

Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Economics



Bachelor Thesis

Bitcoin and other virtual currencies

Inna Chetchasova

© 2018 CULS Prague

BACHELOR THESIS ASSIGNMENT

Inna Chetchasova

Economics and Management

Thesis title

Bitcoin and other virtual currencies

Objectives of thesis

The main goals of this Bachelor thesis are to justify what is virtual currency, identify several types of it, assess the impact of these currencies on the modern world economy, to compare virtual currencies with fiat ones by analyzing several paper works, books and articles of various economists and journalists.

Methodology

This Bachelor thesis is divided into two parts: theoretical and practical. Practical part consists of timeseries forecasting, technical analysis and correlation matrix analysis performed by the author in order to make conclusions about mentioned objectives.

The proposed extent of the thesis

40 – 60 pages

Keywords

cryptocurrency, virtual, finance, economy, bitcoin, exchange rate

Recommended information sources

- Davis, G. (1994). A history of money: from ancient times to the present day. 1st ed. Cardiff: University of Wales Press
- Franko, P. (2014). Understanding Bitcoin: Cryptography, Engineering and Economics. 1st ed. John Wiley & Sons
- Genkin A., Mikheyev A. (2018). Blokcheyn. Kak eto rabotayet i chto zhdet nas zavtra. Moscow: Alpina Publisher
- Kenny, D. A. (1979). Correlation and causality. 1st ed. New York: John Wiley & Sons
- Lee J. J., Murphy J. J.(1986). Study Guide to Technical Analysis of the Financial Markets: A Comprehensive Guide to Trading Methods and Applications. 1st ed. New York Institute of Finance.
- Lowry, S. (1998). The magic of moving averages. 1st ed. Traders Pr; Imprint Wasendorf & Associates Inc.
- Rothbard M. N., (1963). What Has Government Done to Our Money? Ludwig Von Mises Institute

Expected date of thesis defence

2017/18 SS – FEM

The Bachelor Thesis Supervisor

Ing. Petr Procházka, Ph.D., MSc

Supervising department

Department of Economics

Electronic approval: 5. 3. 2018

prof. Ing. Miroslav Svatoš, CSc.

Head of department

Electronic approval: 6. 3. 2018

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 07. 03. 2018

Declaration

I declare that I have worked on my bachelor thesis titled "Bitcoin and other virtual currencies" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 14.03.2018

Inna Chetchasova

Acknowledgement

I would like to thank Ing. Petr Procházka, MSc, Ph.D for his valuable advises and overall help and support granted to me during the writing of this thesis.

Bitcoin and other virtual currencies

Summary

In the given Bachelor thesis various cryptocurrencies including Bitcoin will be analysed to obtain a better understanding of the way of functioning. The main aim of this thesis is to answer the question: “is a cryptocurrency able to replace fiat currencies which are commonly used as main way of payment in the modern world?” Thesis itself is divided into parts: theoretical and practical.

Various books and articles of researchers in economic and legal field were reviewed for the purpose of obtaining better understanding of the topic and answering mentioned question. In result of theoretical part of thesis, it was concluded that exchange rate of cryptocurrency is strongly dependant on the social opinion and other psychological factors. However, it was decided to make a financial analysis to inquire if there are any economic factors influencing the position of virtual currency.

In the practical part of this thesis, various economic tools and analyses were implemented to get a detailed view on the behaviour of cryptocurrency. An attempt to predict the future behaviour of virtual money was made by mean of timeseries forecasting. Technical analysis was performed for making an overview of the current position of electronic currency. Correlation matrix was conducted to find out whether fiat and virtual currencies depend on each other.

Keywords: Cryptocurrency, Money, Economy, Finance, Exchange Rate, Bitcoin, Analysis, Virtual.

Bitcoin a další virtuální měny

Souhrn

V dané bakalářské práci jsou analyzovány různé kryptocity (kryptoměny) včetně Bitcoinu, a způsoby jejich fungování v současném ekonomickém světě.

Hlavním cílem této práce je najít odpověď na otázku: "Zda-li kryptoměny jsou schopné nahradit fiat měny, které jsou běžně používány jako hlavní způsob platby v moderním světě?" Bakalářská práce je rozdělena na dvě části: teoretickou a praktickou.

Za účelem lepšího pochopení tématu a odpovědi na uvedenou otázku byly revidovány různé knihy a články výzkumných pracovníků v ekonomické a právní oblasti. V průběhu teoretické části práce bylo konstatováno, že směnný kurz šifrovací kriminality je silně závislý na sociálním pohledu a dalších psychologických faktorech. Bylo však rozhodnuto provést finanční analýzu a zjistit, zda existují ekonomické faktory, které ovlivňují pozici virtuální měny. Byly revidovány různé knihy a články výzkumných pracovníků v ekonomické a právní oblasti za účelem lepšího pochopení tématu a odpovědi na uvedenou otázku. V důsledku teoretické části práce bylo konstatováno, že směnný kurz šifrovací kryptoměny je silně závislý na sociálním pohledu a dalších psychologických faktorech. Bylo však rozhodnuto provést finanční analýzu a zjistit, zda existují ekonomické faktory, které ovlivňují pozici virtuální měny.

V praktické části práce byla použita řada ekonomických nástrojů a analýz, které umožnily získat detailní pohled na chování kryptoměn. Pokus o předvídání budoucího chování virtuálních peněz byl proveden pomocí předpovědi časových plánů. V důsledku technické analýzy jsme obdrželi přehled současného stavu elektronické měny. Na závěr byla provedena i korelační matice, která stanovila, zda fiatové a virtuální měny závisí na sobě.

Klíčová slova: Krypto-měna,, peníze, ekonomika, finance, směnný kurz, Bitcoin, analýza, virtuální.

Table of Contents

1. INTRODUCTION.....	11
2. OBJECTIVES AND METHODOLOGY	11
2.1. Objectives.....	11
2.2. Methodology.	12
3. THEORETICAL PART	12
3.1. History of Virtual Currency	13
3.2. Bitcoin. How does it work?.....	16
3.2.1. Main advantages and disadvantages of cryptocurrency on the example of Bitcoin. .	19
3.3. Predictions for virtual currencies.	22
3.4. Time series forecasting analysis.	25
3.5. Technical analysis.....	26
3.6. Correlation Matrix.	28
4. PRACTICAL PART	29
4.1. Time series analysis.....	29
4.2. Technical Analysis.....	35
4.3. Correlation matrix	40
5. RESULTS AND DISCUSSION.....	41
6. CONCLUSION	42
7. REFERENCES	43

List of Tables

Table 1: Model 1: OLS	30
Table 2: Indicators of Model 1	31
Table 3:Model 2: OLS	31
Table 4:Indicators of Model 2	32
Table 5:Analysis of the quality of in-sample forecast	32
Table 6:Forecast evaluation statistics	33
Table 7: technical analysis indices	37
Table 8:Moving Averages for various periods	38
Table 9:Pivot Points	39
Table 10:Summary of Technical Analysis	39
Table 11: Correlation matrix	41

List of figures

Figure 1: Timeseries for Bitcoin (2011-2017)	30
Figure 2: Graph of forecast for the last week of sample.....	34
Figure 3: Graph of forecast for the next week of sample	34
Figure 4: Price of Bitcoin	35
Figure 5:Candlestick chart	36
Figure 6: Price of BTC in 2017.....	40

List of Abbreviations

BTC – Bitcoin

ETH – Ethereum

USD – American Dollar

GBP – British Pound

EUR – Euro

RUB – Russian Ruble

CZK – Czech Crown

MA – Moving Average

TA – Technical Analysis

BC. E. – Before Common Era

US – United States

IBM - International Business Machines

TPM – Trustful Platform Module

P2P – Peer-to-peer

DoS-attack - Fraggle attack

POW-tasks – Proof of Work

1.Introduction.

Human society cannot be imagined without money. Money is a specific commodity of maximum liquidity that is universal equivalent to the value of other goods or services. The development of money is inextricably linked with development of the entire human civilization. Goods, products and weapons, coins in various types from bone to gold, paper banknotes, stocks are only small part of what was and still is used as money. (Glyn Davis, 1994)

With development of computer technologies and communication networks, the world entered era of "Electronic money". Coins and banknotes are gradually being replaced by plastic equivalents such as payment cards; also, Internet is full of payment systems, originally created only for electronic payments, such as PayPal, WebMoney, QIWI, etc. Progress does not stand still, and cryptocurrency is being developed - brand new mean of payment of the XXI century, which has a number of significant differences from other types of electronic money which are described in detail in the first article published by Satoshi Nakamoto in 2009 called "Bitcoin: A Peer-to-Peer Electronic Cash System". (Rebecca Burn-Callander, 2014)

At the moment, cryptocurrency is a type of money which a huge number of people around the world enjoy. Nowadays, according to Wikipedia.com, there exist 92 virtual currencies. Of course, most of them are not as popular and wide-known but the situation could change in just a couple of years.

2.Objectives and methodology

2.1. Objectives

This Bachelor thesis aims to inquire what is virtual currency, identify several types of it, assess the impact of these currencies on the modern world economy, compare virtual currencies with fiat ones by analyzing several paperwork, books and articles of various economists and journalists. The goal of this study is to clarify position and status of digital forms of money, in particular, Bitcoin and other cryptocurrencies in their current state. The main task is to determine the viability and necessity of Bitcoin as a financial instrument, determining the need for its adoption. In this paper, history of development of

cryptocurrency will be closely inquired, as well as currency's positive and negative sides; its role in the modern economy will be analyzed based on various works of known economists. Relating to the numerous crises of the modern financial system, the relevance of issuing alternative methods of building the world financial system is difficult to underestimate.

2.2. Methodology.

This Bachelor thesis is divided into two parts: theoretical and practical. Practical part consists of time series forecasting, technical analysis and correlation matrix analysis performed by the author in order to make conclusions about mentioned objectives. For that purpose, numerous works of researchers were reviewed and described in this paperwork. Stated methods were used to observe behavioral side of cryptocurrency and to make a conclusion on whether it should be treated as a currency at all considering its non-stable and swiftly changing character.

Current data was taken from diverse sources for analysis performing in order to get a result which is not dependent on the data source. Additionally, issued timeframe differs in accordance with the requirements of analysis.

3. Theoretical Part

In the theoretical part of this thesis the history of money and cryptocurrency itself was overviewed to get a basic idea on background of the chosen topic. The technology of functioning was inquired and deeply examined. Number of existing cryptocurrencies and the way they are treated in different states were studied.

Main advantages and disadvantages were described and predictions for the future development of Bitcoin as an example of cryptocurrency were made by the mean of researching and reviewing books and articles of known economists and financial experts. The theory of time series, technical analysis and correlation matrix which were used afterwards on practice, were described in this part of thesis as well.

3.1. History of Virtual Currency

Nowadays none of us could imagine the world without money, although that is logical that money did not come to the world with the first Homo sapiens. As it is described by Glyn Davies in his book "A History of money from the ancient times to the present day" published in 1994, before physical money was invented, barter was initiated and was successfully functioning for many decades. However, this process on a grand scale became computationally impossible as soon as moderate standard of living had been achieved and, despite the growing importance of barter in social life and economy in the last four or five decades, modern societies were not able to exist without implementation of new monetary systems anymore. (Glyn Davies, 1994).

Glyn Davies in previously mentioned book also describes the second stage of development which was the so-called commodity money, consisted of shells and pearls, stones with holes in the middle, fur and animal skins, salt bars, metal stubs, etc. This form of money solved the problem of the difficulty of valuing goods, the problem of division, taxation and inconvenience of use to some extent, but often introduced the problem of easy falsification and lack of control over the money supply. (Glyn Davis, 1994)

Gradually, the role of money passed to metals. It is known that at first there were metal objects (arrowheads and spears, nails, utensils), then ingots of different shapes. Since the VII century BC. E. coins came into circulation. Metal has contributed to a sharp expansion of the usage of this type of money and therefore the problem of trust was solved. (Glyn Davis, 1994)

A coin is historically the first organized, universal form of metallic money as it is stated in. With the expansion of the use of metal money in exchange and the involvement of not only gold and silver money, but also various alloys from them, the question of confidence in one or another ingot again arose, because each time one had to check the specific gravity of the precious metal itself in the ingot. To increase confidence in the metal, as an intermediary goods, it was decided to make dimensional pieces (bars of fixed weight) and designate this weight in the form of a stigma on the very piece. At the same time, the stigma had the right to place either a state or a private mint, entrusted with state confidence (special diploma). Later on, the coinage was strictly centralized and was carried out only by state mints. (Glyn Davis, 1994)

Once the credibility of money was confirmed by the authority of the state (for the first time in coins), the question of trust in money became a matter of trust for the economy of the state. (Grandars.ru, 2017).

After a while, paper money appeared, initially as a form of guarantee for the issuance of their stored security by banks and depositories. Such money has further simplified the trade due to the physical ease and convenience of large amounts of money. The first form of paper money is a promissory note; The written obligation of the depository to give the bearer the stored value (most often, valuable metals and coins) It was then that the first banks began to be based. Those who accepted deposits did not give interest on them, but they came up with and began to give loans, and investors, concerned about the increasing profits of store owners, tried to find the reason for the super profits that led to the fact that large sums of money were concentrated with bankers. It turned out that they conducted a partial reservation system, which is used to this day. This moment is the paramount problem of the modern economy in the author's understanding. As a result, investors demanded that they also be paid interest for their contribution and settle down on it. The gold standard, which implies securing the US dollar as a world reserve currency with gold and guaranteeing their exchange at a fixed exchange rate, lasted until 1971, when the US refused to freely exchange dollars for gold. The reason, as usual, is one - the mercenary aims of the regulator, which caused issue a huge amount of dollars, not provided with real gold. From this moment, the extensive development of the financial sector, stock markets and derivatives markets has gone, which has now ceased to be tied to fundamental concepts, at least to such a basic thing as the value of metal, which previously was the provision of value for money. (Murray N. Rothbard, 1963)

Cryptocurrency in its history of development is very young, but it also appeared only as high technological breakthrough in the level of human development. Why did this happen at all? In the 20th century, the money underwent significant changes, gold and silver receded into the background, paper money began to develop in massive quantities with declarative gold, and by the end of the century various electronic payment systems appeared. The main reason is that all money is controlled strictly by the Central Banks which does not allow to have a full liberty of action to people, therefore, alternative (not centralized) payment system started developing. (Rebecca Burn-Callander, 2014)

Originally, direct transfer of cash made remote payments. At the same time, the parties of the transaction did not have to trust each other. For the seller, the main thing is to get money and make sure of their authenticity. If everything is in order, then the buyer will not have more questions. For the buyer, the main thing was to have a confirmation of sending money, so that the seller could be required to fulfill the obligations. Over time, there were intermediaries, which were trusted by both sides of the deal. The buyer transferred money to the representative of the intermediary, and the seller in another place from another representative received them. Physically, the money did not always have to be transported, since the preliminary stock could be used. This made it possible to speed up and reduce the cost of payments, making them safer. (Pedro Franko, 2014)

Such payment systems became the ability to block or cancel payments. With the development of computer technology, there was an increasing need for electronic payments. But attempts to create "electronic money", which could be transferred between computers as easily and reliably as cash, did not lead to success. The problem was the ability of computers to make an exact copy of any digital information, which could potentially lead to multiple use of the same "coins" for different payments. The buyer could pay for the goods, and then send the exact copy of the electronic "coin" to another seller. Only a third-party trusted intermediary could guarantee sellers no dispute about payment. Control by the intermediary allows the seller to make sure that the buyer has enough money and this will not be a copy of money previously paid to someone. The obligatory nature of the intermediaries made it possible to significantly simplify the system of state control over electronic payments - it was sufficient to establish control over the intermediaries or to require them to control "suspicious" transactions. It also required a reduction in transaction costs, which in some cases were taken up to half of the profit from the transaction. Repeated attempts have been made to create a system of remote payments, which would be cheaper, less dependent on intermediaries, but no less reliable and safer. (Andrey Ostalskiy, 2008)

The first mention of cryptocurrency as a new alternative system of calculations dates back to 1998, the idea of creating them belongs to a Japanese computer engineer named Wei Dai. He described the ideas of the "b-money" cryptocurrency in the mailing of cipher punk. Regardless of him, around the same time, Nick Szabo proposed similar ideas for "bit-gold". Nick Szabo also proposed a model of a market mechanism based on inflation management, and explored some aspects of identifying reliable information in an unreliable decentralized

system. Later, Hal Finney implemented a bundle of hash-chains for a chip-based HashCash system for IBM encryption within the TPM specification. In 2008, a person or a group of individuals under the pseudonym of Satoshi Nakamoto laid the foundation for the creation of a cryptocurrency - a file was published describing the protocol and the operation of the payment system in the form of a peer-to-peer network. According to Satoshi, the development began in 2007. In 2009, he completed the development of the protocol and published the code of the client program. The Bitcoin network was launched. (Heiko Niedermayer, 2016)

3.2. Bitcoin. How does it work?

Bitcoin today has the most extensive and extensive network and is the most liquid cryptocurrency. Bitcoin is non-material and does not have any reference to any state currency, precious metals or natural resources. The Bitcoin course is extremely mobile and is determined solely by the balance of supply and demand. The currency turnover is not controlled by any bodies, departments or organizations and is carried out exclusively between crypto colliers of network participants. Cancellation of the transaction of coins is impossible. Bitcoin is a synchronization network that creates a new payment system and completely electronic money. This is the first decentralized p2p payment network that is serviced by its own users, without central authorities or intermediaries (bitwallio.com). Considering the consumers' point of view, Bitcoin is very much alike to Online Cash. The system uses P2P technology, which allows it to operate without central supervisory authorities; transaction processing and emissions are collectively run thanks to network efforts. Due to its unique properties, Bitcoin opens up new horizons of possibilities that no payment system has provided before. Peer-to-peer (P2P) means that no central authorities issue new money and control the ongoing transactions. The Bitcoin network collectively regulates these tasks. (Genkin A., Mikheyev A., 2018)

Proof of performance - the principle of protecting systems from abuse services (for example, DoS-attacks or spam mailings), based on the need of fulfillment by the requesting party of some rather complicated long-term work (POW-tasks), the result of which is easily and quickly checked by the service party (One-way function). The main feature of these schemes is the asymmetry time consuming - the duration for the initiator of the request and the high speed for the response. (Satoshi Nakamoto, 2009).

SHA-256 Hashing

Cryptocurrency is reliably protected against forgery by means of an algorithm hashing, which is not possible today. Since the result of hashing is unpredictable, there is no algorithm for obtaining the desired result, except random enumeration. If the hash does not satisfy the condition, then the service information block in the header is changed arbitrarily and the hash is recalculated. Usually a large number of conversions is required. When a variant is found, the node sends the received block to other connected nodes that check the block. If an attacker creates a block using a modified version of the program and assigns a reward to himself, this block will not be added to the chain. If there are no errors, the block is added to the chain and the next block must include its hash. (Satoshi Nakamoto, 2009).

Transactions

As a new user, one can start using Bitcoin without understanding the implementation details. As soon as the bitcoin-purse is installed on a computer or smartphone, the first bitcoin-address will be created (which can be created as many times as needed later). After that, it is possible to provide the bitcoin-address to another user so that he can transfer his Bitcoin into your account. This is similar to the way an e-mail works, just the bit-addresses should be used only once. (Genkin A., Mikheyev A., 2018)

In order to manage the received Bitcoin, the addressee must create a new transaction that will take amount of money from the previous address and redirect them to a new one. To prove that a person uses his own Bitcoin to translate, and not someone else's, he must leave his digital signature in the transaction. Then at any point it is possible to make sure that all transactions in the system are valid. (Genkin A., Mikheyev A., 2018)

Chain of transaction blocks

Any electronic payment system is supposed to somewhere and somehow keep record of transactions process. As for Bitcoin, all data is stored in a chain of blocks. Each block consists of a header and a list of transactions itself. The block header has several properties, among which there is so-called "hash" of a previous block. Transactions, as well as blocks, are built into chains, thus, the entire blockchain stores all transactions for the whole lifetime of Bitcoin. (Satoshi Nakamoto, 2009).

Complexity.

The longer gold is mined, the more difficult (costlier by resources) it becomes to extract it. This ensures that inflation will be under control. In Bitcoin, similar behavior is achieved by introducing a function of the speed of the total extracted coins from time. The production rate decreases with time and tends to zero, and Bitcoin's emission volume is limited by the total number of coins to 21 million. The issuance of cryptocurrency is carried out by means of extraction or mining of blocks. Periodically, every 2016 blocks are extracted, the complexity of their extraction is corrected. The adjustment is based on the production rate in the last period and is necessary to maintain the average interval of extraction of blocks at a mark of 10 minutes. (Franko, Pedro, 2014).

Mining is the process of using computing power of computer systems for creating a chain of transaction blocks of cryptocurrency. In each block, the first transaction in the list is a special transaction. Coins are redirected to the one who generated the block in which the transaction is located. Also, the author of the block is transferred to the commission from those transactions that are in the created block. This is a kind of reward for the time and resources spent on generating the unit. Thus, the miners simultaneously extract new coins and conduct all the transactions of the cryptocurrency. If the miners stop their work, the cryptocurrency will cease to exist. Every four years, the award is reduced by half, thus the total number of coins in circulation is stabilizing. To master the largest cryptocurrency resources of a conventional personal computer to date is not enough, and miners use "farms" - powerful computer stations that have superpower. In order to engage in bit-mining, you need to have a good amount to buy equipment. All the equipment for bit-mining is quite affordable, since the main component of such a computer is powerful video game cards that, instead of processing pictures and video, calculate the generation of new bitcoin. Bitcoin's production is meaningful only as long as the cost of Bitcoin is higher than the cost of equipment and electricity. Since the complexity of production is steadily increasing, the least energy-efficient production facilities are gradually eliminated from the process. (Burn-Callander R., 2014).

Nobody has owner's rights on the Bitcoin network, nor does anyone own the technology behind the e-mail. Bitcoin is controlled by all the users worldwide. While developers improve the software, they cannot forcefully change the protocol, because all users are free to choose which software and what version to use. In order to be consistent with each other, all users must use software that runs with the same rules since bitcoin can work correctly

only when full agreement between all users is reached, therefore, all users and developers have an inducement to protect the functioning system. (Burn-Callander R., 2014).

3.2.1. Main advantages and disadvantages of cryptocurrency on the example of Bitcoin.

Advantages:

Decentralization of the monetary system. All transactions, including the issue of a new currency, are recorded in a common history, available to every user. If desired, it is possible to trace the path of each unit until it appears. That's why it is impossible to forge the cryptocurrency, it is possible to not completely delete the transaction history, because it is simultaneously stored on computers and servers of millions of users around the world. (Franko, Pedro, 2014)

Open cryptocurrency code and anonymity. The source code for cryptocurrency and Bitcoin's theory is open. In bitcoin, the same algorithms are used as in internet banking. The only difference between Internet banking is the disclosure of information about the final user. In Bitcoin network, all the information about the transaction is shared (how many, when), but there is no data about the recipient or sender of coins (there is no access to personal information owners of accounts). (Franko, Pedro, 2014)

Peer-to-peer network of cryptocurrency. In such networks, there is no main server, responsible for all operations. Protocols work as a peer-to-peer network, like torrents. Exchange of information (in our case - money) is committed between 2-3 or more client programs. All installed users of the purse program are part of the Bitcoin network. Each of client keeps a record of all transactions completed and the number of Bitcoins on every wallet. Transactions are made by hundreds distributed servers, they are also called "earners". Neither banks, nor tax, nor the state can control the exchange of money between users' wallets. (Satoshi Nakamoto, 2009).

Unlimited possibilities of transactions. Each of the holders of the wallet can pay to anyone, anywhere and for anything. Transactions are not possible to control or prohibit, so that it is possible to make transfers to any point of the world, where there would be another user with a wallet of cryptocurrency. Cryptocurrency works as a "live cash", combining the functions of e-commerce. (Satoshi Nakamoto, 2009).

Very low commission. Payments with the help of cryptocurrency now are made either without a commission, or with incredibly low commissions. Users can include commissions in the transaction to get priority in processing - this gives a faster confirmation of transactions by the network. In addition, there are processing companies that help traders in the implementation of transactions, transferring the cryptocurrency into the currency of the currencies, which are sent directly to the accounts of entrepreneurs day-to-day. Since these services are based on Bitcoin, they offer a commission much lower than when using PayPal or plastic cards. (Genkin A., Mikheyev A., 2018)

Disadvantages:

Insufficient distribution and recognition. Despite all its advantages, Bitcoin payment system has not yet received a large-scale distribution. If you go to the store and ask if it is possible to pay bitcoins there, you will see the seller's round eyes. So, the use of bitcoin for payments is acceptable only in certain areas for now. (Genkin A., Mikheyev A., 2018)

Exchange rate fluctuations. After a rapid increase in bitcoin in the fall of 2013, a substantial number of hunters for easy earnings began to buy this cryptocurrency with speculative goals, and they all "burned out", because since then and until now the course of bitcoin only decreases. Since there is a very certain amount of Bitcoin money typed out, any large transactions can cause quite strong exchange rate fluctuations, which is dangerous for other participants in the system. (Investopedia.com)

Unpredictability. In fact, the bitcoin system is a kind of startup, and it is rather difficult to predict its further development. For now, it successfully passed only its initial stage. How will the system develop further? This can only be assumed, and it is not necessary that these assumptions proved to be faithful. This is a serious minus of bitcoin. (Niedermayer H., 2016)

Lack of guarantees. Owners of bitcoin have no guarantees that they at least can return their invested money back. Exchange rate is to be set by the bitcoin market and could even fall to zero considering the global circumstances. No one can ensure that this will not happen. In addition, bitcoin as a currency in no way will be supported, in addition to the computing power used to create it. (Pedro Franko, 2014)

State bans. Different states relate differently to payment system of bitcoin, and at any time can enter all kinds of prohibitions on its use, for example, as a means of payment for goods and services. In particular, the risks of the bitcoin ban are very high in most countries. Loss

of monopolization of the role issue of money for the state will mean a loss of power over people, therefore they will try not to allow this, or somehow take the bitcoin system under its control. This can cause rapid and severe devaluation of cryptocurrency. (Roman Yankovskiy, 2017)

Turnover of illegal goods. The use of bitcoins in the black market allows to ensure non-control by national authorities in trade the goods such as weapons, drugs, etc. As an example, such trade is often considered by media in the history of the online trade of Silk Road. At the same time, during the hearings in the US Senate about virtual currencies, it was noted that cash for illegal transactions is used much more often, but this does not become a basis for criticism or prohibition of cash. (Kislyy V., 2017)

Security Concerns. Nevertheless, bitcoin is considered to be untraceable system, and therefore it is very hard to hack, this is still a possible thing to do. According to the security experts, nearly one third of wallets are tried being hacked or even defrauded. It is very easy to guess the reason it is so attractive to hack a bitcoin wallet - the exchange rate is very high. The case of trying the stealing bitcoin accounts were particularly often to happen in the begging of the system when it was not that well secured. (Roman Yankovskiy, 2017)

To define virtual money as strictly positive or negative system of payment would be one-track minded and it would not reflect the essence of such an economic phenomenon of modern times as the cryptocurrency. Cryptocurrency represents by itself an answer to a number of challenges and innovations of modern life. The rapid growth in settlements of cryptocurrency is happening due to the fact that it is possible not just reach the needed level of confidentiality and anonymity but also do not require communication with the center for confirmation of the payment. (Genkin A., Mikheyev A., 2018). Therefore, the cost of transaction is minimized. Such systems can be effectively used to provide micro payments that cost less than 1\$ while traditional credit card systems become economically unprofitable. It is micro payments that are able to provide the main sales turnover of the information on the Internet. (Pedro Franko, 2014)

The main problem of the money surrogate is that it is an instrument that is not provided with anything, and in case of problems in use (economic entities will refuse to accept the instrument in calculations), its cost is minimized, and the likelihood of compensation of at least some equivalent, too. It can be assumed that close problems are possible with the use of legal means of payments issued by the state. An ineffective state policy may lead to a

decrease in the purchasing power of the national monetary unit - up to the restoration of barter or the total refusal to use it and replacement by foreign exchange, which in the world economy is known as currency substitution. But the state is obliged to function to ensure the well-being and development of economic entities and citizens residing on its territory, which makes its bankruptcy an unlikely event (the state as much as possible seeks to prevent it) and is the main defense of its obligations, including money. (Pedro Franko, 2014)

The ambiguous interpretation is also the cryptocurrency position, such as the decentralized system of mining: on the one hand, it is the possibility of re-issuing settlement funds (although this parameter is very relevant for virtual instruments), but on the other hand, in conditions of independence from any state account regulator, or transfer any information to third parties, translations cannot be "rolled back". Yes, and political risks affect them significantly less than on financial obligations. (Genkin A., Mikheyev A., 2018). The duality of cryptocurrency in the modern economy has led to an ambiguous assessment of this economic phenomenon and has caused diverse ways for governments to react to its development. (Burn-Callander R., 2014)

3.3. Predictions for virtual currencies.

Cryptocurrency is, perhaps, the currency of the future. But the near or far future? This is another matter. Opinions about the prospects of the bitcoins were divided: some believe that the bitcoins will come to an end while others believe that everything is just beginning. Each side has its own convincing facts and counterarguments. The stumbling block of both sides is the legality of the cryptocurrency. Optimists believe that the rate of bitcoin in a couple of years (perhaps tens of years) can generally reach up to 100 thousand dollars per 1 BTC, but it is only in the future. Personally, I think that this is quite realistic, if the governments of the countries can agree among themselves and make it legal. Comparison bitcoins with real gold (they are often called "virtual gold"). And what is gold? Than it is provided? It's just metal. Bitcoins are also not provided with anything. However, the potential opportunity to make it an international currency makes for it unlimited growth prospects. Pessimists are sure that governments will never legalize the currency with such prospects. The second weighty argument against bitcoins is the issue of the security of virtual money. But if Bitcoin has nothing to do with the currency that does not depend on anything, then what should be the price for 1 coin? When forming the ruble against the dollar, everything is clear, and the number of factors influencing the exchange rate includes: the rate of inflation (the higher the

inflation rate in a country, the lower its currency rate, unless other factors counteract it); The balance of payments situation (with the passive balance, the demand for foreign currency for the repayment of international obligations is increasing and the exchange rate of the national currency is decreasing); Difference in interest rates in different countries; Foreign exchange market activities and speculative currency transactions; The degree of use of a certain currency in the euro-currency market and in international settlements; Acceleration or delay of international payments; The degree of confidence in the currency; Currency policy, which is aimed at either raising or lowering the exchange rate, proceeding from the tasks of monetary and economic policy. Cryptocurrency will work well in a united world, but the world is not yet ready for them: in 300 years - it will be absolutely amazing thing, but in our situation, when the world is divided into states and blocks of states that sometimes are at war with each other, the cryptocurrency will work all the same worse. As soon as they interfere with any state, they will be banned, they will be fought (Kaspersky, 2015).

It is necessary to analyze Bitcoin from the point of view of the Quantitative Theory of Money, which is today the basic in economic science. According to this theory, the value of money depends only on three parameters.

The value of money = $Y / (V * M)$ M is the amount of money in circulation. V- is the speed of money turnover. Y - is the amount by which you could make transactions for the same period of time. The traditional approach is to consider only transactions that go to the Gross Domestic Product (GDP). And there are deals only with goods intended for direct use. We do not take into account transactions with other currencies, raw materials and semi-manufactures, antiquaries (what changes the owner only, but is not made), etc. The value of money is the reciprocal of the average price level. That is, if prices for goods grow, then money becomes cheaper. What does all this mean for Bitcoin? Depending on how these three parameters change, the value of the currency can grow, fall, and even go to zero. The amount of Bitcoin is constantly growing, albeit slowly. This will lead to impairment, unless, of course, the number of transactions with that currency increases. Speed of circulation - in the traditional economy this value is stable, it depends on what proportion of money is in purses for saving, how often wages are paid to workers in the country (once a month or once a week), the speed of conducting transactions in banks, etc. With electronic money, there is no such stability. Changes in the rules of conducting transactions can affect the speed of circulation. (Pedro Franko, 2014)

Money can be provided only by sellers who are ready to sell them for actual goods. And it is necessary to discuss exactly the possible advantages for sellers in the turnover of Bitcoin. And here convenience and reliability are important. So far, because of the course jumps from 1 to 30 dollars and back, there is no special reliability. A limited number of coins and the inability to print them when they want - this is just Bitcoin's problem. Demand fluctuates, and supply cannot adapt. Here, the instability of the course is inherent in principle. The dollar is popular precisely because of the large base of transactions with it. Of course, it is not possible to print dollars in any quantities, but the US GDP is about 14 trillion USD plus deals outside the US. The base is so large that no real emission will ensure such price fluctuations as in Bitcoin. Bitcoin is nothing tangible - nothing that would have real value in the ordinary world: it is not oil, not a valuable metal, not wheat. (Kislyy, 2017).

Firstly, the maximum number of bitcoin in circulation is 21 million of bitcoins. Although it will be achieved by 2140 ("extraction" is being carried out at a gradually decreasing pace, and today slightly more than half of this volume is produced), but it will be assumed that the users already have 21 million BTC-units in their hands.

Secondly, the total volume of markets on which Bitcoin can find use. Any operation involving the transfer of funds from one pocket to another can be carried out with the help of bitcoins. Suppose for now that the new currency is interested only in Internet business. Annually, Internet sales amounting to more than one trillion dollars are made (the trade association of electronic commerce, i.e. IMRG gives a forecast of 1.25 trillion for the current year). Suppose that all monetary activity here instead of national currencies is conducted in bitcoins. For that there are a lot of good reasons: bitcoin is universal for all countries, anonymous, working is cheap (there is no commission for working with plastic cards). How much will cost 1 BTC in this case? Having divided the second into the first, we get 59 thousand dollars for one bitcoin. At the moment about 11 million PTS is produced, and in fact only a small part is in circulation, and if Bitcoin is interested in offline retail trade, the potential market volume immediately grows two or three times, it turns out that in one BTC will be given up to Million dollars.

The deflationary nature of bitcoins (the potential for a constant rise in price due to the inability to "print" over 21 million BTC) and steep jumps in the rate make it unfit for business. Yes, it is inconvenient that the price is swinging from side to side, but in general, such "swings" - a rarity: most of the time the Bitcoin rate is stable. If the truth is to look at

Bitcoin as an investment, then one needs to calmly concern with the hectic that is going on now in the press and on forums. Let the course jumps and falls by tens of percent. Let the journalists wash away the bones of random bitcoin millionaires, let them guess, whether the crowds or large speculators stand behind the next price hurdle. The more noise, the better: like any asset in the free market, as the number of participants increases, volatility falls (less price fluctuation) and liquidity rises (it's easier to sell a certain amount of money). It is possible to survive when the public loses interest in Bitcoin. Thus, the attitude to cryptocurrency is a matter of subjectivity to everyone. (Niedermayer, 2016).

It is not possible to say unambiguously about the prospects of cryptocurrency. At the moment, Bitcoin is the most popular electronic currency. A huge number of people use it in trade, they try to make money, both at fluctuations in prices, and at its extraction. Today, those times have come, which will determine the future of the cryptocurrency. Everybody knows the prohibitions on the use of Bitcoin in some countries at the legislative level. At the same time, the US is discussing further prospects for the development of the cryptocurrency, leaving positive feedback when using Bitcoin. The EU authorities plan to deal with the circulation of the cryptocurrency and try to regulate it. The main initiator in the future of cryptocurrency is the German Central Bank, which not only advises on the use of cryptocurrency, but also discusses further development prospects with other central banks in Europe. (Yankovskiy, 2017).

To perform more accurate forecast of cryptocurrency development, in this work several types of analysis will be conducted: Time series analysis introduced in open-sourced software Gretl; Technical analysis and Correlation Matrix which are described in detail in the following chapters.

3.4. Time series forecasting analysis.

Under the time series (a dynamic series, or a series of dynamics) in the economy is implied a sequence of observations of a certain trait (random variable) x in consecutive moments of time. Individual observations are called series levels, which we denote by x_t ($t = 1, 2, \dots, n$), where n is the number of levels. Time series is a set of chronologically ordered values of the statistical indicator characterizing the change in socio-economic manifestations in time. The process of economic development is depicted as a set of interruptions of a continuous, allowing to analyze in detail the features of development by means of characteristics that reflect the change in the parameters of the economic system in time. The time factor here is

of decisive importance. The process of changing socio-economic trends over time is that there is a change in the impact on this development of many factors of social, economic, technological and any other process, and the time factor accumulates their influence. Considering as example economic factors it is assumed that they change under the influence of internal causes of economic development in general, but from the outside this development looks like development in time. Each time series includes two mandatory elements: time (t) and a specific value of the indicator, or the level of the series (y_i). The analysis of time series makes it possible to follow the development of the phenomenon, to show its main ways, trends and rates. The choice of appropriate methods and methods of analysis depends on the objectives of the study and is determined by the nature of the original data. Main stages of the analysis of time series are: graphical representation and description of the behavior of the time series; the allocation and removal of regular (non-random) components of the time series (trend, seasonal and cyclical components); smoothing and filtering (removal of low- or high-frequency components of time series); the study of the random component of the time series, the construction and verification of the adequacy of the mathematical model for its description; forecasting the development of the process under study on the basis of the available time series; the study of the relationship between different time series. For making an efficient analysis of time series it is applicable to perform reduction of time series to a comparable type and the detection of abnormal observations, it is possible to reveal the patterns of the dynamics of the phenomena being studied, since this is the main goal in the statistical analysis of socio-economic phenomena. The patterns are determined in the beginning with the help of analytical indicators, that is, the analysis of the absolute speed and intensity of development of socio-economic phenomena. (Afanasyev V., Yuzbashev M., 2001).

3.5. Technical analysis.

Technical analysis of the market determines the direction of the price movement and the nature of this movement, uses the history of already completed transactions, reflected in the price chart. There is a number of main advantages of technical analysis, among which its simplicity and visibility - information is reflected in the graphs and is easily digested; and also applicability for shorter time intervals which is a very important statement in case of quickly changing situation of cryptocurrency. (Kuepper J., 2017)

The three main postulates on which technical analysis is based: The price considers everything. Any factor that affects the price - economic, political or psychological - is already considered by the market and included in the price. Therefore, technical analysis is a universal method of market analysis; The movement of prices is subject to trends. And this means that trends can be identified and described, and therefore used in trade for profit; History repeats itself. The rules in force in the past will work in the present and in the future. This statement gives grounds to carry out not only technical, but also statistical analysis, as each trader makes his own conclusions, exploring the old information. Relying on those postulates, few different methods of technical analysis can be stated. (Kuepper J., 2017)

Classical analysis: The essence of the method is in the chart on the price chart of lines that form trends and show the direction of the price change, as well as price levels showing the areas of maximum involvement of bidders and figures that characterize possible options for continuing, uncertainty or reversal of an already existing trend. Indicator analysis: This method of technical analysis includes mathematical functions, which are divided into trend indicators and countertrend (oscillators). The trend indicators include different models showing the direction of the main trend, smoothed by the chaos of price fluctuations (since there are both growth and decrease moments within one trend, it is therefore not always clear when it was formed and where it moves). The main value of these methods is in confirming the presence or absence of a pronounced tendency, as well as identifying its formation or termination of action. There are two main types of trend indicators: Moving Average and ADX. Mathematically, they are calculated a little differently, but they both serve a common goal - identifying the main trend and committing transactions in its direction. The group of oscillators include mathematical methods for designation of both unreasonably high (overbought) or, otherwise, low (resale) prices in relation to previous variety of motion. In any trend, there are periods of both growth and decline. And this means that there is an opportunity for both buying an asset at a low price in an increasing trend with further selling at a fairly high price, and selling at a high price, as well as buying at the lowest price (with a short sale within a downtrend) oscillators. The two main oscillators are the Relative Strength Index and the Stochastic Oscillator. They show the position of prices within the established successively changing ranges of price fluctuations - both downward and upward. Trend indicators and oscillators are often used in combination with each other. Trend indicators are used as a filter (in a growing market, sales are excluded, and on a falling one, purchases are excluded). (Lowry, S., 1998).

Oscillators, in turn, are used to more accurately select the most attractive price. Analysis of trading volumes: more attention has been paid recently. The volumes are analyzed both in the classical technical analysis and in the constantly emerging new methods: cluster analysis and analysis of horizontal volumes. For example, figures in classical TA, in addition to the technique of drawing on the price chart, are confirmed by a certain dynamic of change in volumes. And some indicators - for example, the book volume (OBV) - for the base of calculation take just changes in trading volumes. (Lee J. J., Murphy J. J., 1986)

Candlestick Analysis was developed by the Japanese trader Munehisa Homma. (Nial Fuller, 2017). The essence of the method is in forecasting prices based on special combinations of Japanese candles relative to each other. It's no secret that the very notion of an upward tendency assumes that the next candles are higher than the previous ones. And the analysis of candles and their combinations allows to look into the "anatomy" of the trend and better understand how it is arranged. In candle analysis, also separate candles, bearing a certain semantic load, depending on the location in the trend. To such candles, it is possible to carry, for example, a candle Harami on an extremum, which speaks about a possible change of tendency. The logic of the trend, in turn, reports the balance of forces of sellers and buyers with equal opening and closing prices. (Gregory L. Morris, 2006)

In this paper work all of the mentioned methods will be used to fully determine the economic position of the cryptocurrency on the modern world market.

3.6. Correlation Matrix.

Correlation matrix is a square matrix consisting of the correlation coefficients between all possible pairs of variables used in the analysis. The number of rows and columns of correlation matrix corresponds to the number of analyzed variables. At the intersection of the row and column, the correlation coefficient between the corresponding variables is indicated. Correlation matrix is symmetric with respect to the main diagonal, therefore in practical problems only the "upper" or only "lower" triangle of correlation matrix are considered. All the values on the main diagonal are equal to 1. The correlation coefficient takes values from -1 to 1. The coefficient modulus indicates the degree of dependence: the closer its value to 0, the weaker the linear dependence is. The closer the correlation coefficient is from 0 to 1, the stronger the linear dependence is, the closer from 0 to -1 - the stronger the inverse linear dependency. In practice, it is considered that if the modulus of the

correlation coefficient is greater than 0.6, then the linear dependence is strong, and if less than 0.3, it is almost absent. (Tereshchenko, 2002)

Correlation analysis is used to assess the degree of linear relationship between pairs of factors, is performed with the purpose of selecting and preprocessing input fields for use in trainees on these models. For example, the presence of a correlation between input factors is extremely negative in the construction of linear regression.

4. Practical part

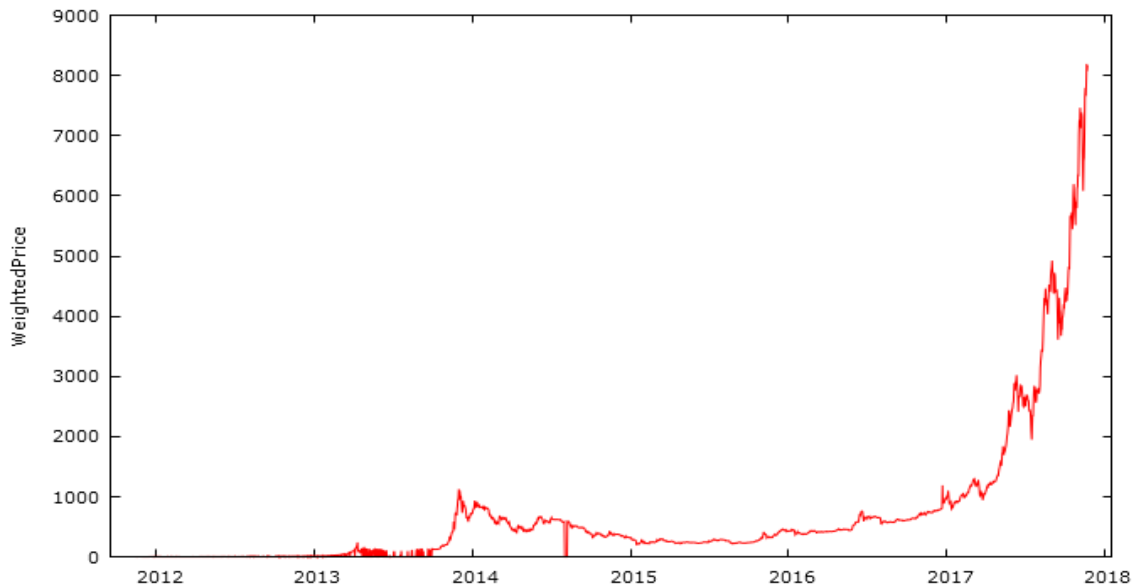
In order to understand clearly the position of cryptocurrency on the world market, several technics will be implemented to give information about most popular, and therefore expensive cryptocurrency, and its amount in circulation. The currency analyzed is Bitcoin since higher amount of data can be found about it than any other cryptocurrency.

4.1. Time series analysis.

As people get used to a new, rapidly gaining market, it is important to try and understand what is happening to it. There are many risks, both at the micro level (for example, personal investment) and at the macro level (for example, preventing market crashes or large capital losses) (Brockwell P.J., Davis R.A, 2010).

For this analysis, Bitcoin will be taken as an example as the first and most known cryptocurrency. It cannot be said that the currency has always been behaving smoothly. To take a closer look at the daily volatility of the course and implement analysis of time series in Gretl daily data from November 12, 2011 to November 22, 2017 will be analyzed.

Figure 1: Timeseries for Bitcoin (2011-2017)



Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

It is clearly seen on the time series plot above that the data has trend line and seasonality which is seen on the graph represented by spikes going up and down throughout all the time period. Both trend line and seasonality need to be removed to get a normalized result.

Next step is to perform regression of Weighted Price against Time. For that time trend and periodic dummies are added to the dataset. Each dummy represents one day of a week, since our data is a weekly data, e.g. dummy_2 is the second day of the week in the sample and it is going to turn on each time when second day comes at hand; otherwise it will be equal to 0.

The linear regression model:

Model 1: OLS, using observations 2011-11-12:2017-11-22 (T = 2203)

In order to get rid of seasonality, dummy_1 will be excluded from an observation.

Dependent variable: WeightedPrice

Table 1: Model 1: OLS

	Coefficient	Std. Error	t-ratio	p-value	Column1
const	-586.243	62.8089	-9.334	<0.0001	***
time	1.14301	0.0312375	36.59	<0.0001	***
dummy_2	0.744188	74.2962	0.01002	0.992	

dummy_3	2.9232	74.2962	0.03935	0.9686	
dummy_4	-10.1733	74.3553	-0.1368	0.8912	
dummy_5	-5.24789	74.3553	-0.07058	0.9437	
dummy_6	-7.30716	74.2962	-0.09835	0.9217	
dummy_7	-6.94236	74.2962	-0.09344	0.9256	

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

The indicators of performed OLS model are the following:

Table 2: Indicators of Model 1

Column1	Column2	Column4	Column5
Mean dependent var	669.6466	S.D. dependent var	1181.22
Sum squared resid	1.91E+09	S.E. of regression	932.41
R-squared	0.378888	Adjusted R-squared	0.376908
F(7, 2195)	191.2838	P-value(F)	1.10E-221
Log-likelihood	-18185.53	Akaike criterion	36387.06
Schwarz criterion	36432.64	Hannan-Quinn	36403.71
rho	0.997771	Durbin-Watson	0.004523

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

Adjusted R-squared equals only 0.37 which is unusual for the timeseries data, typically this number is closer to 1. That means that overall quality of analysis of the data will be 37% accurate. However, it was decided to proceed with the analysis to get determinate result.

In sample forecast after removing last week information:

Model 2: OLS, using observations 2011-11-12:2017-11-15 (T = 2196)

Dependent variable: WeightedPrice

Table 3: Model 2: OLS

	Coefficient	Std. Error	t-ratio	p-value	Column1
const	-548.661	58.6499	-9.355	<0.0001	***
time	1.09065	0.0292621	37.27	<0.0001	***
dummy_2	1.17494	69.3765	0.01694	0.9865	

dummy_3	3.12032	69.3766	0.04498	0.9641	
dummy_4	-8.61504	69.4319	-0.1241	0.9013	
dummy_5	-4.04245	69.4319	-0.05822	0.9536	
dummy_6	-5.74775	69.3766	-0.08285	0.934	
dummy_7	-6.04153	69.3765	-0.08708	0.9306	

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

Table 4: Indicators of Model 2

Column1	Column2	Column4	Column5
Mean dependent var	646.5426	S.D. dependent var	1109.738
Sum squared resid	1.65E+09	S.E. of regression	869.2854
R-squared	0.388359	Adjusted R-squared	0.386402
F(7, 2188)	198.4661	P-value(F)	3.00E-228
Log-likelihood	-17973.79	Akaike criterion	35963.58
Schwarz criterion	36009.13	Hannan-Quinn	35980.22
rho	0.997611	Durbin-Watson	0.004808

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

Number of observations decreased due to the fact that last week was excluded from the sample. Adjusted R-squared increased slightly to 38%.

Analysis of the quality of in-sample forecast:

The analysis of forecast for excluded variables is run in order to assess the quality of this particular forecast.

For 95% confidence intervals, $t(2188, 0.025) = 1.961$

Table 5: Analysis of the quality of in-sample forecast

Obs	WeightedPrice	prediction	std. error	95% interval
11/16/2017	7659.75	1838.88	871.267	(130.286, 3547.48)
11/17/2017	7792.63	1844.55	871.267	(135.949, 3553.14)

11/18/2017	7658.22	1843.93	871.266	(135.336, 3552.53)
11/19/2017	7882.97	1844.73	871.266	(136.133, 3553.32)
11/20/2017	8190.35	1851.86	871.266	(143.265, 3560.46)
11/21/2017	8073.43	1854.13	871.266	(145.530, 3562.72)
11/22/2017	8166.55	1857.16	871.266	(148.566, 3565.76)

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

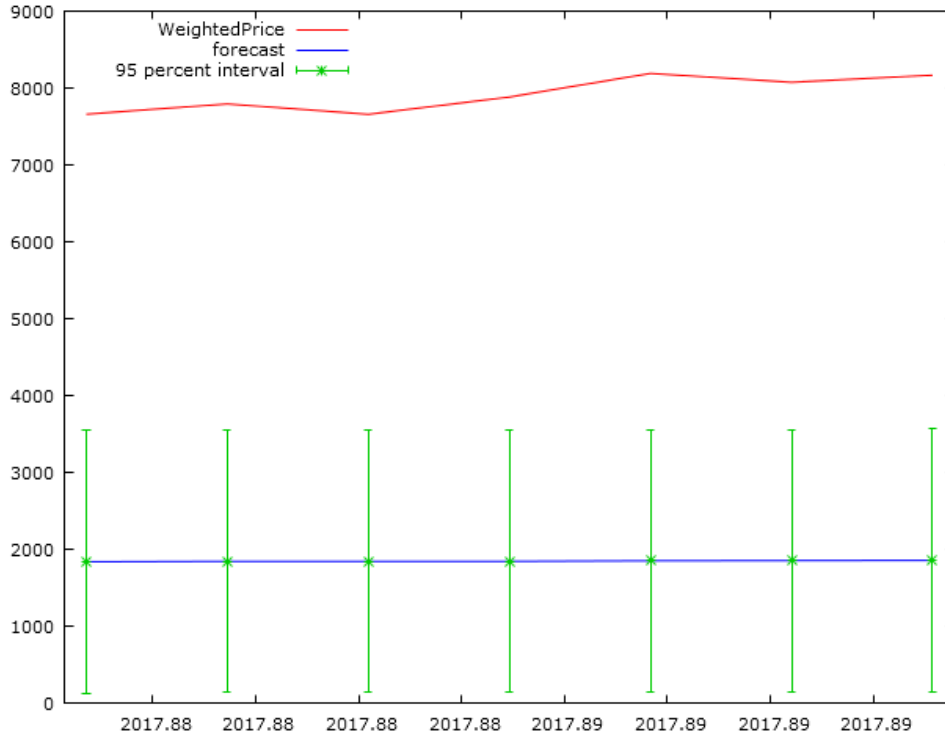
Table 6: Forecast evaluation statistics

Column1	Column2
Mean Error	6069.8
Root Mean Squared Error	6073.3
Mean Absolute Error	6069.8
Mean Percentage Error	76.647
Mean Absolute Percentage Error	76.647
Theil's U	33.014
Bias proportion, UM	0.99886
Regression proportion, UR	0.00095398
Disturbance proportion, UD	0.00018862

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

The comparison of statistical factors from the output data provides the information about the quality of the prediction. For that purpose, the errors are compared. The prediction will be deducted from means for each of the 7 observations, which will result as Mean Error. The common metrics also includes root mean square error and mean percentage error which carries the information about how far above or below the reality the forecast is. (Brockwell P.J., Davis R.A, 2010).

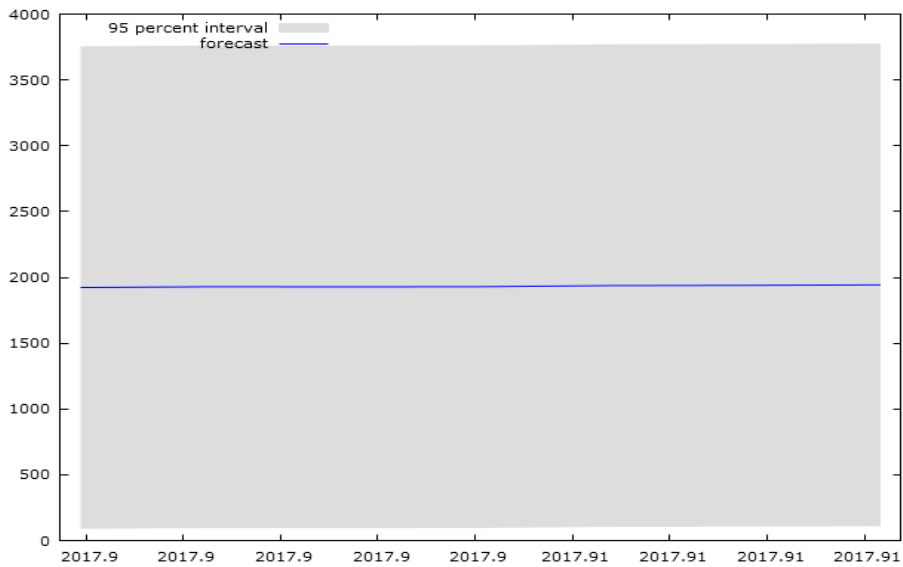
Figure 2: Graph of forecast for the last week of sample



Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

It is clearly seen on the graph that the forecast was very far from reality. Considering Mean Absolute Percentage Error from the analysis above, the forecast is 77% away from the actual observations. Still, prediction for the next week values for Bitcoin is done as follows:

Figure 3: Graph of forecast for the next week of sample



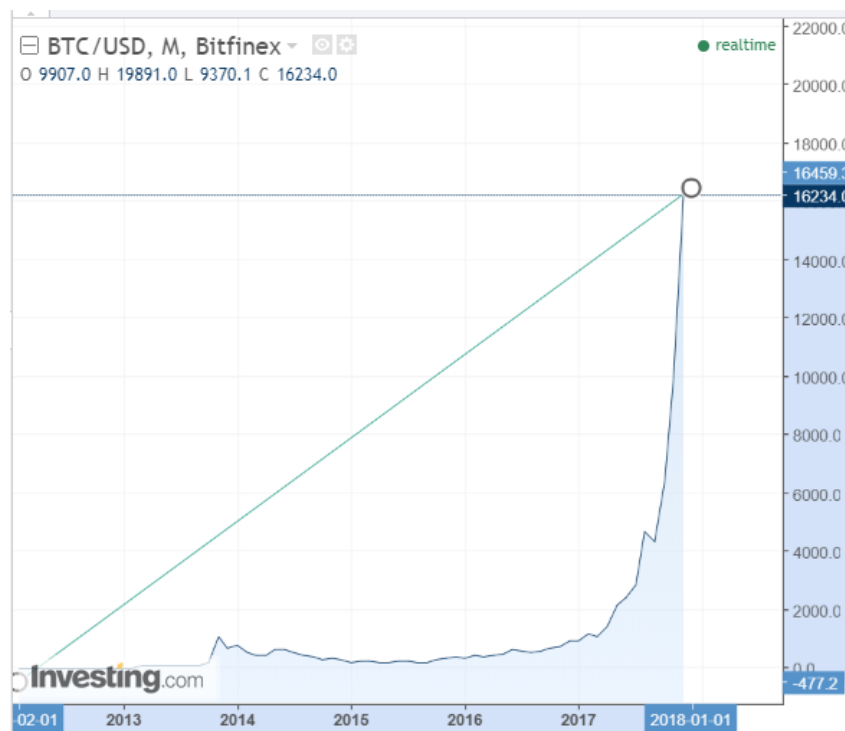
Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

The output of forecasting does not seem to be close to reality considering the history of Bitcoin development and its non-stable character. For that reason, other type of analysis will be implemented in the next chapter.

4.2. Technical Analysis.

Next graphics were prepared within Investing.com

Figure 4: Price of Bitcoin



Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

In technical analysis, it is important to trace the history of the studied object since the history repeats itself throughout time. Considering lifetime of bitcoin from 2013 until December 2017, it is clearly seen on the price chart that trend line is strongly positive. Also, there are not so many figures of shifting of the trend. Last year observed, the price minimum had not fallen lower than value of the beginning of year 2017.

Figure 5: Candlestick chart



Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

The data from December 22, 2017.

As it is seen from the candlestick chart above, the price of BTC has been mostly arising from the opening to the closing period of the market in the year 2017, which means there is an uptrend. There is a need to take closer look to technical indicators to understand whether BTC is really going to grow more in price.

Technical indicators.

Since technical analysis is most commonly used for trading, the quality of position on market is described with trading terms such as “Sell/Buy/Overbought/High Volatility”. (Lee J. J., Murphy J. J., 1986).

The relative strength index (RSI) is an impulsion oscillator developed by technical analyst J. Welles Wilder Jr., that compares the magnitude of recent gains and losses over a specified period of time to measure velocity and alteration of price movements of a security. It is mostly taken in consideration when attempting to identify overbought or oversold conditions in the trading of an asset. (J. Welles Wilder Jr, 1978)

Another helpful indicator developed by Welles Wilder and applied in technical analysis is Average True Range (ATR). In a few words the explanation is: a stock experiencing an elevated level of volatility has a higher ATR, and a low volatility stock has a lower ATR. (J. Welles Wilder Jr, 1978)

Bull/Bear Power is a market-sentiment indicator announced on a weekly basis by Investor's Intelligence that uses information taken straightly from market professionals. This index reflects the sentiments of market participants that perform deals daily within the financial markets which gives a more relevant measure. (Kuepper, 2017).

These and some other indicators were analyzed in this part of Bachelor thesis and are performed in the table below.

Table 7: technical analysis indices

Name	Value	Action
RSI (14)	96.297	Overbought
STOCH (9,6)	32.31	Sell
STOCHRSI (14)	100	Overbought
MACD (12,26)	2180.6	Buy
ADX (14)	83.769	Overbought
Williams %R	-33.201	Buy
CCI (14)	317.4214	Overbought
ATR (14)	2007.8932	High Volatility
Highs/Lows (14)	9016.8447	Buy
Ultimate Oscillator	63.375	Buy
ROC	1820.067	Buy
Bull/Bear Power (13)	18736.5596	Buy
Buy: 6	Sell: 1	Neutral: 0
Summary:		STRONG BUY

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

To simplify the decision-making process, some of the indicators are excluded from observation, which allows to conclude that total number of indexes marked with “Buy” is higher than “Sell” like 6:1 which means that it is a suitable moment to buy Bitcoin.

Moving Averages is a technical indicator that allows a trader to determine average price of the observed object during a certain period of time. The technic is used in this paper to remove white noise from the chart in order to smooth it. There are two types of Moving Average: Simple and Exponential Moving Average.

The most well-known kind of Moving Average is Simple Moving Average, in which sum of all the previous closing prices is taken during a period of time and then divided by the number of considered prices to get a result. (Lowry, 1998).

Exponential Moving Average are issued more closely since it does consider spikes and therefore gives more accurate analysis than the simple one. The periods observed are 5-days, 10-days, 20-days, 50-days, 100-days, 200-days – stated in the table as MA5, MA10, MA20, MA50, MA100, MA200 accordingly.

Table 8: Moving Averages for various periods

Period	Simple	Exponential
MA5	7793.9	8634.1
	Buy	Buy
MA10	4895.5	6143.4
	Buy	Buy
MA20	2826.8	3982
	Buy	Buy
MA50	1387.7	2052.6
	Buy	Buy
MA100	705.4	1170.7
	Buy	Buy
MA200	352.7	638.9
	Buy	Buy
Buy: 12		Sell: 0
Summary:		BUY

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

Analysis of Moving Averages shows that it is recommended to buy Bitcoin considering mentioned time periods. EMA is more reactive than SMA and therefore allows a trader to trace slight changes on the market. Since the chosen time period is too wide, EMA does not significantly differ from SMA as it is seen from the table and so result remains the same – Bitcoin is in a right position for being bought.

Pivot points. The pivot point is the point in which the market sentiment changes from bearish to bullish.

Points above the Main (also called Daily) pivot are Resistance Pivots, marked in the table as R1, R2, R3. Those which are situated below are called Support Pivots, marked as S1, S2, S3. (J. Lee, J. Murphy, 1986)

Table 9:Pivot Points

Name	S3	S2	S1	Pivot Points	R1	R2	R3
Classic	411.9	2918.9	6413	8920.1	12414.2	14921.3	18415.4
Fibonacci	2918.9	5211.4	6627.7	8920.1	11212.5	12628.8	14921.3
Camarilla	8256.7	8806.8	9356.9	8920.1	10457.1	11007.2	11557.3
Woodie's	905.3	3165.6	6906.4	9166.8	12907.6	15168	18908.8
DeMark's	-	-	7666.5	9546.8	13667.7	-	-

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

From the analyzed data the conclusion is as follows: Bitcoin is likely to be profitable as the higher number of pivots is situated in Resistance area.

Table 10:Summary of Technical Analysis

Moving Averages:	Buy (12)	Sell (0)
Technical Indicators:	Buy (6)	Sell (1)
Summary:		STRONG BUY

Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

After analyzing Moving Averages and other Technical indicators, the decision to be made is that BTC is likely to gain in price so the trader must buy it to get profit.

But let us take a closer look on the behavior of price for the year 2017 to assure that it is going to grow in the future.

Figure 6: Price of BTC in 2017



Data from: <https://www.investing.com/currencies/btc-usd-historical-data>

As it is seen, the price hits its maximum historical point (\$19 000) and then swiftly falls \$5 000 lower, then begins to rise again. And if the whole year will be considered, it is clear that BTC is not rising stable but changes its trend over time.

From performed technical analysis, one thing can be known: BTC is not a stable safe currency yet, it pointedly reacts to slight changes, but it is most likely to be gaining in price until it hits the maximum point, as it was in 2013 (\$1 100) and in December 2017 (\$19 000), and then falls very low. The question is what will be the maximum point next time and for how long the currency is likely to survive after those brash falls?

4.3. Correlation matrix

Correlation matrix is a statistical methodology which allows to determine whether different variants affect one another and how strong the dependency between them is, if exists. Correlation could be positive or negative, also it there can be no correlation between the variables. Positive correlation means that a change in first variance reflects as an equally directed change in second variance. Negative correlation takes place when a change of first variance causes opposite change in a second variance. No correlation means that observed variances have no influence on each other. For measuring how strong a correlation is,

number 1 is taken as a comparison point. Positive correlation is strong when a coefficient is closer to 1 (greater than 0,5), weak when closer to 0 (lower than 0.5); same applies for negative correlation. (David A Kenny, 1979)

Table 11: Correlation matrix

Correlation	BTC/USD	EUR/CZK	EUR/USD	ETH/USD	RUB/USD	USD/GBP
BTC/USD	1					
EUR/CZK	0,41633588	1				
EUR/USD	0,33302356	-0,1600425	1			
ETH/USD	0,74241713	0,0339462	0,56183936	1		
RUB/USD	0,65706663	0,04572502	0,73070239	0,57752571	1	
USD/GBP	-0,5040966	0,17582246	-0,84413229	-0,7357033	-0,82793221	1

1. Data from investing.com is actual for 25.02.2018, available at:
<https://www.investing.com/currencies/btc-usd-historical-data>;
<https://www.investing.com/currencies/eth-usd-historical-data>;
<https://www.investing.com/currencies/eur-usd-historical-data>;
<https://www.investing.com/currencies/usd-gbp-historical-data>;
<https://www.investing.com/currencies/rub-usd-historical-data>

BTC/USD is positively correlated with all the variables except for USD/GBP, which means that a change in exchange rate of EUR/CZK, EUR/USD, ETH/USD, and Bitcoin will influence the exchange rate of RUB/USD – in case of positive correlation: all the currencies will change in one direction – e.g. when EUR/CZK increases BTC/USD increases as well. The strongest positive correlation is recorded between BTC/USD and ETH/USD which is not surprising since both variances are cryptocurrencies and do depend one on the other. More interesting is that RUB/USD is depending on BTC/USD and possible reason is the huge size of Russian crypto market and additionally the increasing agitation which is taking place in social media and the effect of which is raising of demand on cryptocurrency in Russia, according to “Gazeta Vedomost”, October 30, 2017. But most likely it is a simple coincidence as the correlation is not strong – only 0,6.

However, not all of variances are positively correlated. USD/GBP is in negative correlation with both exchange rates for Bitcoin and Ethereum. It means that while British Pound gains in price, mentioned cryptocurrencies are contrariwise falling.

5.Results and discussion.

Several types of analyses performed and described in this thesis do not give a certain economically useful information about cryptocurrency as the main influencing factors are psychological and not economical.

The forecasting based on time series analysis, considering daily data from November 2011 till November 2017, did not give an expected result as the quality of forecast measured by Adjusted R-square was only 37% which is incredibly low and could be explained by non-stable character of Bitcoin.

Technical analysis was conducted next to obtain a deeper knowledge of the market from the trader point of view. Bitcoin was chosen for this analysis as it is the oldest cryptocurrency and the most well-known as well which ease the process of finding data. Technical indicators considered such as Moving Averages, Pivot Points, Candlestick chart and others allowed to analyze the behavior of Bitcoin throughout time of its existence considering actual data from Investing.com. Analysis of Moving Averages presented in November 2017 showed that it was recommended to buy Bitcoin as it was likely to keep gaining in price until reaching the maximum point, which was reached in December 2017 (\$19,000). From performed technical analysis, one thing can be known: BTC is not a stable safe currency yet, it pointedly reacts to slight changes in social opinion and other psychological factors.

The final analysis was correlation matrix. The conclusions are made when analyzing the final table which includes values (correlation coefficient) from -1 to 1 and when it is greater than 0.6, linear dependence is considered to be strong, if less than 0.3, it is almost absent. The described analysis was performed in Microsoft Excel tool considering current data from Investing.com to investigate whether there is a correlation between virtual currencies such as Bitcoin and Ethereum with other physical currencies such as U.S. Dollar, Czech Crown, Russian Ruble and others. The matrix showed weak correlation between both mentioned cryptocurrencies and Russian Ruble which was unexpected but could be a simple coincidence. Another reason could be that Ruble is a weak currency itself and depend on every factor slightly influencing its exchange rate. Otherwise no real dependency was found.

6. Conclusion

Bitcoin is designed to be a breakthrough in securing funds and can also be used as a significant protection against many forms of financial crime. For example, it is impossible

to forge bitcoin. Users fully control their payments and cannot accept those from unconfirmed accounts - such protection is a security measure against fraudulent. Bitcoin transactions are irreversible and free from fraudulent refunds. Bitcoin allows money to be safe from theft and loss, using very strong and useful mechanisms, such as backup, encryption, and multiple signatures.

Considering all the above it should be mentioned, however, that cryptocurrency is not yet ready to be treated as a fair and equal replacement to existing fiat currencies even though it is a highly technological improvement of financial system which reverberates requirements of modern society. Its exchange rate strongly depends on the slightest changes in the opinion of society which leads to very explosive falls and risings in price.

Another problem described in this thesis is that Bitcoin is a finite currency, the number of its units is limited by 21 million of Bitcoin, fact of what potentially causes difficulties for users as well as the disability of the modern society to implement needed laws for regulating cryptocurrency usage.

7. References

Books:

1. Davis, G. (1994). *A history of money: from ancient times to the present day*. 1st ed. Cardiff: University of Wales Press
2. Kenny, D. A. (1979). *Correlation and causality*. 1st ed. New York: John Wiley & Sons
3. Lowry, S. (1998). *The magic of moving averages*. 1st ed. Traders Pr; Imprint Wasendorf & Associates Inc.
4. Lee J. J., Murphy J. J. (1986). *Study Guide to Technical Analysis of the Financial Markets: A Comprehensive Guide to Trading Methods and Applications*. 1st ed. New York Institute of Finance.
5. Franko, P. (2014). *Understanding Bitcoin: Cryptography, Engineering and Economics*. 1st ed. John Wiley & Sons
6. Genkin A., Mikheyev A. (2018). *Blokcheyn. Kak eto rabotayet i chto zhdet nas zavtra*. Moscow: Alpina Publisher.
7. Rothbard M. N., (1963). *What Has Government Done to Our Money?* 1st ed. Ludwig Von Mises Institute
8. Ostalskiy A. (2008). *Kratkaya istoriya deneg*. 1st ed. Moscow: Amfora
9. Afanasyev V., Yuzbashev M., (2001). *Analyz vremennyh ryadov I prognozirovaniye*. 1st ed. Moscow: Finansy I Statistika.
10. Morris G. L., (2006) *Candlestick Charting Explained: Timeless Techniques for Trading Stocks and Futures*. 3rd ed. McGraw-Hill Education
11. Tereshchenko V. (2002). *Applied Statistics for Social Sciences*. 1st ed. Minsk: BGU.

12. Brockwell P.J., Davis R.A. (2010). *Introduction to time series and forecasting*. 2nd ed. Springer
13. Wilder J. W., (1978). *New Concepts in Technical Trading Systems*. 1st ed. Greensboro, N.C

Online resources:

2. Nakamoto S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [online] Bitcoin.org. Available at: <https://bitcoin.org/bitcoin.pdf>
3. Investing.com. (2018). *Historical data for EUR/CZK - Euro Czech Koruna*. [online] Available at: <https://www.investing.com/currencies/eur-czk-historical-data>
4. Kuepper J. (2017). *Basics Of Technical Analysis*. [online] Investopedia.com. Available at: <https://www.investopedia.com/university/technical/>
5. Grandars.ru (2017). *Metallicheskaya Teoriya Deneg*. [online] Available at: <http://www.grandars.ru/student/finansy/metallisticheskaya-teoriya-deneg.html>
6. Burn-Callander R. (2014). *The history of money: from barter to bitcoin*. [online] Telegraph.co.uk Available at: <https://www.telegraph.co.uk/finance/businessclub/money/11174013/The-history-of-money-from-barter-to-bitcoin.html>
7. Yankovskiy R. (2017). *Gosudarstvo i kriptovalyuty: problemy regulirovaniya*. [online] Moskovskiy gosudarstvennyy universitet. Available at: <http://msu.edu.ru/papers/yankovskiy/blockchain.pdf>
8. Kislyy V. (2017). *Yuridicheskiye aspekty primeneniya blokcheyna i ispol'zovaniya kriptoaktivov*. [online] Zakon.ru, Available at: https://zakon.ru/blog/2017/6/5/yuridicheskie_aspekty_primeneniya_blokcheyna_i_ispolzovaniya_kriptoaktivov
9. Investing.com. (2018). *Historical data for BTC/USD – Bitcoin US Dollar*. [online] Available at: <https://www.investing.com/currencies/btc-usd-historical-data>
10. Investing.com. (2018). *Historical data for ETH/USD – Ethereum US Dollar*. [online] Available at: <https://www.investing.com/currencies/eth-usd-historical-data>
11. Investing.com. (2018). *Historical data for EUR/USD – Euro US Dollar*. [online] Available at: <https://www.investing.com/currencies/eur-usd-historical-data>
12. Investing.com. (2018). *Historical data for USD/GBP – US Dollar British Pound*. [online] Available at: <https://www.investing.com/currencies/usd-gbp-historical-data>
13. Investing.com. (2018). *Historical data for RUB/USD – Russian Ruble US Dollar*. [online] Available at: <https://www.investing.com/currencies/rub-usd-historical-data>
14. Niedermayer H. (2016). *Electronic Cash, BitCoin*. Lehrstuhl Netzarchitekturen und Netzdienste Institut für Informatik TU München. [online] Available at: <https://www.net.in.tum.de/fileadmin/TUM/teaching/Peer-to-Peer-und-Sicherheit/ss11/ECash-BitCoin.pdf>
15. Fuller N. (2017) *The Most Successful Price Action Trader in History: Munehisa Homma*. [online] Learntotradethemarket.com. Available at: <http://www.learntotradethemarket.com/forex-articles/most-successful-price-action-trader-in-history-munehisa-homma>