Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Economics

Bachelor Thesis

Bitcoin and other virtual currencies

Diana Rokhmina

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Diana Rokhmina

Business Administration

Thesis title

Bitcoin and other virtual currencies

Objectives of thesis

Considering the crisis and numerous problems in the financial systems nowadays, it's hard to underestimate the importance of developing new ways of performing main fiscal operations. Therefore, main objectives of this work are:

- to evaluate various kinds of cryptocurrency, bitcoin in particular, as the first one in history and the main one currently;

- to identify the recurring role of digital assets in the world's economy by making an assessment of their main pros and cons;

- to study out the need for bitcoin as a financial instrument in the future.

Methodology

To make sure that the research made to meet the objectives of this work is sound, the necessary data for the analysis of bitcoin and other virtual currencies is to be gathered, presented using descriptive method and evaluated by being synthesized.

Further assessment of the results will be implemented by means of statistical analysis and qualitative data description, to identify digital assets' role in today's financial system and to draw a conclusion about it's future in the economy.

The proposed extent of the thesis

40 pages

Keywords

Cryptocurrency, digital payment, transaction, blockchain, Bitcoin, scrypt, altcoin

---

Recommended information sources

Antonopoulos, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. December, 2014

Campell, Robert. Bitcoin A to Z – The completion guide for beginner to buy, sell, invest and trade, July 10, 2017, Amazon Digital Services LLC

Nakatomo, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. October, 2008. Available at: http://bitcoins.info/bitcoin.pdf

Ron, Dorit and Shamir, Adi. Quantitative Analysis of the Full Bitcoin Transaction Graph. Financial Cryptography 2013

Rosenfeld, Meni. Analysis of Bitcoin Pooled Mining Reward Systems. November 17, 2011. Available at: https://bitcoil.co.il/pool_analysis.pdf

Vigna, P. and Casey, M. (n.d.). The Age of Cryptocurrency. New York, 2015

What is Bitcoin?: We Use Coins [online]. 2010 [cit. 2012-05-15]. Available at: http://www.weusecoins.com

---

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: 22. 12. 2017

prof. Ing. Miroslav Svatoš, CSc.

Head of department

Electronic approval: 12. 1. 2018

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 28. 02. 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 15.03.2018 _____

Bitcoin a další virtuální měny

Abstrakt

Díky nadšení IT specialistů vznikly virtuální měny, které se letos poprvé objevily na burzovním trhu a následně se v něm úspěšně zakotvily, a tím získaly uznání finančních odborníků a analytiků. Dnes Bitcoin je nejúspěšnější a nejpopulárnější kryptoměnou. Bitcoin je souborem na počítači jako třeba hudba nebo textové dokumenty. Stejně jako hotovost Bitcoin může být zničen nebo ztracen. Na rozdíl od tradičních měn Bitcoin není ovládán jakousi firmou, finanční institucí nebo vládou. Místo toho je jeho podstata založena na peer-to-peerové síti klientů, kteří používají dostupný Bitcoinový software s otevřeným zdrojovým kódem. (David Allen Bronleewe, 2011) Ukládání Bitcoinů může být svěřeno online službě nebo se je dá uložit přímo na osobní počítač a následně vynaložit na virtuální i reálné zboží a služby.

Tato diplomová práce se zabývá koncepcí elektronických peněz a digitálních měn, faktory, které ovlivňují jejích vývoj a ovlivňují jejích hodnotu. Vysvětluje podstatu futuresů, shrnuje všechny důležité poznatky o nejúspěšnějších digitálních měnách a objasňuje výsledky inovačního vniknutí Bitcoina a možné cesty jeho dalšího rozvoje.

Klíčová slova: Crypocurrency, digitální platby, transakce, blockchain, Bitcoin, scrypt, altcoin, futures, investice.

Bitcoin and other virtual currencies

Abstract

In virtue of the enthusiasm of IT specialists, virtual currencies have emerged, becoming a novelty for the exchange market, and subsequently have successfully embedded in it, receiving recognition of financial experts and analysts. The most successful and well-known cryptocurrency today is Bitcoin. Bitcoins are computer files, analogous to music or a text document. Just like cash it can be destroyed or lost. However, unlike traditional currencies, it is not controlled by a single company, financial institution or government. Instead, its work is based on peer-to-peer network of clients running the open-source Bitcoin software. (David Allen Bronleewe, 2011) Its storage is either trusted on an online service or it's being kept on a personal computer and can be spent on both virtual and real goods and services.

This thesis work discusses the concept of e-money and digital currencies, factors that influence its development and affect its value. It explains the idea behind futures, summarizes all relevant data about the most successful digital currencies of today and clarifies the outcomes of Bitcoin's innovative intrusion and possible ways of its further development.

Keywords: Cryptocurrency, digital payment, transaction, blockchain, Bitcoin, scrypt, altcoin, futures, investment, miner.

CONTENT

TABLE OF FIGURES

1 Introduction

The world does not stand still. Today – in the age of constantly evolving technologies, their implementation is carried out in all areas of our lives. These alterations also affect the economic environment: in virtue of the enthusiasm of IT specialists, virtual currencies have emerged, becoming a novelty for the exchange market, and subsequently have successfully embedded in it, receiving recognition from the majority of financial experts and analysts in the field of economy and investment. This type of currency is fundamentally new and is unlike any kind of payment types that existed before. At a present moment, there are over a thousand cryptocurrencies on a market, but only a few of them can be called prosperous and are well recognized by investors and, therefore, have a high market capitalization of at least $1 billion. One of the most common and well-known projects in the sphere of digital currency is Bitcoin, which appeared in 2009 and since then has fundamentally changed the perception of the population regarding this new type of payment, and, additionally, now accounts for about a half of the market capitalization of all virtual currencies in general. Bitcoin is a convenient, cheap and technological way of paying for goods and services, which makes it more and more popular today among millions of people. Performing the functions of servicing the motion of financial resources, Bitcoin acts as an instrument of payment and exchange operations in the channels of movement of national money and world currencies. The applicability of the work and the research is in the relatively recent appearance of Bitcoin and other virtual currencies on the marker, as well as the speed of their development and the rapid growth of prices per-token. Simultaneously, their role in the economic operations and systems in the future is to be discussed from the perspective of regulation and practical use.

2 Objectives and methodology

2.1 *Objectives*

Given the crisis and numerous problems in financial systems at present, an importance of developing new ways of performing basic financial operations arises. The main goal of the work is to analyse Bitcoin as the most popular and successful cryptocurrency on the market, determine the factors that influence its price per coin, and could possibly be helpful in making the assessment, as well as the prognosis of Bitcoin's value changes in the future. However, there are several objectives that are to be met in order to reach the final goal of the work:

- to study out the concept of e-money – an electronic representation of money, explain the main concepts of digital currencies and, finally, to analyse the common points and fundamental differences between them;
- to understand the factors, that could potentially influence the development of cryptocurrencies;
- to assess the basic concepts of Bitcoin, the timeline of its evolution, provide the necessary technical background for understanding basic Bitcoin operations, the ways it can be obtained; to identify the determinants of its price fluctuations in the past and recognize which ones of them are still sound right now and might be in the future;
- to provide a basic overview of the futures and ascertain their meaning for Bitcoin's value;
- to specify various kinds of digital currencies, evaluate their future potential in the form of a guide for the ones who are looking to invest in cryptocurrency in the following year;
- to determine the need for bitcoin as a financial instrument in the future and study out the possible ways of its further development.

2.2 *Methodology*

The Bachelor thesis consists of the following parts: literature review, practical part and conclusion. Main focus of the theoretical part is based on collecting, summarizing and presenting all the relevant data about electronic types of payment, digital currencies and Bitcoin. The necessary research has been implemented by means of obtaining data from existing documents – literature and publications – through documentary analysis.

The aim of the practical part is to conduct a trend analysis of Bitcoin's price fluctuations and its determinants; therefore, the applicable information and statistical data on Bitcoin's prices throughout recent years and its dependency on BTC or another cryptocurrencies acceptance has been gathered and evaluated by being synthesized.

Finally, to identify digital assets' place in the financial systems and economy of the future, a prognosis regarding analytical results of the researches performed has been assembled. Additionally, other types of digital currencies have been studied out, analysed in terms of their market capitalization, current price and circulating supply, and presented in form of an investent guide, providing all time price graphs and further relevant information.

3 Literature review

In order to understand Bitcoin's and other virtual currencies potential impact on the economy, financial systems and international foreign currency exchange, it is necessary to know and comprehend exactly what cryptocurrency is, where it originates from, through which algorithms it works and how it can be obtained. This chapter provides an overview of the e-money and cryptocurrency, explains technology behind digital currency, factors influencing its development and how its platform is being supported, discusses the history of Bitcoin and its potential benefits over traditional currencies.

3.1 *Cryptocurrency in accordance to e-money*

3.1.1 Definition of e-money

Money in a traditional sense consists of two basic formats: physical, such as notes and coins, usually with legal tender status, as well as different types of electronic representations of money – deposits in the central bank, that can be used for payments, or commercial bank money. Let's take a closer look at the second mentioned format. Electronic money or e-money, defined by Committee's on Payments and Market Infrastructures (CPMI) glossary of terms used in payments and settlement systems as "*value stored electronically in a device such as a chip card or a hard drive in a personal computer*", is commonly used around the world today.

E-money balances according to the legislation, applicable in a particular jurisdiction, and is usually denominated in the same currency as central bank or commercial bank money. It can easily be exchanged at par value or redeemed in cash. (CPMI report on digital currencies, November 2015)

As mentioned in CPMI's publication on digital currencies, subsequent definitions of e-money have broadened the concept to include a variety of retail payment mechanisms, possibly extending to digital currency schemes. Although digital currencies meet the general conceptual meaning of e-money, they do not satisfy the legal definition of it,

according to most jurisdictions. In the case of the European Union, for example, e-money is required to have the issued balances as a claim on the issuer, issued on receipt of funds. Therefore, as explained in CPMI report mentioned above, units of digital currencies, even though they can be bought and sold later on, in some schemes will not be considered e-money in a legal sense as they are not issued in exchange for funds and may not be issued by any individual or institution.

3.1.2 Cryptocurrency's distinguishing features

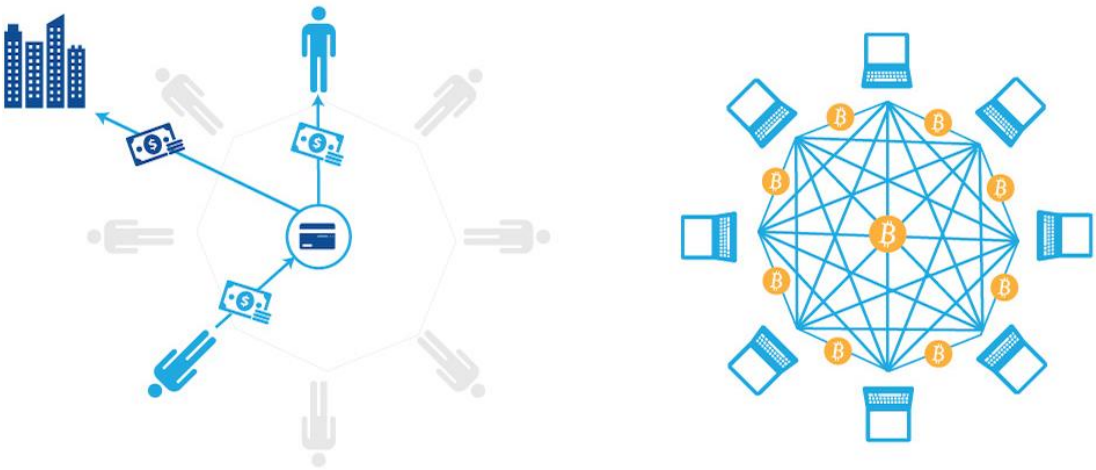
Currently, hundreds of similar distributed ledgers-based digital currency schemes have been introduced and successfully exist or are in development. They are sharing several key features that make them different from traditional e-money schemes. (Morten Bech, September 2017)

According to Bech, first of all, in the majority of cases, these digital currencies are assets, which value, similar to commodities such as gold, is determined by supply and demand. They, however, have a zero-intrinsic value. Moreover, in contrast to traditional e-money, cryptocurrencies are not considered a liability of any individual or institution and aren't backed by any authority, resulting into their value relying only on the belief that they might be exchanged for other goods or services. The establishment of new units, in other words - the management of the total supply, is generally defined by a computer protocol and an algorithm, as no single entity has the discretion to manage the supply of units over time. The invention and issuance of new units is determined by various schemes, which have different long-run supplies and specific predetermined rules that help to create scarcity in the supply. These schemes tend not to be denominated in or tied to a sovereign currency, such as the US dollar or the euro. In case of Bitcoin, for example, the unit of value being transferred is a bitcoin.

The second distinguishing feature of these schemes is how the value in being transferred from a payer to a payee. Until recently, a peer-to-peer exchange was restricted to money's physical format, because of the absence of trusted intermediaries. According to a 2015 CPMI report on digital currencies for the Bank for international settlements, electronic representations of money are usually exchanged in centralised infrastructures, where a trusted entity clears and settles transactions, and the key innovation of some of these digital

currency schemes is the use of distributed ledgers to allow remote peer-to-peer exchanges of electronic value in the absence of trust between the parties and without the need for intermediaries. Thus, a payer is able to access the value through a digital wallet, where his/her cryptographic keys are stored and used to initiate a transaction that transfers a specific amount of value to the payee. Performed transaction then goes through a process of validation and adds it to a unified ledger, where many copies are distributed across the peer-to-peer network. This process for digital currency schemes can vary in terms of speed, efficiency and security. The way transactions are recorded is similar to the way the value is transferred and stored. Finally, as mentioned above, when the distributed across the decentralized network ledger is updated, the transfer is completed. The ledger can store various amounts of information: from a bare minimum, such as the distribution of value across network, to details about the payer, payee, transactions and balances. In the majority of cases today, very little information is required to be kept in the ledger in order to perform cryptocurrency schemes.

Figure 1: Banks/Financial Institutions vs Decentralized P2P network



Source: *https://www.marutitech.com*

Finally, according to the same report of the year 2015 by the CPMI mentioned above, traditional e-money schemes require several service providers, embedded in the operation, such as: the issuers of e-money, the network operators, the vendors of specialised hardware and software, the acquirers of e-money, and the clearer(s) of e-money transactions. These providers represent liabilities on the issuer's balance sheet. Even though some

cryptocurrency schemes are actively promoted by certain intermediaries, they are not operated by any specific individual or institution, and their decentralized nature excludes identifiable scheme operator, a role that is typically played by those financial or other institutions that specialise in clearing in the case of e-money. Various technical services, such as: "wallet" services, that enable digital currency users to transfer value, or help to facilitate the exchange between cryptocurrency units and sovereign ones, are provided by a number of intermediaries. In some instances, these intermediaries store the cryptographic keys to the value for their customers.

The Committee on Payments and Market Infrastructures claims, that potentially disruptive innovations associated with digital currency schemes refer to the following closely linked aspects: the "asset aspect", which means, that digital currencies are issued automatically and are not a liability of any party, as well as the "payment aspect", where payment mechanisms are based on a distributed ledger that allows peer-to-peer transfers without the involvement of trusted third parties. Degrees of interaction with existing infrastructures and payment service providers define the numerous ways in which digital currencies and distributed ledgers could operate. Some cryptocurrency schemes aim to create an isolated-working network, or payment mechanisms with only a marginal connection to it, which would allow the users of the system to directly open accounts in a single distributed ledger, send and receive peer-to-peer payments denominated in the native to the network digital currency. *The only connection with the existing payment system would occur in exchanges and trading platforms, where the digital currency units would be exchanged for sovereign currency, usually at free-floating rates that reflect supply and demand*.[2] (Digital currencies – Bank for International Settlements, 2015)

3.2 *Factors influencing the development of digital currencies*

Cryptocurrencies predicated on the utilization of a distributed ledger represent a genuinely incipient development in the payments landscape. Yet, the majority of the factors that have spurred the development of digital currencies have withal stimulated innovation in more traditional payment methods. Among some of the factors underpinning both digital currency development and broader payment system innovation are reduced cost and increased speed, including the areas of e-commerce and cross-border transactions. It's particularly important to highlight the role of technology in driving the development of

digital currencies and other innovations. Technological advances have always been identified as a key, enabling the changes in payment services, with an impact on both demand and supply of these. Nevertheless, there's a range of factors, related to cryptocurrency's decentralized features, which are individual to it, based on distributed ledges. (Rodney Garatt, 2017)

3.2.1 Supply side factors

According to the BIS reports on digital currencies (2015), on the supply side, the development of digital currencies based on the use of a distributed ledger has been mostly driven by non-banks private sector. For the most part, financial institutes tend to avoid interacting with cryptocurrency's intermediaries, instead of engaging with them directly, due to uncertainty over legal or compliance issues. Only recently there have been reports regarding private banks' research on the potential business opportunities arising from digital currencies and distributed ledgers, such as investing in companies that provide corresponding services, among which - offering customers interfaces to digital currency exchanges or exploring the use of decentralised ledgers for office applications. The question, which emerges while considering implementing this type of digital currency-linked services, is whether such implementation might pose security challenges. The drivers that have led to the development of digital currency schemes are additionally diverse, and underlie many of the differences in design between various initiatives. One of them relates to commercial versus not-for-profit motives. If commercial motives are the main driver, the entity might be seeking to earn profits from digital currency schemes in a number of different ways: these profits can be achieved by issuing cryptocurrency units from a capital gain on the units associated with the scheme and from transaction fees from payment intermediation. Cryptocurrencies can also form a part of a larger business model where the scheme is generally created to produce revenues through the sale of other items or services. However, a greater number of digital distributed ledgers-based schemes have been developed with particular non-profit objectives. These might, first of all, include the motivation to create and use alternative methods to existing financial infrastructure, or facilitating financial inclusion, as well as the benefits gained through experimentation and innovation for its own sake.

Let’s have an overview of some of the supply side factors that may be influential for the future development of digital currencies based on the use of a distributed ledger, presented by Bank of International Settlements’ report on the topic of interest:

• *Fragmentation:* More than 600 cryptocurrencies with different protocols for transaction processing and confirmation and different approaches to the growth in the supply of digital units are in circulation today. This diversity may represent difficulties in use and acceptance of these schemes, as fragmentation in various initiatives could be an obstacle to achieving the critical mass necessary to realise the network effects that are common to all payment networks.

• *Scalability and efficiency:* Due to a limited scale and acceptance, cryptocurrency schemes are expected to be able to evolve in order to process a significantly higher number of transactions, as the number of transactions that are being processed today is smaller than those handled by widely used retail payment systems. The increased efficiency of these schemes cannot be underestimated, some of the most important ones are resource-intensive in terms of the energy and computing power required to process a small number of transactions. Improvements in processing power and speed and the tendency for computing and hardware costs to decrease imply that scalability and efficiency issues might be addressed over time. Other schemes require fewer resources to operate.

• *Pseudonymity:* It’s important to note that cryptocurrency transactions are normally observed on a public ledger and aren’t intentionally disguised via anonymizers or mixers, thus the degree of anonymity and privacy provided by some digital schemes might dissuade financial system participants to use it or to provide facilities for cryptocurrency use to their customers, as AML/CFT requirements may be difficult to satisfy in relation to digital currency transactions.

• *Technical and security concerns:* To make sure the distributed ledger, which is the base for the majority of cryptocurrencies, is singular, in other words, that the ledger, with its history of transactions and balances, distributed across the network, is unique, digital currencies have to set up consensus among network participants. Their acceptance can be affected, if there’s a possibility of a long-term coexistence of different versions of the ledger, or, for example, if the procedures to achieve consensus are not performed correctly.

Malefactors can seek to obtain profit by entering fraudulent transactions into the ledger and by encouraging other participants to verify these falsified operations.

• *Business model sustainability:* For some digital currency schemes, building a sustainable business model in the long term can become a particular problem. In various cases, incentives for certain participants supporting this scheme, by, for example, verifying transactions and including them in a ledger, are directly related to the issuance of a currency that tend to become limited or be reduced over time. At the same time, the costs incurred by these entities may be significant in some digital currency schemes. In these cases, it is unsure whether there will be the right incentives for the functioning of the scheme, when the supply of new digital currency units will decrease or disappear. Moreover, to compensate for the loss of revenue in the form of new digital currency units, it is possible to increase the charge per transaction, but it can affect the demand and long-term sustainability of the scheme. It is noteworthy that not all schemes correspond to the same model, and the costs associated with the operation of the network and the commission for transactions can differ. It should also be emphasized that, to a large extent, these factors seem to be more closely related to the specific technical implementations and procedures of the various digital currency schemes, than to the wider concept of distributed ledgers. Competing schemes, all of which are based on distributed ledger systems, can follow different business models depending on their design, as well as varying degrees of efficiency, anonymity or technical security.

3.2.2 Demand side factors

Digital currencies based on distributed ledgers are expected to provide end-users with advantages over traditional services in order to increase reception and usage. (Morten Linemann Bech, 2017) Some of the potential factors that could affect the evolution of demand for cryptocurrencies and the payment mechanisms associated with them, as reported by CPMI for BIS (2015) are:

• *Security:* An important factor in the demand associated with the use of digital currencies based on distributed registers is the risk of loss. Security breaches can not only undermine users' confidence in the digital currency scheme, but also influence the intermediaries faced by the end-user after performing operations with digital currency units. Somewhat

similarly to cash, if a user loses certain specific information that grants him "ownership" to the digital currency units stored in the distributed ledger, these units are not likely to be recoverable. Some digital currencies users rely on intermediaries to hold and store information related to their possession of the digital currency units and therefore must trust these intermediaries to reduce the risk of loss from being hacked, operational disruptions or misappropriation.

• *Cost:* It has been argued that the transaction fees offered by distributed ledgers-based digital currencies might be lower than the ones of the other payment methods. In some schemes, payment processing is rewarded by newly issued units, which may potentially receive "capital gains" measured in units of sovereign currency, rather than transaction fees. In this regard, such digital currency schemes become an attractive alternative for some individuals and organizations, in particular for cross-border payments, which usually bear high fees paid to payment service providers. In addition, to facilitate the payments, transactions in these schemes do not require intermediaries that may be related to high processing costs. However, the transaction costs in these schemes are not always transparent, and there may be other costs, for example, if the user does not want to maintain the balances expressed in digital currency units, there is a conversion fee between the digital currency and the sovereign currency.

• *Usability:* Usually, ease of use is significant for the adoption of payment methods and mechanisms and can reflect such factors, as the number of steps in the payment process and whether a particular process is convenient and easy to integrate with other ones. Some advantages of ease of use, compared to existing methods, can determine whether digital currencies and distributed ledgers will be used. Currently, many providers aim to improve the experience of users in digital currency schemes and to make it easier.

• *Volatility and risk of loss:* If users prefer to hold a digital currency asset received as a payment, then they might experience the losses and expenses associated with price and liquidity risks. Considering the volatility and market dislocations that have been witnessed by some of the best-known digital currency schemes, these risks can be substantial. For most users the variability of exchange rates represents an obstacle to wider adoption, while the others see the volatility as an opportunity to make speculative profits out of it. It remains an open question to which degree the price of volatility will decrease if

cryptocurrency schemes are widely used, as well as the long-term risk of loss from holding digital currencies with zero intrinsic value.

• *Irrevocability:* Distributed ledger-based schemes often do not have the capacity to resolve disputes and thus offer irrevocable payments, which will provide payee's with compensation for payments, cancelled due to fraud or chargebacks. Although this function may be attractive to such payees as, for example, sellers, it can also discourage acceptance and use by consumers.

• *Processing speed:* Cryptocurrencies are said to have the potential to be faster than traditional systems in clearing and settling transactions, although the processing speed of the various schemes may change accordingly to their technical details. Nevertheless, it is necessary to mention that a number of innovations not related to digital currencies - for example faster retail payment systems - are aimed at addressing this growing demand for improved payment speed as well. In addition, real-time gross settlement systems already underpin the wholesale financial markets and provide opportunities for very rapid payment, as well as settlement of large payments.

• *Cross-border reach:* Virtual currencies, based on the distributed ledgers by its nature are open networks with global coverage. The digital schemes, used to perform the transactions, do not distinguish users based on their location and, therefore, allow the transfer of value between users across borders. Besides, the transaction speed does not depend on the location of the payer and the payee either. In addition, due to the decentralized character of these digital currency schemes, it is difficult to impose restrictions on transactions that can be applied by national authorities on cross-border operations.

• *Data privacy/pseudonymity*: Although this is not the main feature of distributed ledgers, some digital currency schemes, based on them, have the ability to implement financial operations without disclosing personal data or confidential payment credentials. Due to this fact, combined with cryptocurrency global reach, as well as the avoidance of authorities and bank services, which provides anonymity, that might be attractive to the users looking to circumvent laws and regulations, digital currency schemes are potentially vulnerable to illicit use. However, there are legitimate reasons why users may prefer to use anonymous payment methods, over the other ones, for example, in case of online sales from person to

person, where the parties usually do not have previous experience of interaction and the recipient is not trusted to protect the disclosed information.

• *Marketing and reputational effects:* Due to developing technologies, virtual currencies are regarded as an innovative and interesting payment method. The technology may attract the users to start buying products and services online due to its newness and simplicity, while the merchants might find accepting payments through a digital currency schemes more appealing as it boosts demand for their goods.

The factors mentioned above are not only relevant for the direct use of the cryptocurrencies and distributed ledgers by end users, but can also potentially be applied indirectly, for instance when a provider, responsible for payment services uses a digital currency scheme as its back-end payment infrastructure.

3.2.3 Role of regulation

Regulatory arrangements may be influential towards the development and use of digital currencies. Generally speaking, their novelty, recent development and implementation of the design do not allow them to be specifically regulated or classified under already existing regulatory definitions and structures. Indeed, even though other identifiable third-party providers can be regulated easier, unlimited borderless online nature of the virtual currencies, as well as the absence of an identifiable "issuer" of the instrument, might create particular problems for regulatory attempts made by the national authority. Boundless and without any restrictions, generally unregulated online systems do not include layers of correspondent banks and can potentially make transactions faster, more convenient and feasible at lower costs. On the other hand, these types of systems have also caused serious concerns of law enforcement institutes and authorities regarding the use of the discussed systems for unlawful activities, as well as compliance with the obligations that are applicable to traditional methods of payment and intermediation. There has been a number of publications on cryptocurrencies by The Financial Action Task Force (FATF), and it's necessary to mention one of the reports, published in 2014, which discussed digital currency issues, noting that *"convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and*

terrorist financing", however, more recently a guide to a risk-based approach to virtual currency payments has been published, observing the importance of the establishment of certain recommendations in different jurisdictions relating to the same goods and services according to their functions and risk profile for enhancing the effectiveness of the international AML / CFT standards. While regulation normally imposes costs on intermediaries and providers of the payment systems, providers of digital currencies might find the fact of not being a subject of these costs beneficial. Regulatory costs may arise, in particular, for liabilities directed to the issuer of a payment. Several countries have already begun adjusting existing regulations and applying new rules to address the problems of law enforcement. Some users and developers of digital currencies are against such changes, considering them incompatible with the advent of new technologies that are less regulated than the traditional payment industry. Others consider the lack of regulation an obstacle to increasing public confidence in the matter, as some participants may refrain from investing in this new technology due to legal uncertainty and lack of protection provided for users. (Anders Laursen and Jon Hasling Kyed, Payment Systems, 2014)

3.3 *Introduction to Bitcoin*

3.3.1 The history of creation and development

The developer of the first graphic NCSA Mosaic Internet browser – Marc Andreessen argues that the Bitcoin system, at the fundamental level, is a result of a breakthrough of 20 years of research on cryptocurrencies and 40 years of common efforts on cryptography of thousands of computer scientists around the world. Let's consider the timeline of the major events that have led to development and introduction of the Bitcoin:

• In **1983**, *David Chaum and Stefan Brands* proposed the first "electronic cash" protocols.

• In **May 1997**, *Adam Back* offered Hashcash, based on the system of proof of the work's performance, to counteract the sending out of spam and DoS-attacks. Subsequently, another implementation of a similar system became a part of the procedure for creating new blocks in the bitcoin database.

• In **1998**, *Wei Dai*, a graduate from the University of Washington, described the ideas of the cryptocurrency "b-money" in the cipher mailing. Regardless of Dai's work, around the same time, *Nick Szabo* – a computer scientist and cryptographer – proposed the same ideas for "bit-gold". Nick Szabo has 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 on, an American computer scientist and developer *Hal Finney* implemented a bundle of hash-block chains for a chip-based Hashcash system for IBM encryption within the TPM specification and became the second member of the Bitcoin network.

• In **2008**, a file describing the protocol and the principle of operation of the payment system in the form of a peer-to-peer network was published by a person or a group of people under the pseudonym *Satoshi Nakamoto*. According to Satoshi, development of the protocol began in 2007 and was completed in 2009, when the code of the client program was published.

• On **January 3, 2009**, the first block of 50 bitcoins was generated.

• On **January 12, 2009**, the first Bitcoin operation was completed: Satoshi Nakamoto sent Hel Finney 10 Bitcoins.

• In **September 2009** the first exchange bitcoins took place : *Martti Malmi* sent 5050 bitcoins to a user with a nickname *NewLibertyStandard*, and received 5.02 dollars on his PayPal account in exchange.

• The first bitcoin exchange for real goods occurred in **May 2010** - an American *Laszlo Hanech* received two pizzas for 10 000 bitcoins.

Further development is coordinated and carried out by the developer community, however, any significant changes in the protocol must be accepted by the majority of owners of the mining pools.

• On **August 1, 2017**, the block structure of the blockchain has been changed. The group of developers and miners launched a Bitcoin "fork" under the name "Bitcoin Cash". The new cryptocurrency has a backward compatibility with Bitcoin on the block structure until August 1, but an incompatible structure after it.

As discussed by Nicholas Plassaras (2013), Bitcoin, conceptually, is two things in one: it is, first of all, a digital currency with a legal tender status, but with no physical counterpart, and, secondly, a *currency provided by private enterprise aimed at combatting government monopolies on the supply of money* (Friedrich A. Hayek). In case of Bitcoin transactions and operations, traditional financial services providers, such as central banks or government institutions, are not involved. The interaction between traditional and digital currencies is not regulated by law. Therefore, as it has been previously mentioned, there is little legal regulation or supervision of the usage: all of the Bitcoin's aspects, from its supply to the means by which it's generated, are controlled by its users only. Hayek argued that traditional currencies, supported by the government, are a subject to a number of weaknesses, among which are the exposure to inflation and political corruption. Moreover, Hayek claimed, that private currencies are more stable than the traditional ones, because they do not share these shortcomings. As mentioned above, in 2009, an anonymous hacker, or a group of hackers, calling himself (or themselves) Satoshi Nakamoto, created Bitcoin - world's first digital, decentralized and partially anonymous currency. Wei Dai, whose article on cryptocurrencies written back in 1998 became Nakamoto's source of inspiration, pictured a system in which *"untraceable pseudonymous entities . . . [could] cooperate with each other more efficiently, by providing them with a medium of exchange and a method of enforcing contracts."*He had an idea of creating an exchange environment that wouldn't have a need for intermediaries in electronic transactions, and could also avoid government involvement, which, according to him*"[was] not [only] temporarily destroyed but permanently forbidden and permanently unnecessary."*

Unlike traditional currencies, the value of which is determined by law and guaranteed by the state, Bitcoin is not supported by the government or a legal entity. Additionally, Bitcoin does not have a central authority in charge of the money supply or a clearing center. Bitcoin transactions do not involve any traditional financial institutions; all the steps of the transactions are performed solely by the users, involved in the given financial operation. Bitcoins are not tied to any real currency. Instead, their value in relativity to other currencies is determined by supply and demand. To maintain the anonymity of its users and the integrity of transactions, Bitcoin works using peer-to-peer networks and cryptography. Its software is an open source that allows all users to view and understand how a basic computer code works.

Described by Nikolei M. Kaplanov in his publication ‘Nerdy money: bitcoin, the private digital currency, and the case against its regulation’ (2012), bitcoins are computer files, analogous to music or a text file, and similarly to cash it can be destroyed or lost. Their storage is either trusted on an online service or it’s being kept on a personal computer and can be spent on both virtual and real goods and services. Since bitcoins are just computer files, the procedure of "spending" them is as easy as sending an e-mail, as it simply entails sending them from one user to another. Individual transactions of the bitcoins are encrypted, registered by a decentralized network running on thousands of computers, and recorded in a public accounting book – a ledger, which keeps the record of how many bitcoins have been taken or spent. However, such ledger does not provide any identification information of the participants of the transaction, to ensure the anonymity of the users. Bitcoins are transferred from one user to another as soon as the transaction has been cleared by another Bitcoin user in the Bitcoin peer-to-peer network. Transactions occur without the presence of any entity, such as government, bank, payment network or another third party. Instead of traditional institutional protections Bitcoin relies on various technological measures, for example a “cryptographic proof” system, to ensure the security of its transactions.

3.3.2 How to obtain Bitcoin

There are three general ways for users to obtain bitcoins. First of all, they can be purchased by exchanging "real money" (dollar or Euro), for Bitcoin files. Just like the traditional market, the price of bitcoins floats against other currencies and is estimated by supply and demand. Secondly, again, similarly to traditional currency, users can get bitcoins in exchange for goods or services. Finally, it’s possible to gain Bitcoin by generating them through a process called "mining", that allows the users to generate digital currency rather than buying it. (Nicholas A. Plassaras, 2013) As explained by Allan Harris and Corey Conley in “Will Bitcoin Kill the Dollar?” a user who wishes to “mine” a Bitcoin essentially uses their computer’s processing power to solve a complicated computer algorithm. Bitcoins are awarded every ten minutes depending on which miner can calculate the number below a certain threshold. However, mining is not limitless, but a hard and time-consuming process. *The Tuesday Podcast: Bitcoin, NPR Planet Money (2011)* argued, that the typical office computer would take about five to ten years of running

nonstop to find any Bitcoins, and the cost of electricity would outweigh the value of the Bitcoins produced. Moreover, the number of the units generated through mining is controlled and over time its software slows this generation so that there will never be more than 21 million in circulation. By doing so, the system makes sure that Bitcoin cannot be artificially inflated or deflated or get controlled by any entity with an aim to destroy its value.

3.3.3 Bitcoin Miner

Bitcoin Miner is a software that is entitled to be used to confirm transactions after its connected to the network to benefit from BTC. Mining can take place in a pool or solo (meaning you are not a part of a mining pool), and the calculations can be made by using CPU (central processing unit) or GPU (graphics processing unit). In other words, while the actual Bitcoin development process is handled by its mining hardware itself, a special mining software is needed in order for Bitcoin miners to be connected to the blockchain and Bitcoin mining pool as well, if they are a part of one. The work is being delivered to the miners by the software, which then receives the completed work and relays that information back to the blockchain and the mining pool. The best software of such kind can run on almost any operating system, such as OSX, Windows, Linux. Besides relaying the input and output of the Bitcoin miners to the blockchain, the software monitors them and, additionally, displays such general statistics as temperature, fan speed, as well as the hashrate and an average speed of the Bitcoin miner.

There are a few different types of Bitcoin mining software out there and each have their own advantages and disadvantages:

- **Phoenix Miner** was released by the Bitcoin community in 2011. It is defined as a BTC mining software that can work with a sub-memory of 300MHz. When mining, it searches for nonce (an arbitrary number used only once in a cryptographic communication) in the entire 32-bit space. The project is open-source and is available for free with a X11 license. Miner can connect via the MultiMiner Protocol (MMP), used to connect to the MultiMiner Server.

- **Poclbm** (PyOpenCL bitcoin miner) is a mining machine written in Python designed for mining on a GPU, that uses OpenCL to quickly execute hash calculations.

Works with AMD - 4xxx and higher cards, Nvidia - 8xxx and higher. There is a GUI extension for it, called poclbm-gui or GUIMiner, as well as a modified version called poclb-mod. If the modification is used for field mining, its efficiency can grow up to 100% compared to the basic miner, which has an average efficiency of about 20%. Poclbm is available for Windows and Linux, Poclbm-gui for Windows and Mac, combo-mod for Windows and Linux.

- **Cpu Miner** is a simple software that performs pool or solo mining. In the application pool, it receives a block from the server and tries to find a nonce. After it's found, this value is sent to the server. Communication with the server takes place over HTTP POST by default on port 8332. The application is designed as multi-threaded, which is used with a multi-core CPU.

4 Practical part

The objective of this chapter are:

- to conduct a trend analysis and an investment evaluation based on qualitative statistical data on Bitcoin's prices throughout recent years;
- to consider the acceptance of the payments via Bitcoin or other cryptocurrencies in accordance with its price chart;
- to research and study Bitcoin's futures as its main derivative;
- to identify digital assets' place in the financial systems and economy of the future, by assembling a prognosis, regarding analytical results of the researches performed.

First, let's consider a timeline of how the value of the Bitcoin was developping:

In the year of **2009**, when Bitcoin was introduced with the initial price of just $0.001, it wasn't expected to gain such popularity. Over the next five years, the rise of its price was slow with little oscillations, as there were no significant events.

In **2013**, the financial crisis in the Republic of Cyprus attracted a lot of attention to the Bitcoin The year has ended with a rapid price increase, growing by 1000 percent, as

starting from November the BTC was bought by the Chinese in large quantities. Nevertheless, such value rise didn't last long.

In February **2014**, Mt. Gox – a Shibuya (Tokyo, Japan) based exchange, controlling around 60 percent of all digital transactions at a time – has suffered a DDoS attack. As an impact the Bitcoin lost 40 percent of its value and continued to fall throughout the year.

During **2015** and **2016**, Bitcoin started taking its positions back by earning more trust and interest among investors with a slow, but steady price rise throughout the year.

In **2017**, the Bitcoin went from the 14 percent price fall to being the fastest-growing asset in the world, having gone up by over 900 percent and reaching its historic high at $17,900 in December.

Figure 2: Market price chart (USD)

Source: coinmarketcap

The year of 2017 has become significant in the history of Bitcoin and digital currencies in general, as BTC rate broke all the possible records and the value of other similar currencies are also constantly increasing its value. Despite the growth in its cost, Bitcoin in particular, unknown for some people just a year ago, has become a hot topic and a reason for many debates. The ones, who didn't know about it, are now thinking about buying some amount of shares as their first investment, and more experienced investors, who were skeptical about the Bitcoin in the past, due to its unsecure nature are now analyzing whether its value has reached its peak and what's the future of this cryptocurrency in our society. Despite its development and a significant increase in its popularity and demand, its role in the economic systems of the future is still questionable. Will bitcoin and other less popular

crypto-currencies become a classic method of payment for goods and services? Will its value continue on growing, or is it a bubble, ready to burst?

4.1 *Fundamental analysis and evaluation of the investment*

Fundamental analysis is a methodology widely used by investors. This evaluation method estimates the 'real' value of an investment, and then compares it to the price at which it is trading on financial markets, in order to make a judgement on the potential for future price fluctuations (gains or losses). It is based on the assumption that short term price may differ greatly from underlying value, due to the nature of financial markets, but that over a longer time horizon the two will tend to converge. Investors can therefore profit by using this methodology to gauge whether something is undervalued or overvalued, and then buy or sell accordingly. (Pablo Fernandez, 2007).

Fundamental analysis requires the investor to collect and process financial data that is relevant to the country's economy, including such determinants, as gross domestic product (GDP), unemployment rate, interest rates, national debt, reviews of industrial production and consumer spending, political events, etc.

The evaluation of the investment is one of the most important steps in the assessment of whether the project will be profitable in the future. This procedure includes the comparison of results and costs of the investment projects based on standard financial criteria.

Let's evaluate the profitability of the investment in Bitcoin over a period of 6 month, starting from 1st of October 2017 and ending on 1st of March 2018. The amount of the investment will be 10.000 US dollars. The net cash flows for a six-month period are shown in the table below:

Month	Price per token	% change	Cash paid	Cash equivalent	Cash flow
1	$ 4,403.74	-	$ 10,000.00	-	$ -10,000.00
2	$ 6,767.31	53,69	-	$ 15,369.00	$ 5,369.00
3	$ 10,975.60	62,18	-	$ 24,925.40	$ 9,556.40
4	$ 13,657.20	24,43	-	$ 31,014.69	$ 6,089.29
5	$ 9,170.54	-32,85	-	$ 20,826.37	$ -10,188.32
6	$ 10,951.00	19,41	-	$ 24,868.76	$ 4,042.39

The following assessment will be implemented by calculating project's net present value (NPV), profitability index, internal rate of return (IRR) and the payback period.

a. Net Present Value (NVP) shows the difference between the present value of cash inflows and outflows. The calculations are based on cash flows instead of net income and takes under consideration the time value of money. Discounted cash flow is calculated via multiplication of cash flow and discounted factor. Further, we summarize the results for each month and substract the amount of the original investment from this value:

NPV (time value interest at 5% p.m.)			
Month	**Cash flow**	**Discounted factor $(1+i)^{(-n)}$**	**CF discounted**
1	$ 5,369.00	0.95	5100.55
2	$ 9,556.40	0.907	8667.6548
3	$ 6,089.29	0.8638	5259.928702
4	$ -10,188.32	0.8227	-8381.930864
5	$ 4,042.39	0.7835	3167.212565
SUM			13813.4152
NPV = 13813.4152 - 10000 = 3813.4152			

Net Present value is positive, so the investment should be considered.

b. Profitability index compares the present value of future cash flows from an investment versus the current cost of making that investment. In our case, instead of present value we use NPV:

Profitability index
PI = 13813.4152 / 10000 = 1.3813

PI ratio greater than 1 is the most desirable outcome, as it shows that the investment is profitable.

c. Payback period calculates the minimum period required to make sure the revenues generated from the investment are greater, than the invested funds:

Payback period		
Month	**Cash flow**	**Accumulated cash flow**
1	-	-
2	5369	5369
3	9556.4	**14925.4**
4	6089.29	21014.69
5	-10188.32	10826.37
6	4042.39	14868.76

Having invested 10000 US dollars in the beginning of October 2017, generated revenues would exceed our funds by December 2017.

d. Internal Rate of Return (IRR) is an alternative way of assessing the profitability of the investment. It is a tool to evaluate or compare capital investments, the preference is given to a project with a highest IRR.

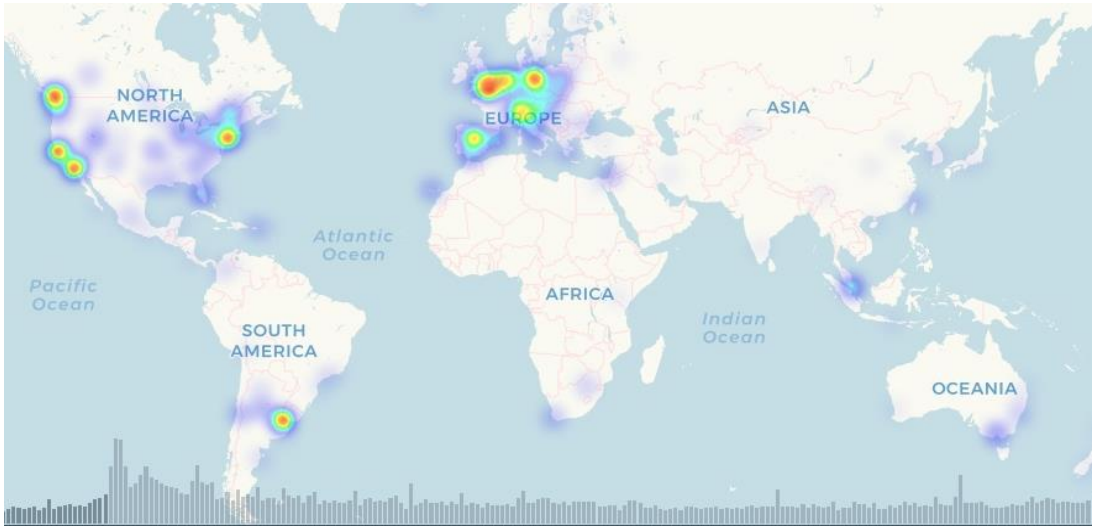
Internal rate of return (IRR)	
Month	**Cash flow**
1	-10000
2	5369
3	9556.4
4	6089.29
5	-10188.32
6	4042.39
IRR	**31%**

Having made the necessary calculations, as well as having observed Bitcoin's price changes over a period of 6 month, the investment can be considered profitable, as it has a positive NVP, IRR and a decent profitability index ratio. Moreover, due to a rapid increase in Bitcoin's cost per token in December, the real money equivalent of the return exceeds invested funds by more than 2 times in a relatively short period of time. However, this particular interval has been crucial for BTC value, resulting into a very high demand, which has also fundamentally influenced its current value. Thus, such high returns can't be expected in the nearest future, unless cryptocurrency is on a big rise again.

4.2 *Acceptance of the Bitcoin*

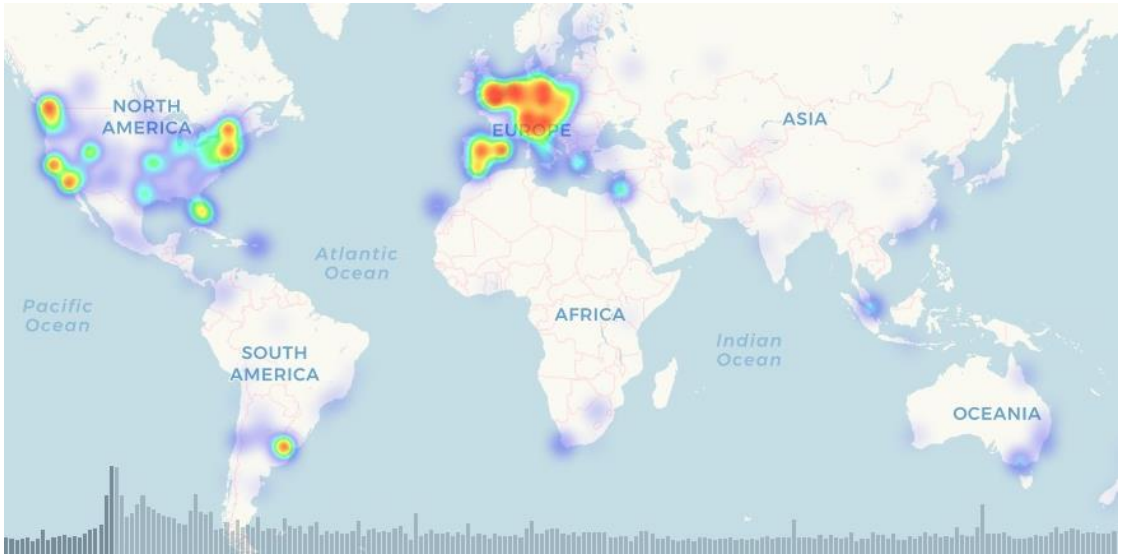
Regarding to the prevalence and degree of acceptance of Bitcoin by shops, cafes and so on, the number of businesses and institutions whose goods and services can be paid for using the cryptocurrency of our interest is increasing daily. It is worth noting that Brazil and the Czech Republic became the first locations where the option of paying with the help of Bitcoin became available. The first major leap on BTC acceptance path was in the period from 12 to 26 November 2013: the number of establishments that allow payment with the Bitcoin has almost doubled from 552 on November 12 to 1011 on the 26th of the same month, just two weeks after. Such a significant increase can be explained by an increase in demand from the Chinese market, mentioned earlier, accompanied by a major boost in the cost of Bitcoin which has also resulted in an upturn of its interest and popularity among investors. However, it should be noted that such growth in the number of the Bitcoin-

Figure 3: 552 venues on 12th November 2013



accepting venues occurred mostly in the areas where it already existed, such as Central and Western Europe, North America, United States in particular, and Brazil, rather than in the new places where the popularity of bitcoin as a means of payment was significantly lower.

Figure 4: 1011 venues on 26th November 2013.



Source: coinmap

Despite its volatility and instability of its exchange rate, the number of venues where it is possible to use your Bitcoin Wallet as a means of payment is steadily growing. It is clear that this is due to the great demand and popularity of Bitcoin, as well as its adaptation and integration into everyday life. Among the biggest companies accepting BTC as a currency today are: Microsoft, Overstock, Virgin Galactic, Tesla, Lionsgate films, Subway, Alza and Big Four's PwC. Nevertheless, some statistics show, that Bitcoin is only accepted at three out of 500 top online merchants. For example, in July 2017, James Faucette – Morgan Stanley payments analyst, claimed, that, quote: "Bitcoin owners are reluctant to use the cryptocurrency given its rate of appreciation, more evidence that bitcoin is more asset than currency, way easier to trade speculatively than convince new merchants to accept the cryptocurrency."

The Bottom Line

Bitcoin represents a lot of opportunities that did not exist before its development. Nevertheless, it has not yet managed to convert investors into its potential adoption rates as an alternative currency. The recent confirmation of the IRS that Bitcoin is an asset for tax purposes has clarified the situation for investors, and the promise of a cost-free transfer offers innovative options for the use of foreign direct investment. In the short term, most of the volatility will depend on the investor's perception of the ability of locks to protect individual holdings and provide a reliable margin of value as the adoption increases.

4.3 *What are futures?*

Futures are financial contracts obligating the buyer to purchase an asset or the seller to sell an asset, such as a physical commodity or a financial instrument, at a predetermined future date and price. Futures contracts detail the quality and quantity of the underlying asset; they are standardized to facilitate trading on a futures exchange. Some futures contracts may call for physical delivery of the asset, while others are settled in cash. To put it in other words, after the completion of the futures contract, both parties must buy and sell at the agreed price, regardless of the actual market price on the date of performance of the contract.

Futures contracts' goal is not necessarily to maximize profits. It is a tool that is often used in financial markets to minimize or avoid the risk of changes concerning the price of an asset, bought and sold on a regular basis. This type of contracts is discussed and traded on the futures exchange, which appears as an intermediary.

Futures are also used in portfolios to balance the oscillations that may occur in investment prices, especially in case of high volatility of an underlying asset.

4.3.1 What are Bitcoin futures?

Futures do not only relate to physical assets, they can also be sold and traded on financial assets. In case of a Bitcoin, the futures contract would be based on its price, and speculators may bet on what they think Bitcoin will be worth in the future. Moreover, this allows investors to speculate on the Bitcoin value, without owning Bitcoin.

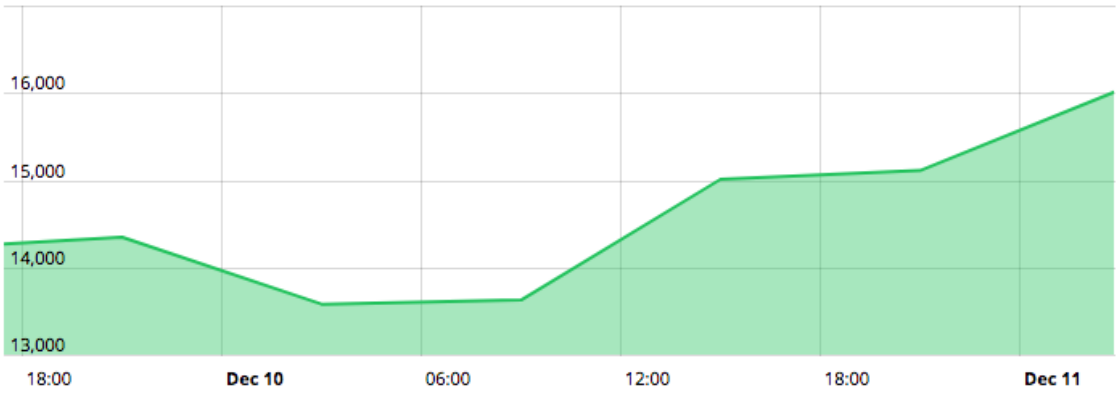
Futures contain two characteristics, fundamentally different from bitcoins:

- Although Bitcoin itself stay unregulated, its futures can be traded on regulated exchanges. This approach can be a green flag for the investors who are concerned about the risks associated with the lack of regulation in the industry.
- Additionally, Bitcoin futures make it possible for investors to continue speculating on BTC price in those areas, where its trade is banned, such as Algeria, Bolivia, Bangladesh, Ecuador, Nepal and Kyrgyzstan.

4.3.2 What do Bitcoin futures mean for the Bitcoin price?

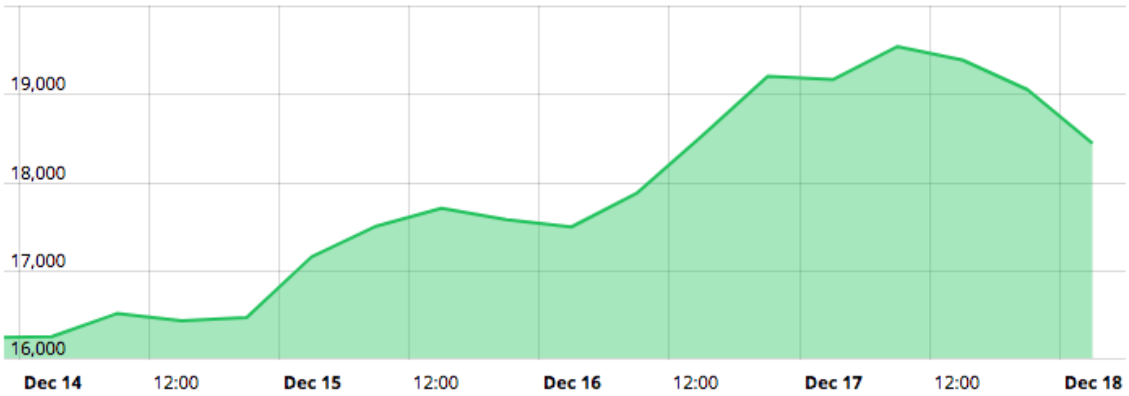
As the general interest in the cryptocurrency is growing, in the short term, futures push BTC value upwards. Let's consider the following example: in December 2017, one day after Bitcoin Futures' first launch at the Chicago Board Options Exchange (CBOE) – a large regulated exchange, the price escalated by almost 10% to $16,936.

Figure 5: BTC price before the futures launch



Furthermore, likewise the first launch, its introduction on one of the world's biggest futures exchanges – CME group (Chicago Mercantile Exchange & Chicago Board of Trade), the price of bitcoins hit a new record high of $20,000.

Figure 6: BTC price after futures launch



Source: coindesk

The long-term impact of the Bitcoin's futures on its value, however, is harder to prognose, but it is likely to continue on boosting its price, as, firstly, being regulated on public exchanges gives more confidence to the potential investors, who were previously in doubts due to the lack of it. Secondly, futures contribute to a higher market liquidity, simplifying the buy, sale, trade mechanism of digital currencies and, therefore, making it much more profitable. Finally, futures have an aim to counterbalance underlying assets' price fluctations, thus, it could lower Bitcoin volatility.

5 Discussion

5.1 *What are the determinants of the Bitcoin price?*

Bitcoin's cost is resolved against fiat cash, for example, Euro (BTCEUR), US Dollar (BTCUSD) or Chinese Yuan (BTCCNY). In this manner it shows up on the exchange market like any other traded symbol. However, it differs from fiat monetary standards, as there is no official cost; just different midpoints considering value bolsters from worldwide trades. Bitcoin Average and CoinDesk are two records detailing the average cost. It's typical for Bitcoin to be exchanged on any single trade at a cost somewhat different to the actual average. What factors determine Bitcoin's price?

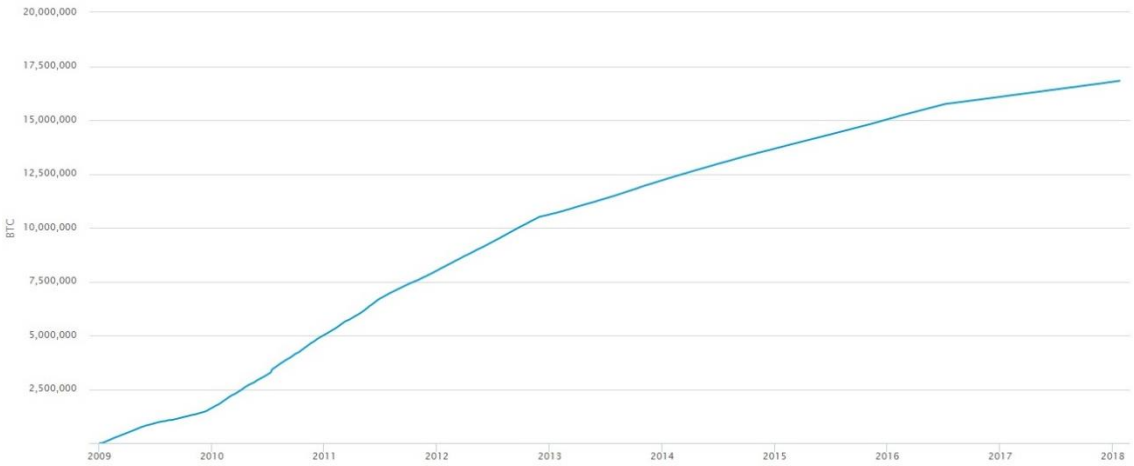
1. Market demand and supply

The primary standard of economics states that if individuals purchase money, its value grows and if it is sold – the value respectively falls. Digital currency is no exception: today, there's no physical equivalent comparable to Bitcoin in the real world, so BTC are traded and sold on exchanges. For instance, as it has already been mentioned in the timeline of Bitcoin's value development, in fall of 2013, its price went up by 10 times as a result of Chinese demand.

2. Total amount of Bitcoins and Bitcoin holders

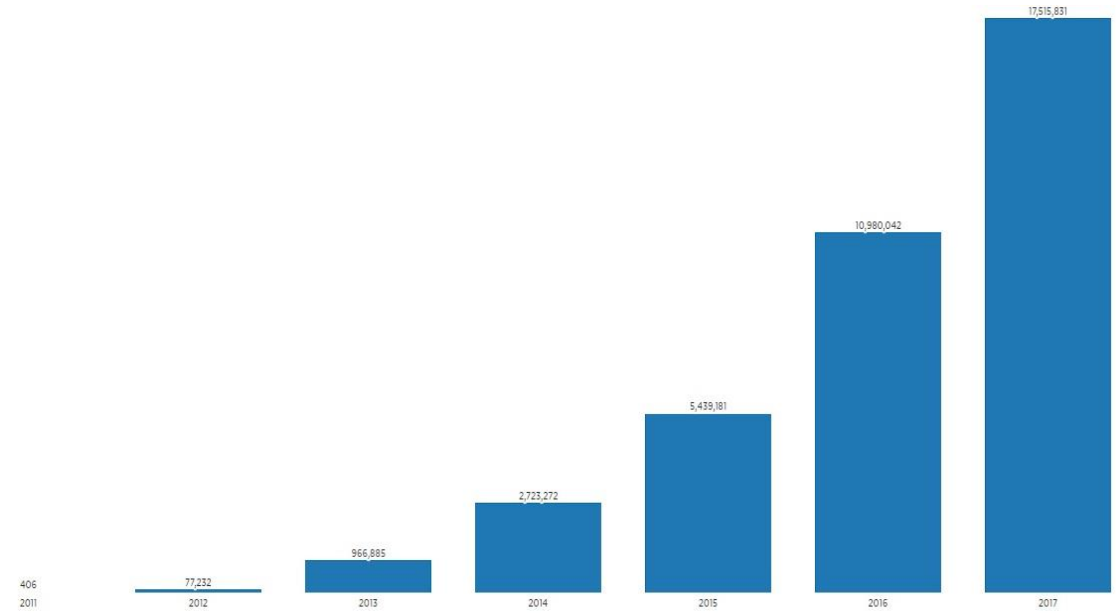
The aggregate sum of Bitcoins is 21 million, yet its production takes time. As of now, there are around 16.8 million BTC and over 17 million individuals possess BTC wallets. This number is developing quickly and since the quantity of Bitcoins is fixed, the cost will keep on rising.

Figure 7: Bitcoin circulation



Source: coinmarketcap

Figure 8: Number of wallets as of Dec 31 each year



Source: coinmarketcap

3. Technical issues

Bitcoin's source code is open for everyone to examine. This concept forces the community to report software design issues, and as long as it is done so, the bitmap value reflects the level of confidence in the design of the protocol as a whole. Paradoxically, this approach to security is able to produce great outcomes, being a number of beneficial open source software overtures, such as Linux. However, BTC can become volatile in either direction when its security vulnerabilities are exposed. New updates for bugs settling and code's weak links can create a driving force for value development. At the same time, the exchange rate can be brought down by successful hacking or server attacks. Let's consider a few examples, regarding Bitcoin price fluctuations throughout its history to prove the weight of this determinant: in April 2014, the OpenSSL vulnerabilities attacked by the Heartbleed bug and reported by Google security's Neel Mehta drove Bitcoin prices down by 10% in a month. Additionally, in August 2016, a few programmers came upon a security issue in Bitfinex and the cost along these lines fell.

4. Mass media and political and economic events worldwide

Human factor and the way individuals may respond to the news included. News and occurrences that might scare potential investors include geopolitical events, as well as government statements that Bitcoin is likely to be regulated. Consider the following examples: Ross Ulbricht's arrest in May 2015 for creating an online black marketplace that would use Bitcoin to avoid law enforcement has resulted into a 25 percent price fall and, by contrary, the anticipation of the Winklevoss' exchange-traded fund (ETF) hearing has brought BTC price to its all-time high as of March 2017. Moreover, the early adopters of Bitcoin included several mal actors among them, who would control the production of the news headlines that would potentially arouse fear among the future investors. Among such news: the bankruptcy of Mt. Gox in early 2014 and that of the South Korean exchange Yapian Youbit. These incidents, along with the public panic, subsequently led to a rapid decline in the cost of Bitcoins compared to a fixed currency. Nevertheless, bitcoin-friendly investors rather viewed these events as a proof of the digital currency's market maturity, maintaining the value of bitcoins versus the dollar shortly after the events took place.

5. *High volatility*

Volatility is a statistical measure of the dispersion of returns for a given security or market index. In other words, it is a degree of trading price variation over time, which refers to the measure of uncertainty or risk in a security's esteem. Higher volatility implies that the value of a security can possibly be spread out over a bigger scope of values, which also signifies that the cost of the security can change drastically over a brief period of time in either direction.

5.2 *Why is Bitcoin's price so volatile?*

As well as its value variances, Bitcoin's volatility on its exchanges is determined by several factors. In terms of traditional markets it is calculated by means of the Volatility Index, also known as the CBOE Volatility Index (VIX). Since as an asset digital currency is still on its early stages, Bitcoin's volatility doesn't yet have a commonly accepted index, it is known, however, that Bitcoin is prone to instability in a relatively short period of time in the form of about 10 times changes in value versus the U.S. dollar

Here are a few of the factors behind Bitcoin's volatility, derived from the analysis of the history of its price fluctuations and determinants:

1. Bitcoin's perceived value fluctuates

One of the reasons for bitcoin fluctuation with respect to fiat currencies is a perceived margin of value compared to the fiat currency. Bitcoin has properties that make it similar gold. It is regulated by the constructive decision of the developers of the basic technology to limit production to a fixed amount – 21 million BTC. Considering this difference from the fiat currency that is administratively governed with an aim to maintain low inflation, high employment and satisfactory growth through investment in capital resources, since an economy constructed using standard currency shows signs of strength or weakness, investors may consider partly allocating their assets into cryptocurrency, Bitcoin in particular, as it's the most known and developed asset of its kind nowadays.

2. *An excess of variance in perceptions of Bitcoin's store of value*

Volatility of BTC is also largely determined by the change in perception of the intrinsic value of the digital currency as a store of value and a method of transferring value. Store value is a function which allows an asset to be useful in the future with some predictability and which can also be saved and exchanged for some good or service in the future. Value transfer method is any object or concept used to transfer possessions in the form of assets between the parties. Today's volatility makes store of value considerably vague, yet it promises an almost invaluable transfer of value. On account of these two factors of Bitcoin's current spot price vary depending on the dollar and other currencies, BTC value can fluctuate based on news events similarly to fiat currency.

3. Little option value to large holders of the currency

The volatility of bitcoins is also based on the holders of large shares of the total number of unrealized currency floats. It is unclear for Bitcoin investors with current reserves over $10 million how they would convert their assets into cash without a severe market shift. As Bitcoin's volume is similar to a small cap stock, the currency did not reach the mass market acceptance rates that are necessary to provide option value to larger currency holders.

4. Bitcoin's high-profile losses at are another driver of volatility

It is worth noting that the mentioned losses and subsequent news about it had doubled its impact on volatility. The total float of Bitcoin has been reduced approximately, creating a potential rise in the number of remaining units due to an increase in deficit. Simultaneously, the redefinition of this elevator was a negative consequence of the subsequent news cycle. It is noteworthy that the mass failure in Mt Gox seemed positive to other Bitcoin gateways in terms of cryptocurrency's long-term prospects, which further convoluted the already complicated history of volatility. Since early manufacturing companies are eliminated from the market due to poor management and dysfunctional processes, later entrants get the chance to learn from their mistakes and build stronger processes in their own operations, by applying the amplification to the infrastructure of the currency as a whole.

5. Bitcoin and foreign direct investment in countries with high inflation

As a currency for developing countries which are presently experiencing high inflation, Bitcoin is beneficial, considering its volatility in these countries compared to volatility in US dollars. Bitcoin is much more volatile in relation to the US dollar than the Argentine peso with high inflation against the US dollar. At the same time, the almost limitless transfer of bitcoins across borders makes it a potentially alluring borrowing tool for Argentines, since the high inflation rate for loans expressed in pesos potentially justifies the adoption of some intermediate risk of currency volatility in a loan expressed in bitcoins financed outside of Argentina. Likewise, funding organizations outside of Argentina under this scheme can receive higher returns than they would get using debt instruments denominated in their national currency, which can offset some of the risk of exposure to a highly profitable Argentinean market.

6. Tax treatment of Bitcoin also affects the volatility

Recent IRS announcements claiming that the currency is in fact an asset for tax purposes has had mixed consequences for volatility. On one hand, any statement of currency recognition has a positive effect on its market valuation. Contrarily, on the other hand, the IRS decision to call this property had two negative effects: firstly, the added complexity for users willing to make payments with it. According to the new tax legislation, users would be obliged to register the market value of the currency during each transaction, no matter how small it would be. Obviously, such measure can delay the adoption, as it seems to be too big of a problem for what it costs for many users. Secondly, a resolution to consider a currency a form of property for tax purposes may be an indication to some shareholders that the IRS is getting ready to apply stricter regulations later. A very strong currency regulation can lead to the fact that the rate of adoption of the currency is slowed down to such an extent that it cannot achieve mass acceptance, which is crucial for its overall utility in society. IRS recent actions are not clear about their signal motives and therefore have mixed signals in the market for bitcoins.

5.3 *Where to invest in 2018?*

Again, the first crypto currency appeared in January 2009. Nine years later, in 2017, virtual currencies are flourishing: while almost every day their capitalization is breaking records, the yield from trading them is tens and hundreds of times higher than the one from Forex, securities and bank deposits. Today, there are over a thousand virtual currencies in total, and their total capitalization exceeds $135 billion, which is more than, for example, Mastercard (121 billion). Simultaneously, only 10 of the most popular digital currencies have a capitalization of at least $1 billion. These account for the biggest amount of their total value and can be called the most promising in terms of returns: due to their popularity it's easy to find the exchanges, where they can be bought and sold. The following list provides 10 of the most popular and promising digital currencies in terms of their capitalization volume. The data is relevant as of March 2018.

5.3.1 Ethereum Classic (abbreviation: ETC)

This currency originated on July 30, 2015 after the division of the Ethereum. A year and a half ago (August 2016) it's value was only $1.84. Today it's worth $36.05. Thus, the price of the Ethereum Classic has increased by 19.59 times in 18 months. Total amount issued: 100.16M ETC.

Figure 9: Ethereum Classic price chart

Source: coinmarketcap

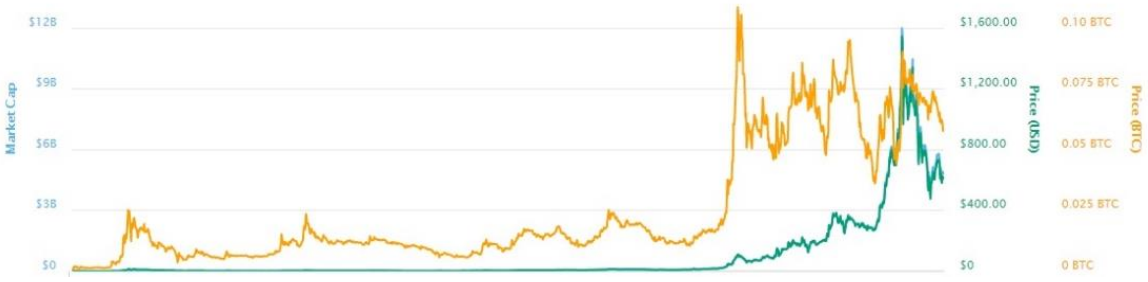
Why to invest in Ethereum Classic:

- Market capitalization: $3.61B;
- Uses core Ethereum concepts;
- Has the ability to create smart contracts as well as decentralized applications;
- Low price per token.

5.3.2 Dash (DASH)

The first issue was on January 18, 2014. It is self-funded and self-governed, moreover, it is the first Sybil proof decentralized organization. A year ago its value was $13.22. It's value today is $614.08. The price has grown by 46.45 times. Total amount issued: 7,91M DASH.

Figure 10: Dash price chart



Source: coinmarketcap

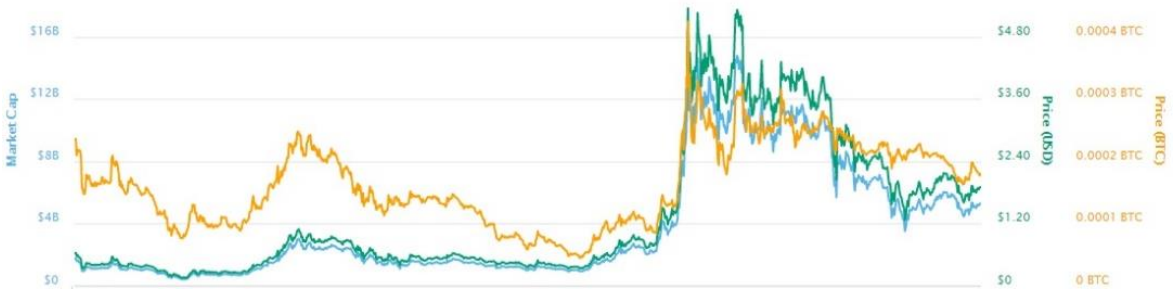
Why to invest in DASH?

- Market capitalization: $4.86B;
- Has a remarkable business structure;
- Fast transactions;
- Unique scalability features;
- User-friendly network.

5.3.3 IOTA (MIOTA)

First issued: June 11, 2016. Eight months ago (earlier data could not be found) the value was $0.62. The rate for today is $1.9. In eight months its value grew 3 times. Total amount issued: 2,78B MIOTA.

Figure 11: IOTA price chart



Source: coinmarketcap

Why to invest in IOTA:

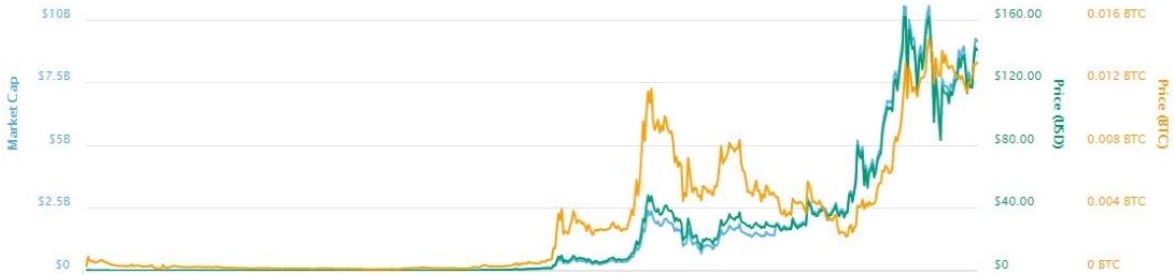
- Market capitalization: $5.27B;
- Low price per token;
- Offline transactions;
- Zero transaction costs;

Has a potential for indefinite scalability.

5.3.4 NEO (NEO)

This Chinese project has its start in 2014 with the original name AntShares, which in August 2017 changed its name to NEO. It is fundamentally similar to Ethereum (decentralized apps, smart contracts) A year and a half ago its value was $0.32. The cost today is $140.06. In 18 months its value increased by 437.5 times, which makes Neo the most profitable and fast growing digital currency in 2017. Total amount issued: 65,000,000 NEO.

Figure 12: NEO price chart



Source: coinmarketcap

Why to invest in NEO:

- Market capitalization: $9.1B;
- The fastest growing cryptocurrency in 2017;

Issues:

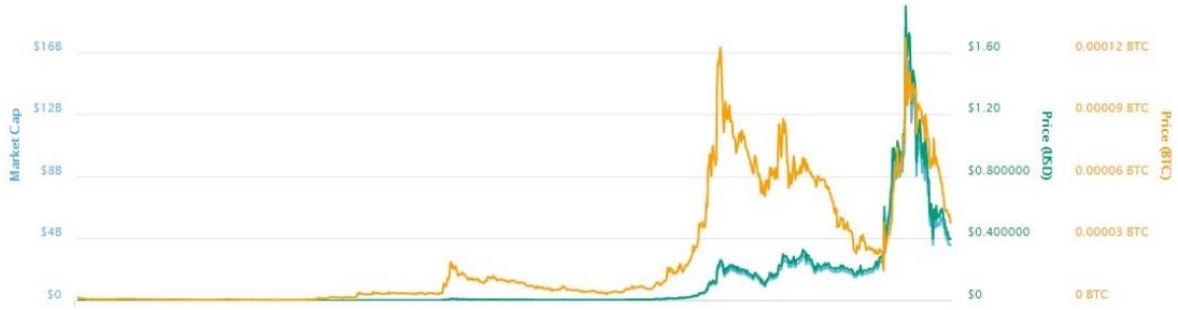
- Suffers in the marketing department;
- Can be difficult to purchase.

5.3.5 NEM (XEM)

The project started on March 31, 2015 in Japan. Developed using Java. Uses a proof of importance instead of generic proof of work algorithm. A year and a half ago the value was

$ 0.007. The cost today is $ 0.399. The price for 12 months increased by 57 times. Total amount issued: 9B XEM.

Figure 13: NEM price chart



Source: coinmarketcap

Why to invest in NEM:

- Market capitalization: $3.6B;
- Uses multisignature accounts;
- Uses encrypted messaging;
- Low price per unit;
- Good for those who want to invest small amounts.

5.3.6 Litecoin (LTC)

Created in 2011 by Charlie Lee – a former Google employee. The first issue took place on October 12, 2011. A year and a half ago the rate was $3.75. The cost today is $217.67. The price has gone up by 58 times. Total amount issued: 55.4M LTC.

Figure 14: Litecoin price chart

Source: coinmarketcap

Why to invest in Litecoin:

- Consistent growth over the years;
- Cheap cost per unit;
- Market capitalization: $12.06B.

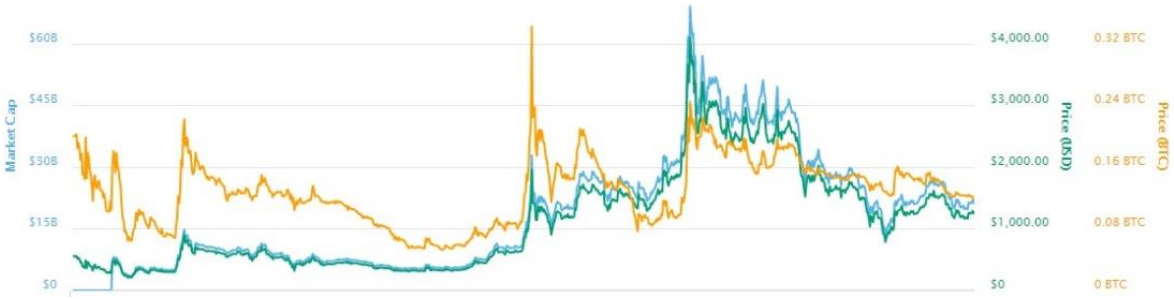
Issues:

- Wastes a lot of resources.

5.3.7 Bitcoin Cash (short for BCH)

This currency appeared as a Bitcoin fork on August 1, 2017. Value half year ago: $309.94, value today: $1.261.6, which means in half year it's cost has increased by 4 times. Total amount issued: 16.99M BCH.

Figure 15: Bitcoin Cash price chart



Source: coinmarketcap

Why to invest in Bitcoin Cash:

- Market capitalization: $21.43B;
- Low and faster transaction fees;

5.3.8 Ripple (XRP)

The project started in 2012. Ripple – extremely different digital currency, when compared to the others, structurally and fundamentally, as it is a distributed open source internet protocol, that supports real-time gross settlements, fast remittance, and currency exchanges. A year and a half ago the price was $ 0.006. The rate for today is $0.955. In 18 months its price has become 159 times bigger. Total amount issued 39.09B XRP.

Figure 16: *Ripple price chart*

Source: coinmarketcap

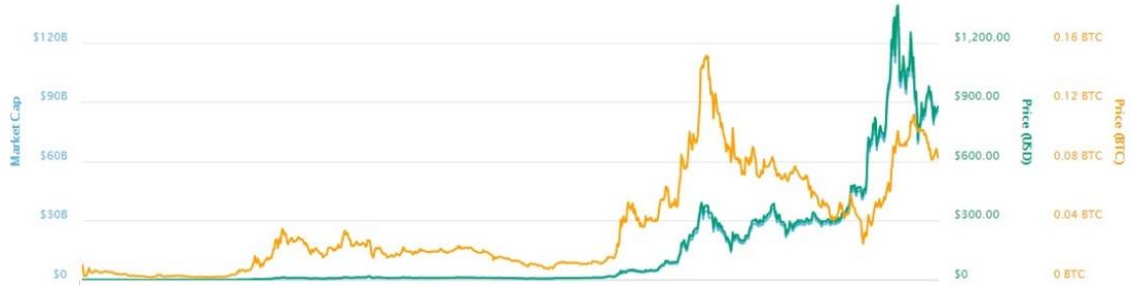
Why to invest in Ripple:

- Market capitalization: $37.37B;
- Extremely low price per token;
- Backed by several banks and corporate bodies (UniCredit, UBS, Axis Bank);
- Faster transactions;
- Fourth most traded cryptocurrency.

5.3.9 Ethereum (ETH)

Created by Vitalik Buterin – a Russian-Canadian programmer – in 2013. First issued: July 30, 2015. One year and a half ago the price was $11.65. The rate for today is $883.19. In 18 months the price went up by 75.8 times. Total amount issued 97.88M ETH.

Figure 17: *Ethereum price chart*



Source: coinmarketcap

Why to invest in Ethereum:

- Relatively low price per unit;
- Market capitalization: *$86.44B;*
- Stable progress over the years;
- Popularity and prompt updates to match new industry standards.

Issues:

- Bugs and loopholes.

5.3.10 Bitcoin (BTC)

First issued: January 3, 2009. A year and a half ago the price per Bitcoin was $586.40. The price today is $10727,9. In 18 months the price has grown by 18 times. Total amount issued: 16.89M BTC. (For Bitcoin price fluctuation graph see CHAPTER 2)

Why invest in Bitcoin?

- Market capitalization: $181.19, which is 49,5% of the total capitalization of the digital currencies;
- Huge popularity;

Issues:

- Much slower, than the altcoins
- Scalability issues
- Mining wastes a lot of power.

6 Conclusion

The spheres of payment transactions and settlement systems has been under the influence of innovation recently, however, the importance and applicability of some of the new technologies, that are being introduced, are debatable from the standpoint of their regulation and practical use. The highest point of the innovative novelty in the area of electronic money are cryptocurrencies: Bitcoin in particular. It is an innovative payment network and a new kind of money. Unlike the traditional currencies it has no physical counterpart, it is not supported by the government or any legal entity and its transactions do not involve any traditional financial institutions. In fact, Bitcoins, similarly to music or a text document, are computer files, that can be destroyed or lost. Choosing digital currency makes a person independent of regulatory financial institutions, banks, law enforcement agencies. The main features of Bitcoin are ensuring the confidentiality of users and anonymity of performed transfers, accelerating the capital funds turnover, significantly reducing the operating costs, which are typically associated with the circulation of paper money, improving the money transfer system, minimizing the impact of inflationary processes, and, finally, simplifying the payment system itself. Absence of the inflation, when it comes to Bitcoin causes the economically active part of the population to deny the traditional currency in favour of the crypto currency. Therefore, Bitcoin as a currency can pose a certain danger to the traditional financial system due to its uncontrollability and unregulated nature in the legal aspect in many countries of the world. Thus, financial institutions are forced to demand the prohibition of its use. At the same time, today Bitcoin is a legal tender in most countries with developed market economies.

What's next?

Although many talk of bitcoin as a bubble, some analysts believe its price could grow by 10 times over the time of coming year. Whether that's a good thing or not is a whole other question. However, at the moment Bitcoin can only be used as a medium of exchange and, until now, the dark economy has profited from it a lot more, than the one involving legal operations. Moreover, due to the absence of any legal authority behind it, Bitcoin becomes resilient to such matters as corruption, censorship and regulation.

To conclude, let's identify three major paths, that Bitcoin and other virtual currencies could possibly take and what outcome it could lead to in the future.

Cryptocurrencies could have an ambitious take-off and become a widely used payment method on a daily basis, being accepted everywhere and facilitating the financial transactions between the parties, regardless the boarders. As a result, a few early investors, similarly to the ones that have been investing in fundamental technologies, such as computers, internet and online platforms in the past, will make a fortune out of it, while the others will have to switch to it without receiving any bonuses in the form of returns. Though, if this 'speculative bubble' bursts, it could have such severe consequences, that could possibly affect the entire sector, making the investors lose their faith in it and dragging them out, bankrupting the miners, who would by this time have spent hundreds thousands, if not millions on single-purpose hardware that requires a high price of a Bitcoin in order to be profitable, and renouncing virtual currencies as a technological dead-end.

Nevertheless, it is possible, that digital currencies won't be facing a major change and things will stay as they are at the moment and as they have been for the past 5 years: its use will stay stable, mostly for the illegal operations, due to the lack of regulation, regardless its market price and high volatility.

7 References

1. Plassaras, Nicholas A. (2013) *Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF*, Chicago Journal of International Law: Vol. 14: No. 1, Article 12.

Available at: http://chicagounbound.uchicago.edu/cjil/vol14/iss1/12

2. Kaplanov, Nikolei M. (2012) *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation.* Publication

Available at: http://www.thebitcoin.fr/wp-content/uploads/2014/01/Nerdy-Money-Bitcoin-the-Private-Digital-Currency-and-the-Case-against-its-Regulation.pdf

3. Bank for International Settlements (2015) *Committee on Payments and Market Infrastructures report on digital currencies.* Publication

Available at: https://www.bis.org/cpmi/publ/d137.pdf

4. www.coinmarketcap.com. (2018) *Cryptocurrency market capitalizations.* [online]

Available at: https://coinmarketcap.com/ [Accessed 2018]

5. www.coinmap.org (2018) Map of Bitcoin accepting venues. [online]

Available at: https://coinmap.org/#/world/54.00454044/9.90966797/4 [Accessed 2018]

6. Nakatomo, Satoshi. (October, 2008) *Bitcoin: A Peer-to-Peer Electronic Cash System.*

Available at: http://bitcoins.info/bitcoin.pdf

7. Campell, Robert.(July 10, 2017) *Bitcoin A to Z – The comple on guide for beginner to buy, sell, invest and trade*.

Available at: http://amazon.com

8. Ron, Dorit and Shamir, Adi. (2013) *Quantitative Analysis of the Full Bitcoin Transaction Graph.*

Available at: https://eprint.iacr.org/2012/584.pdf

9. Rosenfeld, Meni.(November 17,2011) *Analysis of Bitcoin Pooled Mining Reward Systems.*

Available at: https://bitcoil.co.il/poolanalysis.pdf