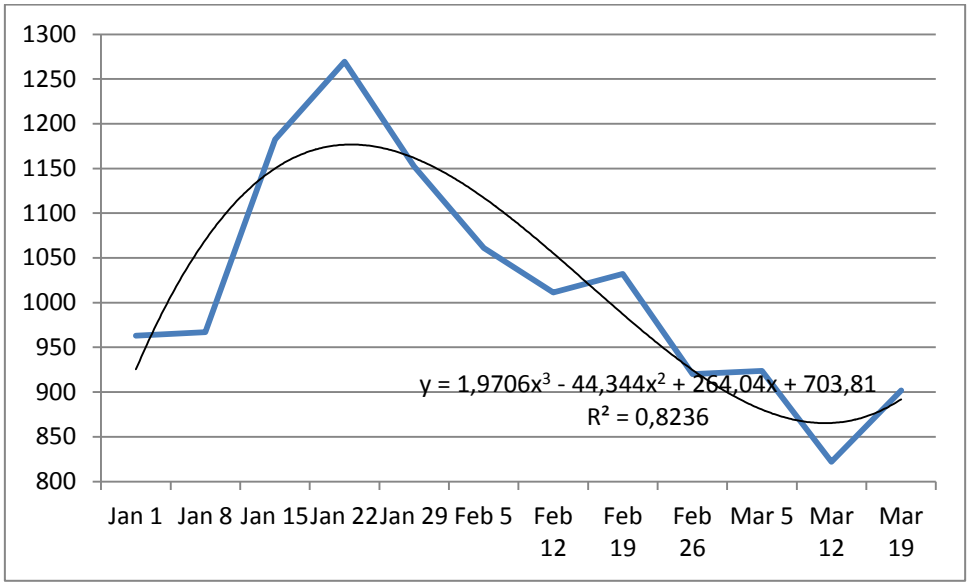
Considering the whole mentioned above the summarization of the brief prediction model is as follows:

- If countries do not introduced sanctions against Bitcoin (which is not probable) its price will most likely continue to rise – USA, China, Japanan and EU are the most important countries when it comes to the economy of Bitcoin.
- Considering the fact that the overall capacity of Bitcoin is solidly fixed, the prices might go higher in the next year exponentially
- After every rapid increase of the Bitcoin price we can observe a 20%-40% decrease (of the latest peak) – this trend will most likely continue

- If the security system of Bitcoin is hacked, there could be significant lowering in the interest if the investors in Bitcoin
- A possible worldwide conflict might render Bitcoin and make it worthless
- In case of decrease of the USD, the Bitcoin price should rapidly increase

Even we mentioned several times that such prediction might be inaccurate here is prediction model based on trend analysis for the next 3 weeks (after March 19).

Chart 21 The Cubic trend line for the evolution of Bitcoin price in USD in the past 3 months



Source: Own computations in Microsoft Excel

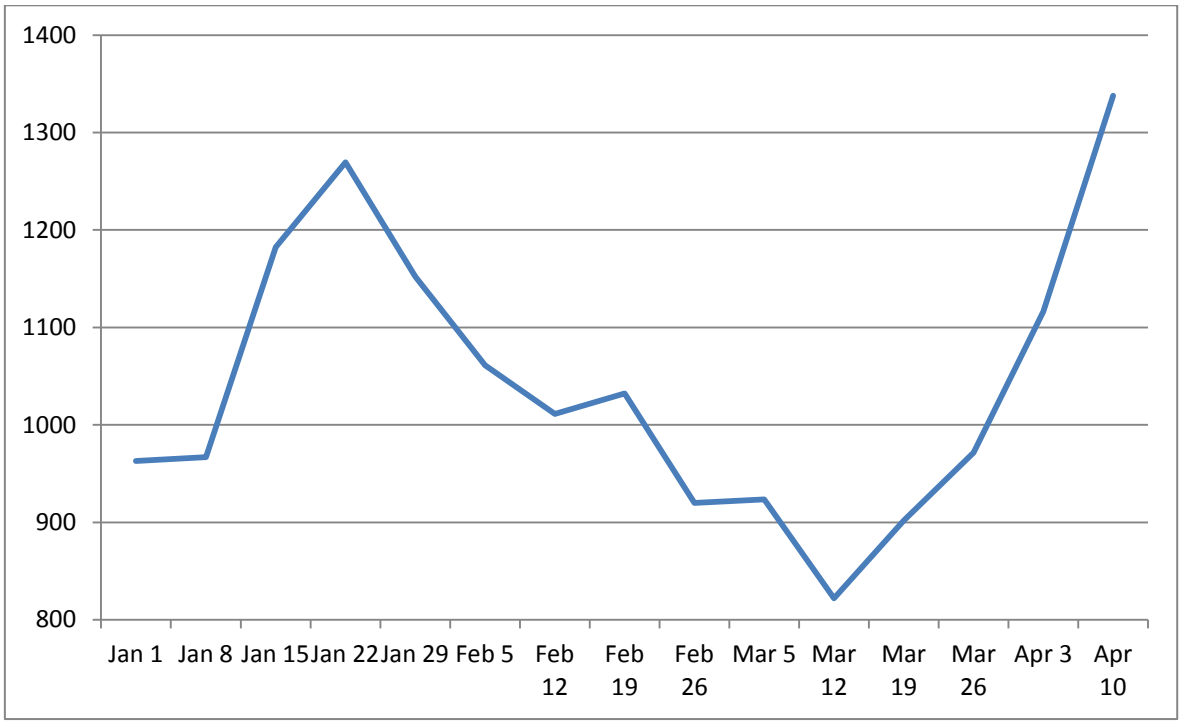
The cubic trend line is chosen because of the highest coefficient of determination (R^2 value).

Table 5 Bitcoin Price in USD with the predicted values

Date	Bitcoin Price in USD
Jan 1	963,1
Jan 8	966,86
Jan 15	1182,5
Jan 22	1269,41
Jan 29	1152,2
Feb 5	1061,07
Feb 12	1011,27
Feb 19	1032,24
Feb 26	920,02
Mar 5	923,63
Mar 12	821,97
Mar 19	901,99
Mar 26	971,6022
Apr 3	1116,2724
Apr 10	1337,785

Source: Own computations

Chart 22 Bitcoin price with the predicted data



Source: own computations

As we see on the graph above the predicted values are a lot higher than the latest value. The price is expected to grow exponentially and even reach its peak for this year, however this is not likely to happen. As we mentioned above the factors affecting Bitcoin price are very hard to measure and simple statistics model cannot predict its development.

5. Conclusion

In the theoretical part of the thesis are included the most important theoretical aspects of the Bitcoin including how it works and how is being created. As for the practical part the thesis reviews the most important methods of the fundamental, psychological and technical analyzes and applies them on the development of the Bitcoin price.

After examining the possibilities of the prediction of the Bitcoin from fundamental and technical point of view – due to the very uniqueness of the currency most of the technical and fundamental methods are not applicable or does not work the same way as with other currencies/assets. Neither fundamental nor technical analysis does not give results based on which we might develop future investment strategy.

The fundamental factors (which most of them are unclear or even unknown) are not possible to be discovered – nor from time period perspective nor from the possible situations mentioned in the macroeconomic analysis. The currency is relatively young (7,5 years) and the first two years of its existence its exchange rate was almost 0 – which does not contribute to the analysis at all.

The technical analysis partly enables us short term prediction, however in longer term there is no quantitate scope. However it enables to generate small profits and to obviate losses – for a very short time.

The psychological analysis observes that most of the Bitcoin trades are in the hands of inexperienced investors who can easily succumb into the mass psychosis. The consequences of this is the high volatility of the currency as well as well as very fast and high profit – on the other hand very fast and high losses can occur.

In the present day the future of the Bitcoin is not very bright even more retailers start to accept Bitcoin as a payment system. The main factors which have impact on the Bitcoin rate development are simply not quantified. They are not numbers which we can search for and subsequently mathematically process. We cannot predict politics nor psychology of the individuals on the stock market.

As for the hypothesis (the price of the Bitcoin is very hard to predict due to high volatility of the currency) it was accepted.

6. References

Antonopoulos, A. (2014). Mastering Bitcoin. 1st ed. O'Reilly Media.

Caetano, R. (n.d.). *Learning Bitcoin*. 1st ed.

Franco, P. (2014). *Understanding Bitcoin*. 1st ed. Hoboken: Wiley.

Frisby, D. (2014). *Bitcoin*. 1st ed. London: Unbound.

Furgang, K. (2011). *How the stock market works*. 1st ed. New York: Rosen Pub.

Green, S. (2016). *Bitcoin : The Ultimate A - Z of Profitable Bitcoin Trading & Mining Guide Exposed!*. Scott Green

Keller, D. (2010). *Breakthroughs in Technical Analysis*. John Wiley & Sons

Keynes, J. M. (2016). *General Theory Of Employment , Interest And Money*. Atlantic Publishers & Dist

McAllen, F. (2012). *Charting and Technical Analysis*. Fred McAllen

Palat, R. (2016). *Fundamental Analysis for Investors: 4th Edition*. Vision Books

Reamer, N. (2016). *Investment: A History: A History*. Columbia University Press

Schlichting, T. (2013). *Fundamental Analysis, Behavioral Finance and Technical Analysis on the Stock Market.* GRIN Verlag

Stevenson, J. (2013). *Bitcoins, litecoins, what coins?: A global phenomenon*. 1st ed.

Online references

BitcoinMiningCom (2013) What is Bitcoin mining? Available at: https://www.youtube.com/watch?v=GmOzih6I1zs (Accessed: 16 March 2017).

BitcoinWebH and Bitcoin (no date) Bitcoin history: The complete history of Bitcoin [Timeline]. Available at: http://historyofbitcoin.org/ (Accessed: 2 March 2017).

BUNTIX, J. (2015) Fiat currency vs Digital Currency. Available at: http://digitalmoneytimes.com/fiat-currency-vs-digital-currency/ (Accessed: 12 February 2017).

Coinbase (2016) Buy and sell Bitcoin. Available at: https://www.coinbase.com/about (Accessed: 12 February 2017).

Collective of Authors (2011) Everything you need to know about Bitcoin mining. Available at: https://www.bitcoinmining.com/ (Accessed: 21 March 2017).

GILSON, D. (2013) Reviewed: BTC-e cryptocurrency exchange. Available at: http://www.coindesk.com/btc-e-bitcoin-exchange-review/ (Accessed: 7 January 2017).

Investopedia.com (2007) 'Exploring Oscillators and indicators: MACD', in Available at: http://www.investopedia.com/university/indicator_oscillator/ind_osc6.asp (Accessed: 25 March 2017).

NAKAMOTO, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf (Accessed: 10 March 2017).

WARD, H. (2015) Bitcoin: The fastest growing currency in the world. Available at: https://www.bond.org.uk/news/2015/02/bitcoin-fastest-growing-currency-world (Accessed: 19 March September 2017).