BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF FOREIGN LANGUAGES
ÚSTAV JAZYKŮ

CRYPTOCURRENCIES
KRYPTOMĚNY

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR — **Anna Šindelářová**
AUTOR PRÁCE

SUPERVISOR — **PhDr. Milan Smutný, Ph.D.**
VEDOUCÍ PRÁCE

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Angličtina v elektrotechnice a informatice**
Ústav jazyků

Studentka: Anna Šindelářová ***ID:*** 173599
Ročník: 3 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Kryptoměny

POKYNY PRO VYPRACOVÁNÍ:

Popište různé druhy měn, jejich fungování a využití. Analyzujte i ekonomické a společenské souvislosti jejich získávání a používání.

DOPORUČENÁ LITERATURA:

Antanoupoulos, A.M. (2014) Mastering Bitcoin. Unlocking Digital Cryptocurrencies. O´Reilly Media.

Narayanan, A. (2016) Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press, 2016.

Termín zadání: 9.2.2018 ***Termín odevzdání:*** 25.5.2018

Vedoucí práce: PhDr. Milan Smutný, Ph.D.
Konzultant: doc. Ing. Václav Zeman, Ph.D.

doc. PhDr. Milena Krhutová, Ph.D.
předseda oborové rady

ABSTRACT

This bachelor thesis focuses on cryptocurrencies. The thesis deals with the creation and development of cryptocurrencies in general, their utilization and description of their basic function principles. Furthermore, three specific cryptocurrencies are described in more details - Bitcoin, Ethereum and Monero. The aim of this thesis is a comparison of these cryptocurrencies, that is done in the last chapter.

KEYWORDS

Cryptocurrency, cryptography, hash function, blockchain, Bitcoin, Ethereum, Monero.

ABSTRAKT

Tato bakalářská práce se zaměřuje na téma Kryptoměny. Práce se zabývá vznikem a vývojem kryptoměn, jejich využitím a popisem jejich základních principů fungování. Více podrobně jsou v této práci popsány 3 vybrané kryptoměny – Bitcoin, Ethereum a Monero. Cílem této práce je provést porovnání těchto vybraných kryptoměn, které je popsáno v poslední kapitole.

KLÍČOVÁ SLOVA

Kryptoměna, kryptografie, hešovací funkce, blockchain, Bitcoin, Ethereum, Monero.

ŠINDELÁŘOVÁ, A. *Kryptoměny*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2018. 50 s. Vedoucí bakalářské práce PhDr. Milan Smutný, Ph.D..

PROHLÁŠENÍ

Prohlašuji, že svoji bakalářskou práci na téma *Kryptoměny* jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu bakalářské práce PhDr. Milanu Smutnému, Ph.D. a odbornému konzultantovi doc. Ing Václavu Zemanovi, Ph.D. za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování mé bakalářské práce.

TABLE OF CONTENTS

INTRODUCTION

Money has been and will continue to be an essential part of our everyday lives. Although its function is still the same, their form has changed over time. From ancient coins, the banknotes were derived and the development of technology has come up with credit cards as well. The latest major shift in the money area is the creation of cryptocurrencies, which started a new era in money development.

Although the first idea of cryptocurrencies was introduced in 1998, only a few people in the world have already heard of this topic. Fortunately, it began to change over the last few years. Cryptocurrencies are no longer just a hobby for programmer enthusiasts, but they are slowly beginning to get into the wider awareness of the world society.

At present, we learn about cryptocurrencies from media and advertising. In most cases, these are reports of investing in cryptocurrencies as well as warning banks not to invest in these currencies, many reports are only about the growth and fall of the Bitcoin price.

Whether we learn about cryptocurrencies in the positive or negative way, they are starting to influence society in the whole world. This is important because cryptocurrencies can be a very dangerous financial product in ignorance of all its contexts.

On the other hand, cryptocurrencies are considered a very popular investment product not only for raising capital but mainly for short-term or long-term investments that are very profitable despite the high risk. The aim of this thesis is to summarise the information about cryptocurrencies and make a basic comparison of the individual cryptocurrencies described.

This bachelor thesis is divided into three parts. The first part is a research of literature focused on the description of cryptocurrencies. This part contains general information about cryptocurrencies, their history, the basic principles of their functioning, storage and acquirement. This is followed by the description of Bitcoin, Ethereum and Monero, their history, technical and economic parameters, storage and use in the real world.

In the second part, the bachelor thesis deals with comparison of the cryptocurrencies described from different points of view. Its purpose is to find out which cryptocurrency is more suitable in particular fields.

1 CRYPTOCURRENCY

A cryptocurrency (also digital currency or electronic money) is a virtual currency that works on a basis of cryptography. Due to cryptographic encryption, cryptocurrencies are anonymous as well as worldwide and borderless [1, p.47, 50].

Only a few decades ago, using a check or a credit card was charged by high transaction fees even for small transaction values, so called micropayments. This was the main reason to create new payment system, which will differ from the traditional ones [2]. The main differences between fiat currencies and cryptocurrencies are *decentralization*, *open-source software* and *peer-to-peer network*.

In contrast to fiat currencies, the cryptocurrencies are not controlled by one person or one central organization like the central bank. They are decentralized, which in practice means that only their users determine what the cryptocurrencies will become in the future and how they will evolve. The transactions within this decentralized network occur directly from one user to the other without third party supervision.

Furthermore, the cryptocurrency's software is an open-source software. The source code is publicly available and each user can, with some basic knowledge, make changes in it to improve cryptocurrency's performance.

This principle is the basis of peer-to-peer (P2P) network when all computers, in other words *network nodes*, are interconnected and communicate with other nodes without any central node - *server*. In this kind of network, all users are equal, everyone has the same competences as the others [3, p.139]. Its advantage is the growing transmission capacity of the network with the growing number of users. On the other hand, starting the initial communication can be difficult [4, p.24].

Because of this peer-to-peer network environment, the cryptocurrencies are much more anonymous than fiat currencies hence it is more difficult to identify their users, the wallet owner or a sender as well as a recipient of a transaction. Considering this fact, the cryptocurrencies are often perceived as something illegal, because they could be used for money laundering and tax evasion, and they are associated with the black market.

Nevertheless, the cryptocurrencies have started to reach the wider public awareness due to the media and the very fast growing Bitcoin price in the last few months. Nowadays, it also becomes a risky but very profitable investment product.

1.1 History of cryptocurrencies

The first idea to create a virtual currency was published in 1998 by American cryptographer Nick Szabo. It was called Bit Gold and it was only a theoretical description of the cryptocurrencies [5].

The Szabo's idea and his scheme of Bit Gold was a basis for creation of Bitcoin, the first real-world cryptocurrency and nowadays the most popular and the most used virtual currency. In most cases, Bitcoin is also the starting point for the creation of other cryptocurrencies. Bitcoin was created by unknown person under the pseudonym Satoshi Nakamoto, but it is generally assumed that the entire group of programmers is hidden under this nickname.

Gradually, other cryptocurrencies were created, many of them were based on Bitcoin, but there are also cryptocurrencies that are more or less different from Bitcoin. The difference can be, for example, the potential number of mined coins, the height of anonymity or the speed of confirmation. At the beginning of 2015, there were around 500 alternative coins to Bitcoin, so-called altcoins. Currently, more than 1,500 cryptocurrencies exist in the world. Although some cryptocurrencies disappear, their total number is steadily increasing [6].

1.2 Cryptography

Cryptography is one of the two main mathematical disciplines of Cryptology. It deals with encryption methods that are used for enciphering transactions with special encryption keys [7].

Firstly, any type of a message in cryptocurrency network must be encrypted by cryptographic algorithm from the form of plain text to the form of encrypted text. There are two types of encryption: *a symmetric encryption* and *an asymmetric encryption*.

The symmetric encryption system uses two keys – encryption key and decryption key. Both keys must always remain secret, because the encryption key can be easily derived from the decryption key. In these systems, it is common for both keys to be the same, thus symmetric systems are sometimes referred to as single-key systems.

The asymmetric system, as well as the symmetric system, uses the encryption and decryption key. Unlike the keys in the symmetric system, it is not possible to derive the encryption key from the decryption one. For this reason, it is enough to conceal only the decryption key, called a private key, and the encryption key may be publicly available. Therefore, it is designated as a public key [8, p.17].

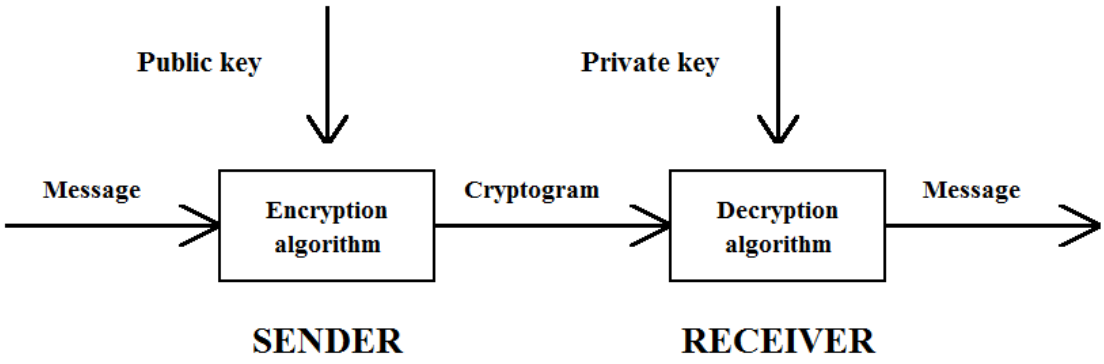


Fig. 1: Principle of the asymmetric encryption system
Source: [8, p.15]

1.2.1 Private Key

The private key is the decryption key used to sign transactions, which the key owner performs, with so called *digital signature*. This key is specific and unique for each network user and must be safely and secretly stored in the cryptocurrency wallet [4, p.90].

1.2.2 Public Key

The public key is, as its name implies, public and freely accessible. It is used for encryption of messages in network for which it is valid and also for verification of the user's digital signatures [4, p.92].

1.2.3 Hash function

Another important term for cryptocurrency functioning is *a hash function*. This function transforms a set of characters of any length to a set of characters of fixed length. The output of this function is called *hash*. Nevertheless, this must be only a one way process, it means that there cannot be an inverse algorithm that would detect the original text from the hash. Of course, each hash needs to be original. In one moment, one hash cannot be the same for two different encrypted strings.

Various hash functions, such as SHA-256 (Secure Hash Algorithm), are used in cryptocurrencies. These hash functions differ from each other by the length of the output hash, because the input number of characters is not crucial. Specifically for the SHA-256 algorithm, the resulting hash consists of 256 bits [7].

The unit of this function is the number of hashes created per second – h/s. This unit indicates the computing power not only for the entire network, but also for each particular node. The computational power of cryptocurrency's networks is often very large sized, therefore derived quantities such as kilohash, megahash, gigahash, terahash and other are frequently used [4, p.85].

1.3 Transaction

In general, the transaction says how many coins of the given cryptocurrency are transferred from one address to the other within a network. As described in Chapter 1.2, each transaction is signed by the private key of the address user [4, p.45].

To include the transaction in the Blockchain and thus to consider it as executed, it is always necessary to pay a transaction fee. The transaction performing speed depends on the amount of the transaction fee. Therefore, preferences have the highest transaction fees. If the fee is too low or in not at all, it may happen that the transaction will never be executed and will remain in the *mempool*, which is a virtual space where all transactions are waiting for confirmation.

To eliminate this risk, some wallets calculate the amount of transaction fee automatically, but usually, it is possible to set any amount of the fee. Because the cryptocurrency networks are decentralized and there is no central organization that

would collect the fees, the transaction fees will be obtained by the one who first mines the block, so called *miner* [4, p.70, 136].

The transaction is deemed to be confirmed once it is included in the Blockchain. The number of confirmations is the number of blocks between the currently mined and the one in which the transaction is included. The more blocks it is, the more unchangeable the transaction is, because to change or modify the transaction, it would be mandatory to recalculate all the blocks that followed the one with the modified transaction and it would be extremely difficult for computing power.

For some cryptocurrencies, there is a special generating transaction in each block. Due to this transaction, new cryptocurrency coins in the network are created. The amount of newly created coins is different in each cryptocurrency network and often changes over time [4, p.83, 87].

1.4 Transaction Blockchain

For most cryptocurrencies, the basis for the execution of transactions is the Blockchain. The Blockchain can be considered as a decentralized publicly available accounting book, in which all the transactions, which have been implemented in the network since its inception, have been recorded.

The basic blockchain unit is one block. Blocks are chronologically written into the Blockchain exactly in the way they were created. Each block contains confirmed transactions, a generating transaction and the hash of the previous block. Each block can always be assigned with a precedent block (except for the first generated block). Thus, this block order is prevented from being switched, modified or deleted.

Transactions are gradually written to these blocks and once this block is completed, at the same time it will be written permanently into the Blockchain as well as a new block will be generated. This principle can be continued indefinitely, the blocks have unlimited number and an infinite number of blocks in the Blockchain can be enlisted.

The time interval depends on the computational power difficulty that is required to find a valid block. This method is sometimes referred to as "proof-of-work" (some cryptocurrencies use a "proof-of-stake" concept).

The time interval, which is calculated from the creation of one block to the creation of the next block, is usually different for each type of cryptocurrency. It always depends on the hashing algorithm used by the specific cryptocurrency.

For the reason that the cryptocurrencies are decentralized, the Blockchain is not only placed on a single network place that can be very easily attacked by hackers. Its copy exists in all nodes of the entire software network, strictly speaking, every user, who has a full-featured software wallet on his device installed, stores the longest string of Blockchain blocks [4, p.28].

1.4.1 Fork

Fork is a special situation that occurs in the Blockchain when more blocks are ranked for one block. In other words, multiple different blocks contain the same hash of one previous block. There are two types of fork – *softfork* and *hardfork* [4, p.24].

Softfork means that newly created blocks with transactions included in them are valid under new rules as well as old rules of the protocol. The opposite is a *hardfork* when newly created blocks with transactions included in them are valid only under new rules of the protocol and no longer under old rules.

An example of the situation where the hardfork can be used is a *split*, which means to separate a new Blockchain and create new cryptocurrency permanently. For illustration, split occurred in Bytecoin Blockchain and cryptocurrency Monero was created [4, p.126, 127].

1.5 Mining and miners

Miners are a very important part of the cryptocurrency's functioning. Their job is to collect and verify transactions in one block. After the block is written into the Blockchain, they create new copies of the Blockchain history. This process, which is called mining, requires a huge computing power for finding the new block, respectively the right amount of nonce (number only used once). This number must be selected in that way that the hash of a new block must be smaller than the target value in the Blockchain.

Everyone can engage in the mining process, but only the one that first solves the computational task of the block will receive a predetermined reward in the form of several newly created cryptocurrency coins, which are often worth several thousand dollars [9].

Compared to that, the almost negligible amount, that miners can obtain, is transaction fees that users pay for the entered transactions. Every user can choose any amount of a transaction fee, certainly there is the theoretical possibility of making a transaction free of charge. However, the rate of charge also depends on the speed of the transaction, because miners usually prefer to verify the transactions with the highest fees first, even if the transaction without a charge was been entered earlier. In the course of time, they move towards smaller and smaller charges, and theoretically it would be possible for them to get to the no-charge transactions. Unfortunately, this does not happen in practice [10].

1.6 Acquirement

As described in Chapter 1.5, cryptocurrency coins can be obtained by mining. For a regular user, this would be a very expensive process and therefore it is easier to buy them. There are plenty of options for buying cryptocurrencies. These options could be divided into two categories - *intermediary companies* and *cash dispensers*.

Stock exchanges belong to intermediary companies. The well-known stock exchanges are for example *Coinbase*, the largest cryptocurrency exchange in the USA. Other stock exchanges include *Plus 500, AvaTrade*, or *eToro*, but the cryptocurrencies in these exchanges are not the major part of their trading. Most exchanges deal with the trading of the most famous cryptocurrencies, therefore it is necessary to include online exchange offices of the individual cryptocurrencies. These servers differ from each other primarily by the *spread*, which is the difference between the buying and selling price. Further, the differences can be found in terms of registration or purchase fees. For their simplicity and the widespread of these servers, this is the easiest way how to get cryptocurrency.

Nowadays, the cash dispensers exist mostly for the best-known Bitcoin, which has so far the most widespread network of these machines. Obviously, the cash dispensers of other cryptocurrencies, such as Litecoin, Dash, or Dogecoin, are slowly starting to emerge [11].

1.7 Storage

Every user who wants to own and store cryptocurrencies must have a wallet. A wallet is a software, that is primarily used for sending and receiving transactions, storage of transaction history and displaying the wallet balance. In addition to this, its purpose is to store and manage private keys of wallet's owner safely [4, p.43].

Each wallet has its own unique wallet address as well as a bank account has its bank account number. The private key of the user is stored in the wallet which will automatically use this key as the user's digital signature when sending the transaction.

While trading on a stock exchange, it is possible that all funds can remain in the exchange account, so the user does not need the wallet if he does not want to make transactions on the network of the specific cryptocurrency. However, this is the least safe option to store cryptocurrencies. The stock market could be attacked by hackers and a lot of users could lose all their funds, as it happened several times in the past. Therefore, it is highly recommended to leave in the stock exchange account only funds that the user wants to trade in the near future and the rest of the cryptocurrencies safely hide in the wallets.

There are 3 basic types of cryptocurrency wallets: *hardware wallets*, *software wallets* and *paper wallets*.

1.7.1 Hardware wallets

Hardware wallets are considered to be the safest way how to store cryptocurrencies. That is also the reason why they are often sold out in stores. Although transactions are online, the financial funds and the private key are stored on offline hardware devices similar to USB. For this reason, they are suitable for the long-term and safe storage of a large amount of financial resources, which the user does not want

to manipulate with. Their only disadvantage is that their interface is not as intuitive as software wallets and this could be a big problem for some beginners.

1.7.2 Software wallets

Software wallets can be divided into *online (web) wallets*, *mobile wallets* and *desktop wallets*. These wallets differ only in the type of device on which they are installed [12].

Online or web wallets, as the name suggests, are on the internet, that means they are accessible at any time from any device with a web browser. These wallets are, similarly to stock exchanges, very prone to hacker attacks or theft, because the private key stored in them is online. Therefore, it is advisable to store only a small number of cryptocurrencies there because the information about these wallets is stored on a third party server.

The mobile wallet works as an application installed on the user's mobile phone. This makes it particularly suited to payments in the stores. As well as in online wallets, it is better to keep only a small amount of money in the mobile wallets because mobile phones are susceptible to malware and viruses.

A desktop wallet is one of the forms of safe cryptocurrency storage. It is a software application installed on a computer or notebook and it is only accessible from this device. Of course, if the device connects to the Internet, there is still a risk that it may be infected with a virus or malware and the user could lose all of the cryptocurrencies stored.

1.7.3 Paper wallets

Paper wallets are considered a predecessor of hardware wallets. They are also very secure, but unlike hardware wallets, they are very easy to use. The specific software is used to create this wallet, which generates a pair of keys that the user prints. Each paper wallet has its own address through which transactions are made from the user's software wallet or vice versa to the user's wallet [13].

2 INDIVIDUAL CRYPTOCURRENCIES

2.1 BITCOIN (BTC)

Bitcoin (BTC) is a decentralized open-source cryptocurrency that operates on the peer-to-peer Bitcoin platform. It is the most common and well-known cryptocurrency and it is also considered to be the basis of a large part of the cryptocurrencies derived from it.

Fig. 2: Logo of Bitcoin
Source: [14]

In Tables 1 and 2, there are listed important technical and economical parameters of Bitcoin. These specifications will be used to compare Bitcoin with other cryptocurrencies in the last chapter.

Platform	Bitcoin
Hash Rate	30.117 EH/s
Difficulty	4,143,878,474,754
Mining profitability	0.5416 USD/Day for 1 TH/s
Blockchain Size	197.50 GB
Block Time	9m 32s
Blocks per Hour	6
Transactions per Hour	8,745

Table 1: Technical parameters of Bitcoin
Adapted from: [15] [cit. 2018-05-15]

Total Bitcoins	17,022,335
Market Capitalization	145,210,167,776 USD
Bitcoin Current Price	8,530.57 USD
Bitcoin Max Price	19,392.4 USD
Static Reward per Block	12.50 BTC
Average Transaction Fee	1.45 USD

Table 2: Economic indicators of Bitcoin
Adapted from: [15] [cit. 2018-05-15]

2.1.1 The History of Bitcoin

In 2007, the first Bitcoin concept was formulated. The programmer or a group of programmers worked on it under the pseudonym Satoshi Nakamoto. In August 2008, the *Bitcoin.org* domain was registered anonymously, and in October 2008, The White Paper, which describes the basic principles of the Bitcoin platform, was published.

In January 2009, the first Block (Block 0) was created, sometimes nicknamed "Genesis Block". A week later, the first Bitcoin transaction was made, specifically in Block 170, between Satoshi Nakamoto and cryptographic activist Hall Finney.

Later in 2009, it was calculated that one dollar has the value of 1,309 BTC. As a result, the first Bitcoin exchange called *The Bitcoin Market* was established in February 2010.

Bitcoin's first real-world transaction took place on 22nd May, 2010. Florida programmer Laszlo Hanyecz paid for 2 pizzas 10,000 BTC, which at the time was about $41. According to today's rate, the value of these two pizzas would reach an unbelievable 114,680,000 USD. Therefore, the Bitcoin Pizza day is celebrated each year on 22nd May in memory of Hanyecz's transaction [16].

Bitcoin was attacked by hackers in August 2010 and a huge number of Bitcoin coins were generated. This resulted in a significant reduction in the Bitcoin price. Despite this fact, at the end of 2010, all mined coins in circulation had worth 1 million USD [17].

In spite of other inconveniences, such as various hacker attacks, Bitcoin theft or the prohibition of Bitcoins in China, Bitcoin's price is fluctuating but still rising. Bitcoin had its most significant price shift in the past year. At the beginning of 2017, its value was 1,000 USD per one Bitcoin, in the middle of August 2017, the value of one Bitcoin was quantified at 4,000 USD, and on November 29, 2017, the price has risen to 10,000 USD, which was considered as another milestone in Bitcoin history, but later the same year, Bitcoin reached its maximum price of 19,392.4 USD.

2.1.2 Wallets

For instance, hardware wallets for Bitcoin are *Ledger Nano S* or *Digital Bitbox*. The first hardware wallet for Bitcoin was *TREZOR* made by Czech company SatoshiLabs [18, 19].

Desktop wallets are for example *Electrum*, *Bither* and *Bitcoin Core*. All of these are designed for Windows, Mac and Linux. Mobile wallets, which are designed for Android, iOS and Windows phones, are *ArcBit*, *Coin.Space* or *Green Address*. Two last mentioned wallets are also designed as the web wallets [20].

Paper wallets can be printed directly by the user. He only needs paper and printer to print the public key and private key together. It is possible to use help with formatting and printing on special websites, that focus on Bitcoin paper wallets, for example *https://bitcoinpaperwallet.com/* [21].

2.1.3 Utilization

There are several ways where Bitcoin can be used. The most popular use is to pay with Bitcoin in restaurants, just by having a phone software wallet installed on the user’s mobile phone. There are almost 100 restaurants in Prague and around 20 businesses in Brno and its surroundings, which allow payments in Bitcoin currency. Of course, it is possible to pay by Bitcoin for example at the hairdresser's, in grocery stores or shops. From April 2016, Bitcoins can also be bought or sold in the Czech Republic through the *GECO* tobacco shops.

Bitcoins can also be used for paying travel costs. At the *CheapAir.com* website, Bitcoins can be spent on plane tickets, at *Expedia.com*, it is feasible to use Bitcoin currency for booking a hotel.

Another possible use for Bitcoins is a payment at internet e-shops. A very wide offer of various goods for Bitcoins is provided by the *Overstock.com* e-shop, where the goods can be shipped to the Czech Republic [22]. In the Czech Republic, it is possible to pay by Bitcoins from May 2017 at the *Alza.cz* e-store using the *BitcoinPay* payment system [23]. Since the end of 2014, Microsoft has been offering video games or other applications for Bitcoins in its Windows Store [24].

Besides already mentioned, there is another interesting utilization of Bitcoin. It can be used to donate a foundation or charity. This is mainly due to the fact that Bitcoin, like all other cryptocurrencies, is anonymous, so the donor's anonymity is preserved when donating any amount. Bitcoin payments are supported, for example, by *UNICEF* or the *Human Rights Foundation* [25, 26].

2.2 ETHEREUM (ETH)

Ethereum is a decentralized software platform that runs on smart contracts. These are decentralized applications that are programmed to work on their own without a risk of failure or without third party intervention. These applications are based on a distributed blockchain database. The Ethereum platform is supported by the Ether cryptocurrency, which are necessary for its operation [27].

Fig. 3: Logo of Ethereum
Source: [28]

In Tables 3 and 4, there are listed important technical and economical parameters of Ethereum. These specifications will be used to compare Ethereum with other cryptocurrencies in the last chapter.

Platform	Ethereum
Hash Rate	265.853 TH/s
Difficulty	3.267 P
Mining profitability	0.0562 USD/Day for 1 MH/s
Blockchain Size	554.67 GB
Block Time	15.3s
Blocks per Hour	236
Transactions per Hour	32,379

Table 3: Technical parameters of Ethereum
Adapted from: [29] [cit. 2018-05-15]

Total Ethereum	99,456,497
Market Capitalization	70,930,678,159 USD
Ethereum Current Price	713.59 USD
Ethereum Max Price	1,389.18 USD
Static Reward per Block	3 ETH
Average Transaction Fee	0.616 USD

Table 4: Economic indicators of Ethereum
Adapted from: [29] [cit. 2018-05-15]

2.2.1 The History of Ethereum

In 2013, the Russian-Canadian programmer Vitalik Buterin described the operation of the Ethereum platform and outlined the conception of the technical protocol and smart contract architecture. Only one year later, he officially introduced this platform to the public at *The North American Bitcoin Conference* in the USA.

In the middle of 2014, the *Ethereum Foundation* was established to finance the further development of this platform. Ethereum Foundation has launched a very successful sale of Ether tokens, for which investors paid 31,591 Bitcoins. It was more than 18.5 million USD and investors obtained over 60 million Ethers [30].

Due to this success, in March 2016, the Ethereum platform was improved. Unfortunately, in June 2016, this platform was attacked by unknown hackers and over 31 million USD were stolen from Ethereum wallets in the Ether cryptocurrency [31].

Despite the fact that developers tried to save the stolen Ether tokens, they did not succeed and it resulted in the division of the network into two groups: *Ether* (ETH) and a new continuation of the existing platform *Ethereum Classic* (ETC). However, Ethereum Foundation has completely distanced itself from the new Ethereum Classic cryptocurrency [32].

2.2.2 Wallets

Many wallets used for Bitcoin storage can also be used for storage other cryptocurrencies. The examples are already mentioned hardware wallets *Ledger Nano S* or *TREZOR*. These wallets are used not only for Bitcoin or Ethereum storage, but also for other altcoins, such as Litecoin or Dash. *KeepKey* wallet is another hardware wallet that can be used for Ethereum.

Software wallets are as well as hardware wallets for more altcoins, not only for Ethereum. As a desktop wallet, *Exodus* can be used. It is the designed desktop wallet for more cryptocurrencies. *MetaMask* can be used as an alternative desktop wallet, which enabled its user basic features like sending and receiving transactions. Moreover, it also supports the use of Ethereum decentralized applications. For mobile phones, application *Jexx* is available to download for Android as well as iOS. *MyEtherWallet* is an example of very safe web wallet [33].

The Ethereum paper wallet can be created by using *MyEtherWallet* webside. The creation is very simple. Only the new unique password to secure the private key in this wallet will be needed [34].

2.2.3 Utilization

Ether as a cryptocurrency has only one use - to be a fuel for the Ethereum platform that would not work without it. However, the Ethereum platform offers many opportunities for use, mainly due to smart contracts, in other words, decentralized applications or dapps.

One of these dapps is *WeiFund*. This is a crowfounding application, such as *KickStarter* or *GoFundMe*, when a target for a financial fund is selected and in some of cases it is also submitted. The difference between *WeiFund* and *KickStarter* is that *WeiFund* does not charge any fees and that the target is collected in the Ether cryptocurrency.

Another application that runs on the Ethereum platform is *Eth-Tweet*. As the name suggests, it is an application similar to *Twitter*, but it is not controlled by any central organization. *Eth-Tweet* allows users to send messages up to 160 characters and due to the decentralization of the application, only the author of this message determines whether the message will be deleted or not.

The *Vevue* project, which works on the Ethereum platform, aims to improve *Google Street View*. The project encourages users to make 30-second videos and share them with others. For this sharing, they could be rewarded with the Vevue tokens or Bitcoin cryptocurrency. This is not happening yet, but applications based on the Vevue project, such as *Make Videos, Earn Bitcoin*, which is constantly improving, can be downloaded from the *Google Play Store*.

4G Capital, which collects cryptocurrency to finance small businesses, is a very interesting project. So far, this support is only for businesses in Kenya, but in the future, it should be extended to the whole Africa [35].

There is a large number of applications already working on the Ethereum platform, many of them are still in the development process and some of them, although technically feasible, will never be put into reality. Such an unrealistic application could be, for example, an organization of elections or a transfer of financial markets to a blockchain [36].

2.3 MONERO (XMR)

Monero is an open-source, decentralized and proof-of-work cryptocurrency working on the CryptoNote protocol. All transactions in this protocol are private, secure and anonymous. Impossibility to detect the sender, the recipient and how much money was sent is considered as the main advantage of this cryptocurrency [37].

Fig. 4: Logo of Monero
Source: [38]

In Tables 5 and 6, there are listed important technical and economical parameters of Monero. These specifications will be used to compare Monero with other cryptocurrencies in the last chapter.

Platform	CryptoNote
Hash Rate	463.292 MH/s
Difficulty	54.386 G
Mining profitability	1.5195 USD/Day for 1 KH/s
Blockchain Size	49.75 GB
Block Time	1m 56s
Blocks per Hour	31
Transactions per Hour	224

Table 5: Technical parameters of Monero
Adapted from: [39] [cit. 2018-05-15]

Total Moneros	16,034,312
Market Capitalization	3,293,539,433 USD
Monero Current Price	205.41 USD
Monero Max Price	471.89 USD
Static Reward per Block	4.6 XMR
Average Transaction Fee	1.59 USD

Table 6: Economic indicators of Monero
Adapted from: [39] [cit. 2018-05-15]

2.3.1 The History of Monero

As mentioned before, Monero is based on the CryptoNote protocol. Nicolas van Saberhagen is the pseudonym of an unknown author who described the working principles of this protocol. The first version of CryptoNote protocol was published in December 2012, the second one was introduced in October 2013 [40, 41].

The first cryptocurrency which worked on this protocol was *Bytecoin*. Its creator is anonymous, as well as the exact date of its origin. Bytecoin became more popular after the creation of Bytecoin thread in the *Bitcointalk* community, hence it is assumed that Bytecoin was created about this time. Unfortunately, cryptocommunity do not trust in this project, because more than 80% of all Bytecoins were mined. No one knew who mined them and owned them, thus there was a risk of rule violation of decentralized cryptocurrency system.

Thanks to the users of the Bitcointalk community, Bytecoin was divided by hardfork on 18th April, 2014. The newly created currency was called *BitMonero*, but only two weeks later, it was renamed to simply Monero. This currency was almost the same as Bytecoin, only some technical mistakes were removed.

At the beginning of the year 2017, Monero's anonymity increased with new function called *Ring Confidential Transactions*. It means that the transaction value can be known only by the sender and the recipient. This function was firstly optional, however, 95% of transactions used this function, so it was installed in each transaction automatically [42].

2.3.2 Wallets

Monero hardware wallet is not available now. One hardware wallet is being developed by Monero community, but it will take some time to create the final product.

One of the Monero desktop wallets is the *MyMonero* wallet developed by *Monero Core Team*. Monero's mobile wallets are available for phones with Android operating system or iOS. These are *Monerujo* available in *Google Play Store* and *CakeWallet* downloadable on *App Store*.

Monero paper wallet can be generated by *Monero offline wallet generator*, available on *MoneroAdress.org*. The principle of generating and printing the wallet is very simple and easy. This generator enables to create a new wallet even on devices without connection to the network [43].

2.3.3 Utilization

Monero can be used as well as Bitcoin in many stores. Moreover, it is possible to pay by Monero in shops that accepts only Bitcoin. It is necessary to use special exchange *XMT.to* to convert Monero to Bitcoin which is then send to the seller. This exchange retains full anonymity of sender or customer, so it is very popular.

Thanks to *XMT.to*, a luxury apartment in Thailand can be bought via *Azur Samui.com*. Another way how to spend Monero is a gambling cryptocurrency site *CryptoGames*, which allows spending not only Monero, but also Bitcoin, Ethereum and other cryptocurrencies. On *TheBigCoin.io*, there are 50,000 retailers that offer you to pay by Monero, as well as Bitcoin, Ethereum, Dash or Litecoin [44].

With Monero, a gift card to different shops, such as *Starbucks* or *Tesco* can be bought. Unfortunately, it works only for few countries, for example Austria, Germany, Italy, Sweden or United Kingdom. This service is not available in the Czech Republic yet [45].

It is often assumed that this cryptocurrency is also used for black market transactions due to its anonymity and impossibility to detect the end-users. For this reason, it cannot be verified whether it is true or not.

3 COMPARISON

In this chapter, the Bitcoin, Ethereum and Monero cryptocurrencies, which were described in the previous chapter, are compared. This comparison is made from different points of view.

3.1 Blocks

The blocks are the basis for the function of the cryptocurrency's Blockchain. Not only the Blockchain size, but also the number of blocks contained in the Blockchain, is different in all cryptocurrencies compared.

	Blockchain size	Number of blocks
Bitcoin	197.5 GB	≈ 520,000
Ethereum	554.67 GB	≈ 5,600,000
Monero	49.75 GB	≈ 1,500,000

Table 7: Blockchain size and number of blocks contained in the Blockchain
Adapted from: [15, 29, 39] [cit. 2018-05-15]

It might appear that Bitcoin has the biggest Blockchain size with the highest number of blocks because it is the first cryptocurrency in the world and it is considered the most popular and famous one. However, as can be seen in Table 7, Ethereum has the biggest size of the Blockchain with the value of 554.67 GB. The Ethereum Blockchain includes approximately 5,600,000 blocks, which is a significant difference from Bitcoin or Monero. Bitcoin Blockchain has the smallest number of included blocks, although its size is bigger than the Blockchain size of Monero. This is due to the fact, that each cryptocurrency works on a different protocol and each of these protocols has different technical parameters.

One of these parameters is the time for which one block is mined. It is possible to mine one block in the Bitcoin network in 9 minutes and 32 seconds, which makes it the slowest time of the cryptocurrencies compared. In the Monero network, the block is mined in 1 minute and 56 seconds and in the Ethereum network, the time of mining one block is in just 15.3 seconds. This means that within one hour, only 6 blocks can

be mined in the Bitcoin network, 31 blocks in the Monero network and 233 blocks in the Ethereum network. This block time and the number of blocks per hour indicate the speed of confirming the transaction on these networks. Therefore, if a sufficient transaction fee is set and this transaction is included in the nearest mined block, the fastest payments are done in the Ethereum network.

The evidence is also the number of transaction included in the Blockchain within one hour. The shorter the time taken to mine one block, the more transactions can be made in one hour. The highest number of transactions made in one hour has Ethereum due to the very fast transaction inclusion to the Blockchain. On the other hand, its main disadvantage is the big Blockchain size. For this reason, Monero will be a better solution. The Monero network makes the transactions in a relatively short time period and its Blockchain does not occupy so much storage disk space.

3.2 Total coins of cryptocurrencies

This comparison is important, because the total number of coins circulating in the network can affect future use of cryptocurrencies and their settlement with fiat currencies. The total number of available cryptocurrency coins in one network shows the extensibility of this currency and, further, it may play a role in the trust of people in this specific cryptocurrency.

Approximately 17 million Bitcoins, nearly 100 million Ethereum and 17 million Moneros have already been mined to these days. Since there is nothing to suggest that someone owns the exact percentage of the compared cryptocurrencies needed to influence their price growth, it can be said that the trust in these cryptocurrencies is very similar by all of them. The same can be said about the enlargement, because each cryptocurrency has enough coins to be owned by a large number of people.

Unlike Bitcoin, Ethereum and Monero have an unlimited total number of coins, it means that for an infinitely long period, new coins of these two cryptocurrencies may be created. In contrast, Bitcoin network is different. The total amount of all generated Bitcoins will be 21 million coins. It is estimated that most Bitcoin coins will be extracted over the next 20 years, and the last Bitcoin will be mined in 2140 [4, p.87].

It causes the major difference in comparison to other cryptocurrencies because with increasing demand for this cryptocurrency, Bitcoin will have a deflationary character. It means that its price will rise against the dollar, so the Bitcoin price of items will decrease. This may leads to the problem, that Bitcoin will not be used for payments if people believe that the goods will be cheaper tomorrow.

This problem cannot happen in the Ethereum or Monero network. On the other hand, without supervision or regulation, prices expressed in ETH or XMR may still rise. It is not possible to say that one cryptocurrency is better than the other, because there are more or fewer coins of this currency. The important fact is to create a certain basis for trustfulness by distributing sufficient amount of cryptocurrency coins between a lot of people. All three cryptocurrencies meet this requirement.

3.3 Static reward

Each generating transaction included in one block contains a static reward that the miners will receive when they have mined the block. This reward is currently 12.5 BTC in Bitcoin network, 3 ETH in Ethereum network and 4.6 XMR in Monero network.

In Bitcoin network, the static reward changes over time. After the Bitcoin network was created, the reward for one mined block was 50 BTC. This reward is reduced to half the size every 210,000 blocks, which is about 4 years. The last so-called halfing was in 2016 and the current reward is 12.5 BTC. Therefore, the next halfing should take place in approximately 2 years to the value of 7.25 BTC. It is assumed that the last Bitcoin will be mined in 2140. Since then, miners will receive a reward for a mined block only from transaction fees [4, p.87].

Bitcoin is much more valuable than Ethereum or Monero. Thus, the reward for mining a block in Bitcoin network is the highest and clearly the most lucrative one.

3.4 Transaction fees

For the transaction to be confirmed in the shortest possible time, it is always necessary to choose a fee that is paid for the transaction. The average value of fees often varies according to the number of transactions waiting in the mempool.

In Bitcoin network, the transaction fees are paid in *Satoshi*, which is the smallest unit of the Bitcoin (1 Satoshi = 0.000,000,01 BTC). On 17th May, 2018, the highest transaction fees were around 1,200 Satoshi, which is 0.09 USD. The most common fees were about 100 Satoshi, approximately 0.008 USD according to the exchange rate in the same day. The lowest ones were, of course, zero [46].

Gwei is the unit in Ethereum network which serves to pay transaction fees (1 Gwei = 0.000,000,001 ETH). The highest fees are around 200 Gwei, approximately 0.000,1 USD. A large part of transactions is in range from 10 to 20 Gwei, which is 0.000,01 USD. The biggest part of Ethereum mempool transactions has the transaction fee only in tenths of Gwei [47].

The transaction fees are on an average of 0.04 Monero, which is 7.92 USD according to the current exchange rate. Even in this network, transactions without fees can be found [48].

When comparing Bitcoin, Ethereum and Monero, it is clear that Ethereum is currently the cheapest way for sending transactions, because the transaction fees are smaller than cents. In Bitcoin network, the fees comes under one dollar. Therefore, the most expensive transaction fee is in Monero network, where the average fee is more than 7 USD.

If the amount of the fee is determined, it will be possible to roughly estimate the time of its confirmation. For example, the transaction fee is 1 USD in all networks. Bitcoin and Ethereum would be sent almost immediately, but Monero would be at the end of the transaction line waiting for confirmation. In terms of user, the most advantageous is Ethereum network, in the miner point of view, the best choice is the Monero network.

3.5 Mining profitability

For mining each cryptocurrency, a certain computing power is needed. This subchapter compares the hardware requirements of Bitcoin, Ethereum and Monero.

In the last few years, a special hardware, so called *ASIC*, was developed for mining Bitcoin. These devices contain several precisely programmed mining chips, and these chips, unlike those in the graphics cards, cannot be used for anything else. This hardware is made in a large design as well as a USB or Cloud device, but the performance of the last two variants is considerably lower. The price of these ASIC devices ranges from 500 USD to 3,000 USD. Their power is measured by hash rate. The best ASIC device power on the market is 16 TH/s, 1 TH/s manages to mine 0.01 BTC per year. USB devices have a maximum of 10 GH/s, its advantage is the price around 50 USD [49].

Special graphics cards are used for mining Ethereum. There have been efforts to construct ASIC hardware for Ethereum, but the Ethereum developers distance from it and modify the blockchain several times in a year so that the ASIC hardware could not be developed [50].

Nowadays, a CPU or graphics chips can still be used for mining a Monero. Cheap mining CPU can be obtained for 30 USD, but even the best CPU power is not enough close to the worst graphic chips. Graphic chips are more expensive, but due to better power, they offer faster return on investment [51].

Table 8 compares the most powerful devices on the market in terms of costs, hash rate and required electricity for individual cryptocurrencies at least for one-year operation. Year profits are calculated with an electricity cost 0.12 USD, which is the average rate per KW/h in the USA [52].

	Bitcoin DragonMint 16T	Ethereum Radeon R9 295X2	Monero Radeon R9 395X2
Price	3,000 USD	600 USD	600 USD
Hash rate	16 TH/s	46 MH/s	46 MH/s
Coins per year	0,192 BTC	2.12 ETH	5.42 XMR
Electricity required	1,480 W	500 W	500 W
Year profit (with electricity costs subtracted)	81.24 USD	986 USD	587 USD

Table 8: Comparison of mining hardware devices
Sources: [49, 50, 51, 52]

As can be seen from Table 8, the most challenging mining from both points of view, hardware requirements and financial costs, is for Bitcoin. Not only that the input costs are 5 times higher than the others, but also the required electricity is almost 3 times bigger. If all the mined coins are sold and the electricity costs are subtracted from it, the highest annual profit will be reached in the Ethereum network. Moreover, the annual profit will be enough to pay the initial costs in the first year of operation. By Monero, the profit may increase due to high transaction fees, but Ethereum's profit will be still the highest one. The transaction fees in Bitcoin and Ethereum network are negligible, so the profits are not affected.

3.6 Utilization

Each cryptocurrency has its own use. Generally speaking, Bitcoin, Ethereum and Monero can be used in many different shops for buying many different items. The problem lies in their very volatile exchange rate. The merchant usually recalculates the price in cryptocurrencies according to the current exchange rate of dollar. It can happen that once the cryptocurrency weakens against dollar, items in the shops will be more expensive in cryptocurrencies than in dollars. We can see it in the following example of buying a laptop.

The notebook will cost approximately 1,000 USD. In conversion to cryptocurrencies, it will cost 0.12 BTC, 1.4 ETH or 4.87 XMR according to

the exchange rate listed in Tables 7 and 8 from 15th May, 2017. Whereas the exchange rate is constantly changing, the laptop may become more expensive if it will be paid in cryptocurrencies. For example, if the values of these cryptocurrencies drop by 10%, the laptop will be available for 900 USD. Of course, the opposite may occur. When the exchange rate of cryptocurrencies increases by 20% within one day, the merchant can claim 1,200 USD for the same laptop.

In spite of the above mentioned problem, many merchants accept cryptocurrencies, but it can be assumed that they consider it as an investment. In this comparison, Bitcoin is the best cryptocurrency that is accepted by the largest number of merchants and very diverse assortment can be acquired for it according to the data presented in previous chapters. Monero is also accepted by many merchants, but often after the conversion to Bitcoin. Ethereum does not serve to classic shopping payments at all.

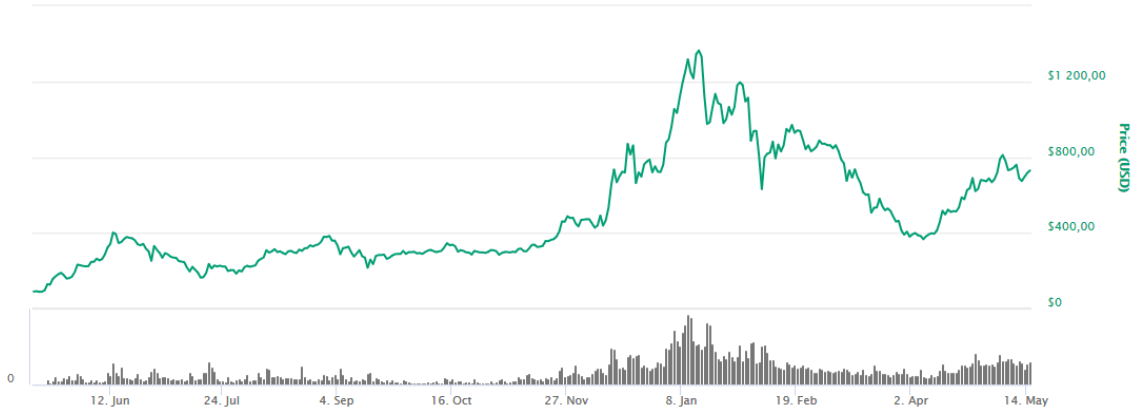
Although Bitcoin offers the best and the most widespread use in practice, cryptocurrencies are used for smaller purchases in which the price drop will not have such a big effect on the product price as in the mentioned laptop example, car or other expensive items. For these items, it is better to use a stable fiat currency for the payment. Currently, cryptocurrencies are mainly used as investment products.

3.7 Price development and investment

For comparison, it is important that the prices of cryptocurrencies are driven only by supply and demand for the specific currency. Supply and demand represent the trust of people in the future use of cryptocurrencies as a supplement of fiat currencies and, above all, the expected increase in value. Therefore, the exchange rate of all cryptocurrencies is very unstable, its value changes every day by a few percent.

Graphs 1, 2 and 3 show the price developments of Bitcoin, Ethereum and Monero during the last year. All the price developments are illustrated against the dollar.

Graph 1: Bitcoin price development from 15th May, 2017 to 15th May, 2018
Retrieved from: [14] [cit. 2018-05-15]



Graph 2: Ethereum price development from 15th May, 2017 to 15th May, 2018
Retrived from: [28] [cit. 2018-05-15]

Graph 3: Monero price development from 15th May, 2017 to 15th May, 2018
Retrieved from: [38] [cit. 2018-05-15]

The graphs show that the price development of these cryptocurrencies is very similar. It is due to the fact that Bitcoin significantly affects the values not only of Monero and Ethereum, but also of other cryptocurrencies.

At the beginning of the reporting period, only a slightly rising price with small fluctuations is visible from May 2017 till September 2017. This moderate growth continues until the end of November 2017. At the turn of November and December, the price of all cryptocurrencies grew sharply. During a relatively short period of time, from the point of view of the entire history of the cryptocurrencies, all monitored cryptocurrencies reached their peaks.

Bitcoin reached its peak on 17th December, 2017 at 19,392.4 USD. Bitcoin is the only cryptocurrency of these compared cryptocurrencies, which has its peak in 2017. The other two currencies, Monero and Ethereum, reached their peaks in January 2018. The first was Monero with its peak at 471.89 USD on 7th January, 2018. Only one week later, on 15th January, Ethereum reached its peak at 1,389.18 USD.

Table 9 compares the percentage difference in the price development of Bitcoin, Ethereum and Monero. The percentage difference is calculated from the maximum price and the current price valid on 15th May, 2018.

	Maximum price	Current price	Price difference in USD	Percentage difference
Bitcoin	19,392.4 USD	8,530.57 USD	10,861.83 USD	56 %
Ethereum	1,389.18 USD	713.59 USD	675.59 USD	48.6 %
Monero	471.89 USD	205.41 USD	266.48 USD	56.5 %

Table 9: Percentage differences of Bitcoin, Ethereum and Monero
Sources: [15, 29, 39] [cit. 2018-05-15], calculations by Šindelářová

The biggest price difference, 10,861.83 USD, can be seen in Bitcoin because of its highest maximum as well as current price. On the other hand, Monero has the lowest price difference, only 266.48 USD, though its percentage difference 56.5 % is the highest one. Ethereum shows the percentage difference 48.6%, which makes it the lowest one.

After these cryptocurrencies have reached the maximums, their prices dropped sharply in the middle of February. The exact cause is not clear, there are only speculations about why these prices drops have occurred. Since then, the prices of all cryptocurrencies have been very unstable and the periods of growth and decline have been changing.

Generally, the prices of Bitcoin, Ethereum and Monero have increased in 2017 and 2018. Bitcoin shows smaller fluctuations in price development compared with Ethereum or Monero. For that reason, Ethereum and Monero Ether appear to be a more risky cryptocurrency, particularly in the short-term investment, because of the highest fluctuations in the price development.

3.8 Investment

A specific feature of investing in cryptocurrencies is that they do not actually exist and deposits are not secured. Meanwhile, losing cryptocurrencies at the time of the cyber attacks is deductible. Another specific feature is that cryptocurrencies are decentralized, in other words they are not regulated and controlled, therefore the investment in them is very dangerous and risky. The reward for taking the risk may be higher return than the one which can be obtained in the financial markets. Stocks with 600% increase in value of the same period can be found, but more common returns are between 70% and 100%.

The following example presented in Table 10 illustrates the price development and return on investment in one year. It is assumed that the buy and sell price equals the exchange rate between the given cryptocurrencies and the US dollar.

	Investment	Purchase on 15th May, 2017	Percentage increase in value on 15th May, 2018	Return	Net profit
Bitcoin	500 USD	0.28 BTC	377 %	2,388 USD	2,338 USD
Ethereum	500 USD	5.41 ETH	677 %	3,860 USD	3,360 USD
Monero	500 USD	17.99 XMR	638 %	3,695 USD	3,195 USD

Table 10: Comparison of return on investment
Sources: [15, 29, 39] [cit. 2018-05-15], calculations by Šindelářová

On the 15th May, 2017, 500 USD was invested in all cryptocurrencies. With the Bitcoin purchase price 1808 USD at the beginning of the investment, we received about 0.28 BTC for 500 USD. The purchase price of one Ether was at the beginning 92.41 USD, thus for 500 USD, 5.41 ETH were obtained. Monero costs 27.79 USD at the time of investment, hence for 500 USD, we received 17.99 XMR.

After one year, Bitcoin increased by 377%, Ethereum by 677% and Monero by 638%. It means that from the original 500 USD, there was net profit 2,338 USD when investing in Bitcoin, 3,360 USD when investing in Ethereum and 3,195 USD when investing in Monero. It is apparent that the net profit of Ethereum was the highest one and higher by 1,000 USD than the Bitcoin net profit.

The example with a one-year increase in value is simplified due to the fact that the person who bought the cryptocurrency could sell it during the year for different amounts because of huge fluctuations. Table 11 shows an increase in value if the sample investment had been sold at the highest possible value.

	Purchase on 15th May, 2017	Price in the time of selling	Max increase in value	Max return
Bitcoin	0.28 BTC	19,392.4 USD	985 %	5,429 USD
Ethereum	5.41 ETH	1,389.18 USD	1400 %	7,514 USD
Monero	17.99 XMR	471.89 USD	1590 %	8,473 USD

Table 11: Maximum profit of investment
Sources: [15, 29, 39] [cit. 2018-05-15], calculations by Šindelářová

During the reporting year, the highest value of each cryptocurrency is also its highest historical value. If the investor had an excellent estimate, he would have earned the highest amount on Monero with the net profit of 8,473 USD. During the investment period, there would be no loss because the value of Bitcoin, Ethereum and Monero did not fall below the purchased value.

In this comparison, Ethereum or Monero can be considered the most profitable cryptocurrencies. Of course, it depends on when they are sold, but their investment returns are many times larger than Bitcoin's one.

CONCLUSION

The aim of this bachelor's thesis was to summarise the main information and knowledge about cryptocurrencies and to compare three individual cryptocurrencies. These cryptocurrencies were compared in the last chapter from different points of view.

In the first chapter, the cryptocurrencies were generally described. It was focused on the general information about their functioning, acquirement and storage. The second chapter dealt with the introduction of each currency, their history, the technical and economic parameters, storage and their real-world use. The last part of this thesis was the comparison of described cryptocurrencies Bitcoin, Ethereum and Monero.

Bitcoin has proved to be a currency suitable for investments. Profits are not large in comparison to Ethereum or Monero, but because of lower fluctuations in price development, this currency is more stable. In the Bitcoin network, miners will also receive the highest static reward per one mined block. Its disadvantage is that this reward is steadily decreasing and the cost of mining is steadily growing.

From compared cryptocurrencies, Ethereum is the best choice despite the fact that its use for payments in stores is not possible. Its biggest advantage is the speed of confirming transactions with very low transaction fees. Mining of Ethereum is not as difficult as Bitcoin and initial cost repayment can be achieved during the first year. As an investment, Ethereum is very profitable, but due to fluctuations in price development, it is very risky.

As Ethereum, Monero is a profitable as well as risky investment product, too. Unfortunately, the transaction fees within the Monero network are the highest of the described cryptocurrencies, which is the major disadvantage for its users. On the other hand, it is beneficial for miners who receive the fees for finding a valid block.

Generally, cryptocurrencies are very controversial and divide the world into their fans and opponents. Despite the fact that no state has accepted them as a full-fledged currency yet, they are becoming more and more popular, mostly as investment products. Each person who wants to invest in cryptocurrencies should understand these problems and know the principles on which the cryptocurrency works. Despite considerable knowledge and also the short history of this technology, no one can accurately estimate their future development.

LIST OF REFERENCES

[1] MARTINÁK, Tomáš. *Bezhotovostní peníze versus elektronické peníze*. Olomouc: Iuridicum Olomoucense, s.r.o., ve spolupráci s Právnickou fakultou Univerzity Palackého v Olomouci, 2015. ISBN 978-80-87382-74-5.

[2] SMEJKAL, Ladislav. Elektronické peníze. *Ikaros* [online]. 2001, ročník 5, číslo 10 [cit. 2018-03-12]. urn:nbn:cz:ik-10800. ISSN 1212-5075. Retrieved from: http://ikaros.cz/node/10800

[3] ANTONOPOULOS, Andreas M. *Mastering bitcoin*. Sebastopol CA: O'Reilly, 2015. 298 p. ISBN 978-1-449-37404-4.

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

[5] Unenumerated: Bit gold. *Unenumerated* [online]. [cit. 2017-12-06]. Retrieved from: https://unenumerated.blogspot.cz/2005/12/bit-gold.html

[6] Introduction to Cryptocurrency - CryptoCurrency Facts. *Introduction to Cryptocurrency - CryptoCurrency Facts* [online]. Copyright © 2017 CryptoCurrency Facts [cit. 2018-05-02]. Retrieved from: http://cryptocurrencyfacts.com/

[7] Úvod. *Kryptografie* [online]. [cit. 2017-12-06]. Retrieved from: http://www.kryptografie.wz.cz/uk.htm

[8] PIPER, Fred and Sean MURPHY. *Kryptografie*. Praha: Dokořán, 2006. Průvodce pro každého. ISBN 80-7363-074-5.

[9] TĚŽBA KRYPTOMĚN: Jak těžit kryptoměny, princip, návratnost, návod. *Investice a spoření | Invest+* [online]. Copyright © [cit. 2017-12-06]. Retrieved from: https://investplus.cz/investice/tezba-kryptomen-jak-tezit-kryptomeny-princip-navratnost-navod/

[10] What Is Cryptocurrency - How It Works, History & Bitcoin Alternatives. *Money Crashers* [online]. [cit. 2017-12-06]. Retrieved from: https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/

[11] Top 4 Altcoins Supported by Cryptocurrency ATMs – The Merkle. *The Merkle* [online]. Copyright © 2017 [cit. 2017-12-06]. Retrieved from: https://themerkle.com/top-4-altcoins-supported-by-cryptocurrency-atms/

[12] What are the different types of Cryptocurrency wallets?. *Steemit* [online]. [cit. 2017-12-06]. Retrieved from: https://steemit.com/crypto/@domaz20/what-are-the-different-types-of-cryptocurrency-wallets

[13] Types Of Cryptocurrency Wallets Explained - Crypto Daily. *CryptoDaily Brings You The Latest News & Crypto Help with Coins, Exchanges & Mining [*online]. Copyright © 2017 [cit. 2017-12-06]. Retrieved from: https://cryptodaily.co.uk/types-cryptocurrency-wallets-explained/

[14] Bitcoin price, charts, market cap, and other metrics. *Cryptocurrency Market Capitalizations | CoinMarketCap* [online]. Copyright © 2018 CoinMarketCap. [cit. 2018-03-12]. Retrieved from: https://coinmarketcap.com/currencies/bitcoin/

[15] Bitcoin (BTC) statistics - Price, Blocks Count, Difficulty, Hashrate, Value. *Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Ethereum stats* [online]. [cit. 2018-05-15]. Retrieved from: https://bitinfocharts.com/bitcoin/

[16] Bitcoin Pizza Index. *Bitcoin Pizza Index* [online]. Copyright © 2018. [cit. 2018-02-08]. Retrieved from: https://bitcoinpizzaindex.net/

[17] Bitcoin History: The Complete History of Bitcoin [Timeline]. *Bitcoin History: The Complete History of Bitcoin [Timeline]*. [online]. [cit. 2017-12-06]. Retrieved from: http://historyofbitcoin.org/

[18] Hardware - Choose your wallet. *Bitcoin* [online]. Copyright © Bitcoin Project 2009 [cit. 2018-03-31]. Retrieved from: https://bitcoin.org/en/wallets/hardware/

[19] SatoshiLabs. *SatoshiLabs* [online]. [cit. 2018-03-31]. Retrieved from: https://satoshilabs.com/

[20] Choose your wallet. *Bitcoin* [online]. Copyright © Bitcoin Project 2009 [cit. 2018-03-31]. Retrieved from: https://bitcoin.org/en/choose-your-wallet

[21] Print Offline Tamper-Resistant Addresses. *Bitcoin Paper Wallet Generator* [online]. [cit. 2018-03-31]. Retrieved from: https://bitcoinpaperwallet.com/

[22] Coinbase | Where can I spend bitcoin? . *Coinbase | Support* [online]. Copyright © 2017 Coinbase [cit. 2017-12-06]. Retrieved from: https://support.coinbase.com/customer/portal/articles/1834716-where-can-i-spend-bitcoins

[23] V Alze zaplatíte Bitcoiny. *Alza.cz - největší obchod s počítači a elektronikou* [online]. [cit. 2018-02-08]. Retrieved from: https://www.alza.cz/platba-bitcoiny-a-btc-automaty-alza

[24] Now you can exchange bitcoins to buy apps, games and more for Windows, Windows Phone and Xbox - The Fire Hose. *The Official Microsoft Blog* [online]. [cit. 2017-12-06]. Retrieved from: https://blogs.microsoft.com/firehose/2014/12/11/now-you-can-exchange-bitcoins-to-buy-apps-games-and-more-for-windows-windows-phone-and-xbox

[25] Blockchain at UNICEF – Stories of UNICEF Innovation. *Stories of UNICEF Innovation* [online]. [cit. 2017-12-06]. Retrieved from: http://unicefstories.org/blockchain/

[26] HUMAN RIGHTS FOUNDATION / DONATE. *HUMAN RIGHTS FOUNDATION* [online]. [cit. 2017-12-06]. Retrieved from: https://humanrights.foundation/donate/

[27] Ethereum Project. *Ethereum Project* [online]. Copyright © 2017 Ethereum Foundation [cit. 2017-12-06]. Retrieved from: https://www.ethereum.org/

[28] Ethereum (ETH) price, charts, market cap, and other metrics. *Cryptocurrency Market Capitalizations | CoinMarketCap* [online]. Copyright © 2018 CoinMarketCap. [cit. 2018-03-12]. Retrieved from: https://coinmarketcap.com/currencies/ethereum/

[29] Ethereum / Ether (ETH) statistics - Price, Blocks Count, Difficulty, Hashrate, Value. *Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Ethereum stats* [online]. [cit. 2018-05-15]. Retrieved from: https://bitinfocharts.com/ethereum/

[30] History of Ethereum — Ethereum Homestead 0.1 documentation. *Redirecting. [*online]. Copyright © 2016, Ethereum community [cit. 2017-12-06]. Retrieved from: http://ethdocs.org/en/latest/introduction/history-of-ethereum.html

[31] A hacker stole $31M of Ether. *FreeCodeCamp* [online]. [cit. 2017-12-06]. Retrieved from: https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce

[32] The history of Ethereum. *ReadWrite | The leading Internet of Things News Platform* [online]. Copyright © 2017 ReadWrite [cit. 2017-12-06]. Retrieved from: https://readwrite.com/2017/10/18/infographic-ethereum-history/

[33] The Top 10 Best Ethereum Wallets (2018 Edition). *CoinSutra: Bitcoin Tips, Tutorials & Community* [online]. Copyright © 2017 [cit. 2018-03-31]. Retrieved from: https://coinsutra.com/best-etherum-wallets/

[34] MyEtherWallet.com. *MyEtherWallet.com* [online]. Copyright © 2018 MyEtherWallet, Inc [cit. 2018-03-31]. Retrieved from: https://www.myetherwallet.com/

[35] 7 Cool Decentralized Apps Being Built on Ethereum - CoinDesk. *CoinDesk - Leader in blockchain news* [online]. [cit. 2017-12-06]. Retrieved from: https://www.coindesk.com/7-cool-decentralized-apps-built-ethereum/

[36] A Current List of Use Cases for Ethereum Around The Block Medium. *Hackerfall - A different way to browse Hacker News* [online]. [cit. 2017-12-06]. Retrieved from: https://hackerfall.com/story/a-current-list-of-use-cases-for-ethereum

[37] What is Monero? Most Comprehensive Guide 2018. *Blockchain community - Blockgeeks* [online]. [cit. 2018-03-17]. Retrieved from: https://blockgeeks.com/guides/monero/

[38] Monero (XMR) price, charts, market cap, and other metrics. *Cryptocurrency Market Capitalizations | CoinMarketCap* [online]. Copyright © 2018 CoinMarketCap. [cit. 2018-03-12]. Retrieved from: https://coinmarketcap.com/currencies/monero/

[39] Monero (XMR) statistics - Price, Blocks Count, Difficulty, Hashrate, Value. *Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Ethereum stats* [online]. [cit. 2018-05-15]. Retrieved from: https://bitinfocharts.com/monero/

[40] VAN SABERHAGEN, Nicolas. *CryptoNote v 1.0* [online]. 2012-12-12 [cit. 2018-03-17]. Retrieved from: https://cryptonote.org/whitepaper_v1.pdf

[41] VAN SABERHAGEN, Nicolas. *CryptoNote v 2.0* [online]. 2013-10-17 [cit. 2018-03-17]. Retrieved from: https://bytecoin.org/old/whitepaper.pdf

[42] SERHACK. *Mastering Monero: The future of private transactions* [online]. [cit. 2018-03-17]. Retrieved from: https://masteringmonero.com/book/preview.pdf

[43] Downloads. *Monero - secure, private, untraceable* [online]. [cit. 2018-03-18]. Retrieved from: https://getmonero.org/downloads/

[44] The ultimate guide to monero - Cointelligence. *Cointelligence - The central nervous system for a crypto economy* [online]. [cit. 2018-03-18]. Retrieved from: https://www.cointelligence.com/content/ultimate-monero-guide/

[45] Buy gift cards online. *Buy gift cards online & earn loyalty points* [online]. Copyright © 2018. [cit. 2018-03-18]. Retrieved from: https://giftoff.com/gift-cards

[46] Johoe's Bitcoin Mempool Size Statistics. *Johoe's Bitcoin Mempool Size Statistics* [online]. Copyright © 2016. [cit. 2018-05-17]. Retrieved from: https://jochen-hoenicke.de/queue/#1,24h

[47] Ethereum Pending Transactions. *Ethereum (ETH) BlockChain Explorer* [online]. Copyright © 2018. [cit. 2018-05-17]. Retrieved from: https://etherscan.io/txsPending

[48] XMR mempool. *XMR mempool* [online]. [cit. 2018-05-17]. Retrieved from: https://pooldata.xmrlab.com/

[49] 5 Best Bitcoin Mining Hardware ASICs 2018 (Comparison). *101+ Best Ways to Buy Bitcoins Online in 2018* [online]. [cit. 2018-05-17]. Retrieved from: https://www.buybitcoinworldwide.com/mining/hardware/

[50] 3 Best Ethereum Mining Hardware GPUs of 2018 (Updated) . *Easy PC - Build Your Dream PC* [online]. [cit. 2018-05-17]. Retrieved from: https://www.easypc.io/crypto-mining/ethereum-hardware/

[51] 5 Best Monero Mining Hardware GPUs & CPUs 2018 (Cryptonight) . *Easy PC - Build Your Dream PC* [online]. [cit. 2018-05-17]. Retrieved from: https://www.easypc.io/crypto-mining/monero-hardware/

[52] Average electricity prices around the world: $/kWh. *OVO Energy* [online]. [cit. 2018-05-17]. Retrieved from: https://www.ovoenergy.com/guides/energy-guides/average-electricity-prices-kwh.html

LIST OF GRAPHS

LIST OF TABLES