

CZECH UNIVERSITY OF LIFE SCIENCES  
PRAGUE

Faculty of Economics and Management

**Informatics**



ANALYSIS BITCOIN VIRTUAL  
CURRENCY

BACHELOR THESIS

Author:

**Jan Potužník**

Bachelor thesis supervisor:

Ing. Pavel Šimek, Ph.D.

**2014**

### **Declaration**

I declare that I **Jan Potužník** carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. I understand that my work relates to the rights and obligations under the Act No. 121/2000 Coll., the Copyright Act, as amended, in particular the fact that the Czech University Of Life Sciences Prague has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 paragraph 1 of the Copyright Act.

In Prague date 10.3.2014

### **Anotace**

Cílem celé bakalářské práce “Analýza virtuální měny Bitcoin” je analýza první decentralizované digitální měny nazývané Bitcoin a stávání se aktivním členem dolování. Tato práce také zahrnuje analýzu odlišných decentralizovaných měn, které vznikly na bázi měny Bitcoin a porovnání těchto měn k měně Bitcoin. Praktická část této bakalářské práce je zaměřena na detailní popis, jak se stát aktivním členem v procesu dolování a zároveň informovat, zda je dolování profitabilní business nebo ne.

### **Annotation**

The goal of the submitted thesis “Analysis Bitcoin virtual currency” is to analyze the first decentralized digital currency called Bitcoin and become an active member of the mining process. The thesis is also supposed to analyze different decentralized digital currencies that were created based on Bitcoin and compare these currencies to Bitcoin. The practical part of this bachelor thesis is focused on the detailed description of how to become an active member of the mining process and if mining is a profitable business or not.

### **Keywords**

Bitcoin, Litecoin, BTC, LTC, virtual currency, mining

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>8</b>
<b>2</b>	<b>Thesis objective and methodology</b>	<b>9</b>
<b>3</b>	<b>Literature review</b>	<b>10</b>
<b>3.1</b>	<b>Transactions before Bitcoin</b>	<b>10</b>
3.1.1	Internet based transaction with middleman	10
3.1.2	Internet based transaction without middleman	10
<b>3.2</b>	<b>History</b>	<b>11</b>
3.2.1	Bitcoin creator	11
3.2.2	Price development	11
<b>3.3</b>	<b>What is Bitcoin</b>	<b>13</b>
<b>3.4</b>	<b>Mining process</b>	<b>13</b>
3.4.1	Who are miners	14
3.4.2	Mining hardware	14
3.4.3	Blockchain	18
3.4.4	Difficulty	18
<b>3.5</b>	<b>Storing Bitcoins</b>	<b>18</b>
3.5.1	Wallet	19
3.5.2	Cold storage	20
3.5.3	Bitcoin trezor	20
<b>3.6</b>	<b>Exchanges</b>	<b>20</b>
3.6.1	MTGox.com	22
<b>3.7</b>	<b>Bitcoin in the future</b>	<b>23</b>
<b>3.8</b>	<b>Hash algorithm</b>	<b>24</b>
<b>4</b>	<b>Analytical part</b>	<b>25</b>
<b>4.1</b>	<b>Bitcoin vs. other currencies</b>	<b>25</b>
4.1.1	Litecoin - LTC	25
4.1.2	Peercoin - PPC	26
4.1.3	Namecoin - NMC	26
4.1.4	Dogecoin - DOGE	27
4.1.5	Quark - QRK	27
4.1.6	Auroracoin - AUR	28

4.2	Altcoins summary.....	28
5	Results and discussion.....	30
5.1	Hardware research .....	30
5.1.1	Hardware searching.....	31
5.1.2	Building mining rig.....	35
5.2	Software setup .....	36
5.2.1	Linux mining .....	36
5.2.2	Windows mining .....	37
5.3	Solo mining .....	39
5.4	Pool mining.....	40
5.4.1	Reward system.....	40
5.5	Pool & currency decision .....	42
5.6	Miner optimization .....	44
5.7	Electricity costs and investment return.....	46
6	Conclusion.....	47
7	References.....	49
8	Supplements.....	51
8.1	List of tables.....	51
8.2	List of figures.....	51
8.3	Acronyms, abbreviations and symbols .....	52
8.4	Used software.....	52
8.5	Used Hardware.....	53

## 1 Introduction

Bitcoin is the first decentralized digital currency in our world; the guy known only by his pseudonym “Satoshi Nakamoto” created Bitcoin in 2009. Bitcoin is currently in its origins and is spreading all over the world and ordinary people are starting to notice this new digital currency. Bitcoin was started on the Internet forums and today’s economy of Bitcoin is larger than the economies of some small nations. The value of one Bitcoin (BTC) was in its early days around one penny US dollars but today (January 2014) it has almost a 1000 US dollars evaluation. Bitcoin was the first digital currency and it was published as open-source software, due to this fact there are a lot of other digital currencies based on Bitcoin, mostly there is only a little difference among these currencies such as Litecoin, Peercoin, Dogecoin, 42coin, etc. Bitcoin is not only for information technology people called “geeks” or “nerds”, somebody could say that Bitcoin changes the understanding of currency as Internet changed this world.

This thesis leads to inform about Bitcoin as a decentralized currency, its analysis, comparison to other digital currencies, how to obtain Bitcoins via online exchanges, introduce to Bitcoin mining and try to define the best or most profitable mining hardware on the market and its comparison.

## 2 Thesis objective and methodology

This Bachelor thesis investigates digital currency named Bitcoin. The main purpose of this thesis is to analyze Bitcoin and show its positives and negatives. The partial goals of the thesis are:

- To analyze Bitcoin digital currency
- To compare Bitcoin to other digital currency called Litecoin
- To do Bitcoin mining and analyze the best mining hardware

Methodology of the thesis is based on study and analysis of digital currency Bitcoin. Thesis is focused generally in Bitcoin and then comparison to other currency such as Litecoin. The practical part is focused on Bitcoin mining. On the basis of theoretical knowledge and author's own work, the conclusions of the thesis will be formulated.

### 1. Introduction to digital currency Bitcoin

Digital currency analysis. Point out on its positives and negatives.

### 2. Compare Bitcoin to Litecoin

Meeting other currencies such as Litecoin, Feathercoin, Dogecoin...

### 3. Bitcoin mining

Setting up own Bitcoin miner. Connecting to pool mining. Comparing mining hardware.

## **3 Literature review**

### **3.1 Transactions before Bitcoin**

Until introduction of Bitcoin payment system in 2009 by Satoshi Nakamoto, transactions between two parties on the internet always needed a third party - middleman.

#### **3.1.1 Internet based transaction with middleman**

Example – Imagine Leonard wanted to sent 50 EUR to Penny over the Internet, it could be for anything. Leonard would have to depend on some third party that creates and maintains the transaction process until it is finished and everyone is fully satisfied. He could use PayPal or classic money bank transfer. PayPal is much more faster than standard money transfer but there are also big fees for transactions and if somebody steals a credit card, then pay via PayPal transactions are canceled and you have to give your money back – and if you sold something to the thief that stole someone’s credit card you could be pretty angry because you don’t have the subject of the transaction and even you have to give back the money you received. One could say that one of the biggest advantages of PayPal is that they use credit cards but the biggest advantage is the worst way to transfer money, because credit cards (or debit cards) were never designed to operate on the internet, this method is very unsecure in digital age where on every corner of the internet is a hacker. Every middleman (like PayPal) has tables (ledger) with the available amount of money that the user could spend and you can never spend more money because of the ledger records, but what if someone changes these records? Credit cards are just numbers that allow you to spend money if you know them and know the right order – it could be also called password and every password can be broken sooner or later.

#### **3.1.2 Internet based transaction without middleman**

Imagine Sheldon is willing to send Amy 70 EUR, but there is no middleman with a ledger (table with the information on how much money you have etc.) and 70 EUR is stored on the computer in one file. Sheldon could send this money by attaching this file with 70 EUR to an email, so when Amy receives the message she



will be richer about 70 EUR. But what if Sheldon makes a copy of the wallet and he will have two files; each will be exactly the same and contain 70 EUR. He could make as many copies as he would want and become a billionaire. This problem is known as double spending (Caldwell, 2014). Only third parties in transaction processes could solve this problem because they are using ledgers. Bitcoin is revolutionary in this field because it has resolved the “double spending” problem and there is no need for a third party in the transaction process. Bitcoin is also designed to only operate with other bitcoins (BTC), but PayPal was designed to work with USD, EUR and some other fiat currencies that have central authority.

## 3.2 History

Steven Levy has formulated the first information about something like digital currency in 1994 in Wired magazine.

*“The killer application for electronic networks isn’t video-on-demand. It’s going to hit you where it really matters - in your wallet. It’s, not only going to revolutionize the Net, it will change the global economy.” (Steven, 1994)*

### 3.2.1 Bitcoin creator

The guy called “Satoshi Nakamoto” has invented Bitcoin in 2009. This name is just pseudonym and nobody knows exactly who this guy is, there are many speculations that it could be Kim Dotcom (owned megaupload.com), or the owner of the black market operated on TOR network called SilkRoad but there are currently no facts who Satoshi Nakamoto is. At the beginning of March 2014 there were speculations that Satoshi Nakamoto has been discovered and that his real name is Dorian Nakamoto that he is 55 years old and he is a programmer from Los Angeles. But this guy denied that he is creator of Bitcoin.

### 3.2.2 Price development

- **Year 2009**

The Bitcoin system has been invented in 2009, but there was no value for 1 BTC, not even for 100 000 BTC, there were no online exchanges and bitcoin users were just cryptographic fans.

- *Year 2010*

In May 2010 Bitcoin has still almost no value, but there was a guy “laszlo” that bought a pizzas for 10 000 BTC (25 USD). He posted to an online forum that he is willing to trade 2 pizzas for 10 000 BTC.

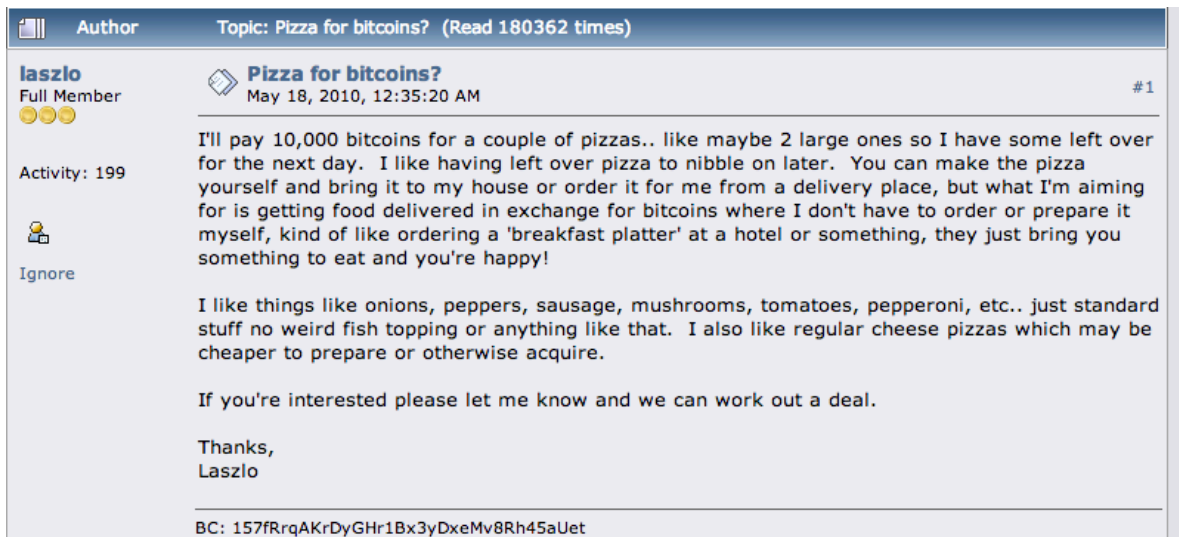


Figure 1: First noted transaction in Bitcoins [Source: bitcointalk.org]

In June 2010 there was a 1000% grew in BTC price in fewer than 5 days price grew from 0.008 USD to 0.08 USD for 1 BTC.

- *Year 2011*

In April the price of one Bitcoin was equal to 1 USD on MTGOX.com (first online bitcoin exchange) and it was considered as a tremendous success of Bitcoin.

In July the price of 1 BTC was around 31 USD and then dropped to 2 USD for one BTC – this time is still considered as the first “bitcoin bubble”.

- *Year 2012*

Bitcoin slowly rose from 2 USD to 15 USD, but no big changes.

- *Year 2013*

In April 2013 one Bitcoin hit 265 USD evaluations during two days and then dropped to a 100 USD. Then the value of Bitcoin was stable and nothing serious happened in its price change, then in November Bitcoin attacked a 1250 USD evaluation. At the end of the year 2013 bitcoin was around 700 USD. 1250 USD evaluation was the highest price of one Bitcoin in its history.

- *Year 2014*

In January Mtgox.com belonged to the one of the biggest exchanges with Bitcoins, but due to its improperly designed exchange software they lost over 740 000 BTC during its operation and at the end of February they closed due to high debt.

### **3.3 What is Bitcoin**

Bitcoin is the first decentralized digital payment system; it is based on open-source platform so anyone may download its code and modify it. Decentralized in this context means that there is no central authority that maintains transactions or holdings of Bitcoins. In a classic conventional payment system there is always a government or a bank that maintains transactions and when in need, a bank can always print or create new money because the rule that all money has to be covered by gold or something else was cancelled a long time ago, but in the Bitcoin payment system we know exactly how many Bitcoins will be in circulation and even when. The process in which Bitcoins are created and transactions verified is called mining.

*“Email let us send letters for free, anywhere in the world. Skype lets us make phone and video calls for free, anywhere in the world. Now there's bitcoin. Bitcoin lets you send money to anyone online, anywhere in the world for less than a cent per transaction! Bitcoin is community run system not controlled by any bank or government. There's no Wall street banker getting rich by standing between you and the people you want to send and receive money from.” (Osmosis)*

Bitcoin is a software and is distributed via a peer-to-peer network, which means that there is no central authority like servers – all the members of Bitcoin network are equal.

### **3.4 Mining process**

The Bitcoin doesn't have a central authority that secures and maintains the circulation (transactions). Though this work has to be done and on the Bitcoin network the hard work is done by “miners”.

This process is called mining because people who are doing this job are compared to gold miners that were digging gold from the ground so everyone could

“use” this gold. In reality bitcoin miners are just software programs that run on sophisticated hardware and maintain the bitcoin network.

### 3.4.1 Who are miners

Miners are collecting transactions on the network (for example when Howard is sending 10 BTC to Raj and then Raj is sending 1.23 BTC to Sheldon) into bundles named blocks. These blocks are continuously linked together into a “ledger” called blockchain. Blockchains contain every verified transaction that occurred in the Bitcoin network. Blockchain is very necessary because it solves the “**double spending**” problem in computer science. If you have one BTC stored on your computer and send it to anyone, this transaction will occur in a blockchain, miners will verify it and everybody in the network will be broadcasted the information that this bitcoin was spent from your address and sent to that address.

Bitcoin blocks are really hard to produce and that ensures that nobody can switch the blockchain. New blocks cannot be just generated at will. Miners have to compute a cryptographic hash that meets the specific criteria to produce new blocks. This process is called hashing. The only possible way to find a valid cryptographic hash that is accepted is by trying “every” possibility and then you will find a hash that works. Finding the valid hash is like “lottery” (Schwartz, 2012) because every new valid block is rewarded with the amount of Bitcoins according to the reward schedule. The difficulty of the criteria for the hash is continually adjusted based on how frequently blocks are appearing, so more competition equals more work needed to find a block.

### 3.4.2 Mining hardware

Mining is just a piece of software that runs on a computer. When the computer has a lot of computing power it would work faster and do more work in finding valid blocks in one second. Mining software may be run on standard conventional CPU (Central Processing Unit, “processor”) but finding the valid hash is trying every possible combination until you find the one that works so it is still the same work only with different parameters and standard CPUs are not optimized for this kind of work and it is better to use GPUs (Graphic Processing Unit, “graphic card”) for mining. GPUs were designed for rendering images to your display

(monitor) so they do the same work for each pixel on the screen therefore there is an optimization for processing the same work over and over in a short period of time. Then people discovered the FPGA (programming cards) but it was mostly for “programming guru nerds”. During some time the Bitcoin gained popularity and people developed specialized “mining hardware” named ASIC (Application Specialized Integrated Circuit). ASICs are optimized for just one work so they work even faster than GPUs. For example very modern CPU could run 15 MHash/s (M – stands for mega), GPU could run 700 MHash/s and ASIC could run 600 GHash/s (G – stands for giga). Hash per second (Hash/s) is a term that is used in mining when comparing hardware – determines the possible speed of the hardware.

#### 3.4.2.1 CPU mining

Running mining software on your CPU and “getting” any bitcoins for the work is impossible nowadays. CPUs are not designed for this job; they are slow and consume a lot of electricity. It was possible to mine on CPU in the early days of Bitcoin estimated till beginning of 2010.



Figure 2: CPU  
[source: intel.com]

#### 3.4.2.2 GPU mining

GPUs are designed to create a large number of polygons on your screen quickly. These calculations are relatively simple to perform, leading GPU architecture to be optimized for a large number of simple processes calculated in a parallel (simultaneously). Developing mining software for the GPU became the logical next step. This idea was proposed on [bitcointalk.org](http://bitcointalk.org) in 2009. Satoshi respond to this post:

*“The average total coins generated across the network per day stays the same. Faster machines just get a larger share than slower machines. If everyone bought faster machines, they wouldn't get more coins than before.”*

*“We should have a gentleman's agreement to postpone the GPU arms race as long as we can for the good of the network. It's much easier to get new users up to speed if they don't have to worry about GPU drivers and compatibility. It's nice how anyone with just a CPU can compete fairly equally right now.” (Satoshi, 2009)*

In September 2010, guy called “puddinpop” released first public software for mining on GPUs by public license under

MIT. First software was optimized for an nVidia (CUDA) graphic card but over a short period of time the miners noticed that ATI (OpenCL) is better optimized for this mining and nowadays the softwares are just for ATI cards.



Figure 3: GPU [source: ati.com]

### 3.4.2.3 FPGA mining

In early 2012 new companies focused on Bitcoin mining hardware and started offering FPGA cards to the public, its speed was around 200 MHash/s per card and its cost was around 1 US Dollar for one MHash/s. But standard graphic cards were much more popular because it was simpler to run bitcoin miner on them. FPGA cards didn't require as much electricity power as high end GPUs.



Figure 4: FPGA card modified for bitcoin mining [source: enterpoint.co.uk]

### 3.4.2.4 ASIC mining

In Bitcoin mining terminology ASICs are equipment that can do only one type of job – hashing (finding new blocks). Compared to previous mining hardware this is designed only for the one job and has much lower electricity consumption for one MHash/s. The company Avalon produced first batch of these devices in late January 2013.



Figure 5: Avalon miner [source: [gizmodo.com.au](http://gizmodo.com.au)]

First ASIC miner that was sold to consumers has 60 GHash/s and power consumption was around 400W – this is the same power consumption as a very high-end GPU that has “only” 800 MHash/s top. The price of the first Avalon ASIC miner was around 1300 USD but the payment was acceptable only in BTC (that time 75 BTC). One year later after the first ASIC miner the hashing speed of these chips increased by 10-20 times and created a new market for people that are developing these chips. KNC Company in December 2013 introduced a new device that was capable of producing 2.1 BTC per day (in ideal conditions) and the estimated delivery was in May 2014. During the 24 hours from releasing this information the KNC Company made 8 million USD for selling pre-orders to public.

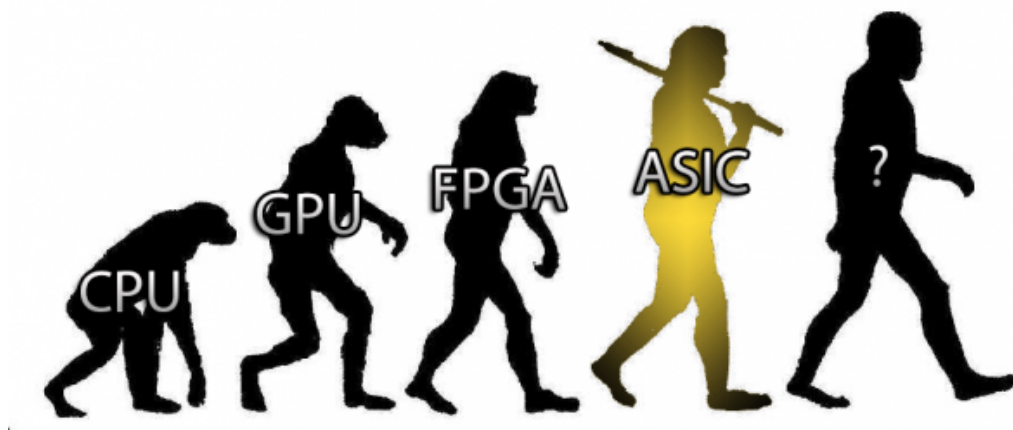


Figure 6: Mining hardware development [source: [thegenesisblock.com](http://thegenesisblock.com)]

### 3.4.3 Blockchain

Blockchain is a transaction database that is visible to all users of the Bitcoin network and it contains every verified transaction in bitcoin history. According to its information one could easily define how much bitcoins this wallet has. Blockchain is in short a Bitcoin.

*“When a Bitcoin client signs on to the network it can trust the blockchain that was most difficult to produce (since this is evidently the one that was being worked on by the most miners). If there was a "fake" blockchain competing with the real ones, the fraudster would have to do as much work as the whole rest of the network to make their block chain look as trustworthy. So essentially, the intense work that goes into finding blocks through hashing secures the network against fraud.”*  
(eMansipater, 2011)

A blockchain is also visible through a web-browser on <https://blockchain.info/>

### 3.4.4 Difficulty

It is a measure of how hard it is to find a hash below a given target. The Bitcoin network has a global block difficulty. Valid blocks must have a hash below this target. Difficulty is being adjusted every 2016 blocks based on the time it took to find the previous 2016 blocks. At the desired rate of one block each 10 minutes, 2016 blocks would take exactly two weeks to find. If the previous 2016 blocks took more than two weeks to find, the difficulty is reduced. If they took less than two weeks, the difficulty is increased. The change in difficulty is in proportion to the amount of time over or less than two weeks the previous 2016 blocks took to find.

### 3.5 Storing Bitcoins

Bitcoin is just binary code and if you have a private key for the Bitcoin you can manipulate with it like sending to another user. Every wallet or storage for bitcoins has its unique ID; in this case it is called address. Address is just a hash of 27 to 30 characters (here is an example of a Bitcoin address: **1MwAM7MB1sPAzMZxqk9UmPwUmfBwaEuhEz**) and a bitcoin address always starts with “1” or “3”. A Bitcoin address works as a normal email address. For most



properly generated Bitcoin addresses, there is at least one secret number known as a private key that is required for access to the funds assigned to that address.

When using a Bitcoin client, private keys are typically stored in the wallet file. The private key has a special purpose - it is mathematically needed to create valid transactions that spend the funds originally sent to the address. If the private key to an address is lost (for example, in a hard drive crash, fire or other natural disaster), any associated Bitcoins are effectively lost forever. (Casascius, 2012)

Because in Bitcoins there is nothing like a Variable symbol or a Specific symbol (standard money transfer) you can generate as many addresses as you want to determine the sender of the money. You just have to give each person (transaction) a new address. Bitcoin is currently capable of  $2^{160}$  addresses and that is an enormously huge number.

### 3.5.1 Wallet

A Bitcoin wallet works almost the same way as any wallet for normal currencies such as EUR or USD. It gives you the ability to send (spend) or receive coins (money). Currently there are many wallets for Windows, Linux, OS X and even for Android and Windows Phone. There were many wallets for iOS too (Apple iPhone, iPad) but Apple has a very strict policy and doesn't like Bitcoins so every wallet in the Appstore was almost immediately removed.

#### 3.5.1.1 MultiBit

MultiBit is a lightweight client that focuses on being fast and easy to use. It synchronizes with the network and is ready to use in minutes. MultiBit also supports many languages. It is a good choice for non-technical users. The best about MultiBit is that doesn't download whole blockchain. MultiBit only connects to servers that contain blockchains and synchronize it.



Figure 7: Multibit symbol [source: multibit.org]

#### 3.5.1.2 Bitcoin-Qt

Bitcoin-Qt is a full Bitcoin client and builds the backbone of the network. It offers the highest levels of security, privacy, and stability. However, it has fewer features and it takes a lot of space and memory. If you want to use this wallet, it has

to be fully synchronized with the network and a whole blockchain is stored in your computer.

### 3.5.1.3 Electrum

Electrum's focus is speed and simplicity, with low resource usage. It uses remote servers that handle the most complicated parts of the Bitcoin system, and it allows you to recover your wallet from a secret phrase.



Figure 8: Electrum symbol [source: [electrum.org](http://electrum.org)]

### 3.5.2 Cold storage

This type of storage stores Bitcoin offline. For example, a Bitcoin exchange typically offers an instant withdrawal feature, and might be a steward over hundreds of thousands of Bitcoins. To minimize the possibility that an intruder could steal the entire reserve in a security breach, the operator of the website follows a best practice by keeping the majority of the reserve in cold storage, or in other words, not present on the web server or any other computer. The only amount kept on the server is the amount needed to cover anticipated withdrawals. Cold storage works in a way that private key is removed from the wallet where it is stored and it could be memorized or better way is to print it to paper because it is very long hash string.

### 3.5.3 Bitcoin trezor

*“TREZOR is a single purpose computer that signs Bitcoin transactions made through a desktop or web-wallet. It makes transactions completely safe even on a compromised or vulnerable computer. TREZOR provides the highest possible security for all Bitcoin and Litecoin users, even the non-technically savvy ones. Because the use of TREZOR is very easy and intuitive we believe it will help Bitcoin being adopted by common people.”* (Slush, 2013)

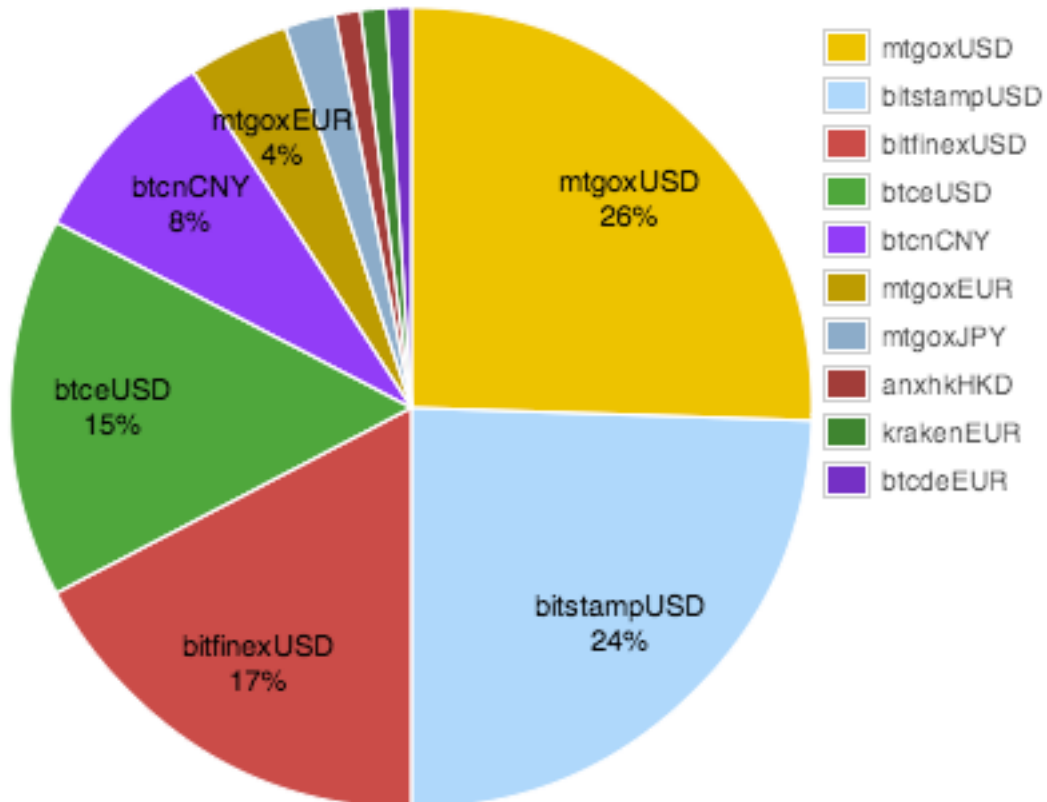
## 3.6 Exchanges

Because Bitcoin was gaining popularity and some people wanted to buy Bitcoin for normal fiat currencies such as USD some middleman in this type of transaction was in order to prevent fraud and dishonest users scam. The first online exchange where you could buy Bitcoins was MTGox.com. Nowadays there is a lot of online

exchanges because it is a very good business when you gain the trust of the (potential) users. Every exchange works on the same principal – they are the middlemen between two nodes where one user is willing to sell BTC and the second one is willing to buy BTC. Because exchange is the middleman and maintain the transaction there are some fees on both sides (it is mostly around 0.5% of the transaction). Selling BTC in online exchanges is faster than buying it because BTC transactions are processed faster than standard money bank transfer (mostly as SEPA for EU or abroad payments). Online exchanges don't support PayPal or paying with a credit card because these payments could be cancelled when somebody stole the credit card or hacked into someone's bank account and if the "hacker" would buy Bitcoins for this money, he could disappear without any steps to find him but the real money would go back to the schmuck that has been robbed.

## Exchange volume distribution

by market



(Bitcoin Charts, 2013)

### 3.6.1 MTGox.com

MTGox was the first Bitcoin online exchange, based in Tokyo, Japan. It was created in 2009 as a trading card exchange (Magic: The gathering cards) and in 2010 it was rebranded as a Bitcoin exchange. MTGox is an acronym to **Magic: The Gathering Online eXchange**. Jed McCaleb founded it and he sold MTGox in 2011 to **Mark Karpeles**. Under Karpeles ownership, the site grew to handle 70% of the world's bitcoin trades by April 2013.



Figure 9: Mt. Gox logo [source mtgox.com]

Bitcoin is known as a completely anonymous system, it is not true because every transaction could be tracked because the blockchain is visible to all. If somebody would use only Bitcoin that would be anonymous but if he is trading BTC for money there is always some name of a bank account that standard money will eventually have to be sent to. Because of (US) regulators MTGox was forced to be system that every user has to be verified to get money in USD (March 2013). Verified means that everyone has to send ID card, driving license or passport copy to MTGox and some utility bill as double check authentication.

#### 3.6.1.1 February 2014 hacking, losses, shutdown and bankruptcy

On **February 7**, MTGox announced that all BTC withdrawals are being halted.

On **February 17**, with all MTGox withdrawals still halted and competing exchanges back in full operation, the company published another press release indicating the steps they claim they are taking to address security issues. In an email interview with the Wall Street Journal, CEO Mark Karpeles refused to comment on increasing concerns among customers about the financial status of the exchange, did not give a exact date on which withdrawals would be resumed, and wrote that the exchange would impose "new daily and monthly limits" on withdrawals if and when they were resumed. More than 3000 users are still waiting to withdraw their money.

On **February 23**, Mark Karpeles, the CEO of MTGox, resigned from the board of the Bitcoin Foundation. The same day, all posts on their Twitter account were removed.

On **February 28**, MTGox filed for bankruptcy protection in Tokyo, and the company reported that the company had liabilities of about 6.5 billion yen (\$64 million at the time), and 3.84 billion yen in assets. The company said they had lost almost 750,000 of its customers' bitcoins, and around 100,000 of its own Bitcoins, totaling around 7% of all bitcoins, and worth around \$473 million near the time of the filing. MTGox released a statement saying "The company believes there is a high possibility that the Bitcoins were stolen," thus beginning a search for the missing money. Chief Executive of MTGox, Mark Karpeles, said technical issues opened up the way for fraudulent withdrawals. MTGox also faces lawsuits from its customers.

On **March 1**, Mark Karpeles had registered the domain Gox.com, but there are no certain facts about old MTGox and its money or about Gox.com

### 3.7 Bitcoin in the future

Many famous people in the world support Bitcoin system and some people started to be famous after entering Bitcoin. Mark "Slush" Palatinus has been interested in Bitcoin since 2009 and he is also the founder of the first pool mining, stratum (better protocol for mining) and last but not least the Bitcoin trezor. He is very famous in the Bitcoin community and he is from the Czech republic.

Winklevoss twins are interest in the bitcoin since 2012 and they are famous because they claimed that Mark Zuckerberg stole their idea of Facebook.com and won in court approximately 70 millions USD.

*Peter Thiel, co-founder of PayPal and famed Silicon Valley investor, has revealed he believes bitcoin could make some serious waves in the world of finance. Speaking at the Thiel Foundation Under 20 Summit in 2013, Thiel said he gave a talk back in 1999 that mentioned the end of monetary sovereignty and how encrypted money was going to "change the world". "I do think bitcoin is the first one of these that has the potential to do something like that," he added. The investor addressed the anti-bitcoin arguments that digital currency is "fake", a temporary "bubble" and "doesn't represent anything real" by stating that a lot of these arguments actually apply to the US dollar too. (Southurst, 2013)*

Bitcoin is completely decentralized so it can't be shut down by some government because it is against the rules; Russia is currently the country that is most against digital currencies. Based on history when media starts talking and

creating news about Bitcoin the price per one BTC would grow. But MTGox was the biggest exchange and for today it is still closed and many people lost a lot of money because of MTGox and some people starting to talk that what happened with MTGox will kill Bitcoin and many other currencies – different people say that this kind of thing happens only once and that this problem is just purification.

### 3.8 Hash algorithm

*A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string the cryptographic hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest. (Moore, 2013)*

The ideal cryptographic hash function has four main properties:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.

*Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for more general functions with rather different properties and purposes. (Muljadi, 2012)*

Bitcoin network use SHA256 (Secure Hash Algorithm) that has been developed by National Security Agency in 1993. It doesn't need a lot of memory or fast memory clock to compute these hashes and that is also the reason that people have optimized ASIC chips for mining on SHA256. The second most used hash algorithm is called Scrypt. Scrypt is a password-based key derivation function created by Colin Percival, The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. Scrypt is used as a proof-of-work scheme by a number of crypto currencies, such as Litecoin.

## 4 Analytical part

### 4.1 Bitcoin vs. other currencies

Bitcoin was the first decentralized digital currency, in other words Bitcoin is sophisticated network software under open-source license so anyone may look in its code. Because downloading and modifying the code is free a lot of people got inspired and created their own digital currency, some of them are very close to the original Bitcoin idea but there are also some that are completely modified. During the development of Bitcoin open-source Satoshi Nakamoto chose properties for the Bitcoin network as that hashing algorithm would use **SHA256D**, time to confirm transaction would take approximately 10 minutes (as well as finding new block) or that 21 millions is the final number of all Bitcoins. It is easy to modify these properties so many people did it and created new and new digital crypto currencies.

There are many variations of digital currencies nowadays such as Bitcoin, **Litecoin**, **Dogecoin**, Peercoin, Namecoin, Quark, Protoshres, Worldcoin, Megacoin, Primecoin, Sexcoin, Casinocoin, **Auroracoin**, Devcoin, Fastcoin, 42coin or Craftcoin... The number of

digital currencies to January 2014 is close to one hundred.



Figure 10: Bitcoin logo [source: [bitcoin.org](http://bitcoin.org)]

#### 4.1.1 Litecoin - LTC

Litecoin is currently considered as number two in digital currencies. It is called as “silver” to “gold” as Bitcoin. Litecoin is different from Bitcoin mainly in hashing algorithm; it uses **scrypt** (Bitcoin use SHA256D). For Scrypt algorithm is currently not possible to create specialized mining hardware (ASIC) because it needs more memory for hashing than SHA256D and memory is one of the more expensive stuff on GPU cards. One could say that SHA256D is only profitable on



Figure 11: Litecoin logo [source: [litecoin.org](http://litecoin.org)]

ASICs based miners but currencies that are using scrypt algorithm could be still mined on and only GPUs. Market capitalization is approximately 10 times lower than Bitcoin network.

#### 4.1.2 Peercoin – PPC

Third most know digital coin is named Peercoin and has market capitalization about one hundred times less than Bitcoin. Peercoin uses the same hash algorithm as Bitcoin but its network solves a lot of negative properties from Bitcoin. Peercoin is based on “**proof-of-stake**” and “**proof-of-work**” and solves the issue when one entity has more than 51% of hashing power in the network (if one entity has more than 51% of hash power in Bitcoin network he could “create” own blockchain and jeopardize whole network). In Peercoin network the entity must have 51% of all Peercoins and for that you would need much more money than buying hardware for a big hash rate.

Creators of this crypto currency also made 1% inflation every year, that means that every year there is 1% more PPC in the network – this mean a theoretically longer lifetime of the currency.



Figure 12: Peercoin logo [source: peercoin.org]

#### 4.1.3 Namecoin – NMC

Namecoin is known as the fourth most valuable digital currency and it has approximately half the capitalization market than the Peercoin network. Main purpose of NMC is to serve as a completely **decentralized system for new DNS** – this purpose solves censorship and tries from government agencies that may easily shut down every page that is against the rules.



Figure 13: Namecoin logo [source: wikimedia.org]



Namecoin is using .bit domain and is possible to use for authentication on the Internet, torrent tracker or instant messaging.

#### 4.1.4 Dogecoin – DOGE

Dogecoins have been created in December 2013 and compared to other digital currencies has very fast initial coin production, in the end of 2014 there should be 100 billions DOGE and then only 5 billions per year. The most known fact about DOGE is that in their logo or memes they are using Shiba Inu (type of dog). This currency belongs to one of the newest (when writing this thesis) but it gained popularity almost immediately and became one of the most profitable digital currency for mining (December 2013 till March 2014). It gained huge popularity because of the memes with Shiba Inu.



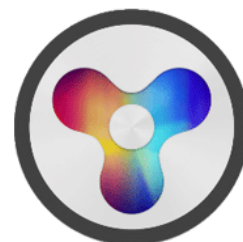
Figure 14: DOGE meme [source: dogecoin.com]



Figure 15: Dogecoin logo [source: dogecoin.com]

#### 4.1.5 Quark – QRK

One of the most interesting digital currencies that have been created yet. Its market capitalization is almost the same as Namecoin. Quark is distinguished in its unique security in hash algorithm that it uses. NSA (National Security Agency) in USA made tremendous steps in informatics and there are rumors that they are capable of breaking some hash algorithms that were considered very secure some time ago. For example if somebody breaks a Script hash algorithm it would be almost possible for him to generate new coins and he would have a certain advantage in the network and also the network would be in jeopardy. Creators of Quark completely redesigned security protocols and Quark is functioning with nine hashing rounds using six hash



**QUARK COIN**

Figure 16: Quark coin logo [source: qrk.cc]

algorithms in random order (Blake, Blue Midnight Wish, Grøstl, JH, Keccak, SHA-3 and Skein).

#### 4.1.6 Auroracoin - AUR

Digital currencies were gaining popularity all over the world and Auroracoin is the first decentralized currency that is released by Island (country in Europe). It is a derivation of Litecoin; the huge difference between these currencies is that Auroracoin is “pre-mined” by 50% and these “pre-mined” coins are supposed to be obtained by Island citizens, each should receive around 31 AUR, this day is being planned on 25 March 2014 and it is called “Airdrop” (unfortunately this date is after the Bachelor thesis due date). This small amount of coins should have pumped market capitalization and the rest of the coins will be mined normally by miners.



Figure 17: Auroracoin logo [source [auroracoin.org](http://auroracoin.org)]

## 4.2 Altcoins summary

That was just a small list of other digital currencies. The expectation is that many digital currencies will perish, because a lot of them are only differently branded Bitcoin or some other coins. They will perish because the community will not accept them, miners will be mining much more popular currencies or the security protocols (blockchain) will be breached and if the community doesn't want to use that currency it would be just a piece of software.

**Table 1: Alternative currencies comparison**

<b>Crypto currency</b>	<b>Hash algorithm</b>	<b>Confirmations (new blocks)</b>	<b>Total amount of coins</b>	<b>Special</b>	<b>Official page</b>
<b>Bitcoin</b>	SHA-256	10 min	21 millions	First digital currency	Bitcoin.org
<b>Litecoin</b>	Scrypt	2.5 min	81 millions	First Scrypt currency	Litecoin.org
<b>Peercoin</b>	SHA-256	60 min	Unlimited	1% inflation, more secure and “green” to environment	Peercoin.net
<b>Namecoin</b>	SHA-256	-	21 millions	Decentralized system for DNS, domain .bit	Namecoin.org
<b>Dogecoin</b>	Scrypt	1 min	Unlimited	100 billions to end 2014, then 5 billions annually	Dogecoin.com
<b>Quark</b>	Six hash algorithms	30 sec	Unlimited	Very secure	Qrk.cc
<b>Auroracoin</b>	Scrypt	100 blocks		50% of coins are pre-mined	Auroracoin.org

## 5 Results and discussion

Bitcoins and other alternative digital currencies have been analyzed and in this chapter there is information about the practical part of this bachelor thesis.

### 5.1 Hardware research

The first part was to find the best hardware for mining on the Internet. On the current market (Internet) there are many types of hardware with different parameters and different prices.

Price range for the mining investment was defined at around 1000 USD to 1200 USD (approximately 20K – 25K CZK) and then seeking for the most profitable hardware begun. Because digital crypto currencies are very new in this world and there is no precedent of how they will develop in the future so the money that was invested must return as soon as possible. From Bitcoin analysis it was determined that mining on the best CPU of nowadays is still much more slower than mining on GPUs or ASICs. Between defined price ranges it is not possible to find an miner that could mine hash algorithm based on scrypt or SHA256 simultaneously. FPGA cards are behind the price range it was decided that GPUs would be bought. According to mining hardware comparison for hash algorithm SHA256, available [https://en.bitcoin.it/wiki/Mining\\_hardware\\_comparison](https://en.bitcoin.it/wiki/Mining_hardware_comparison) and hardware comparison for scrypt mining, available on [https://litecoin.info/Mining\\_hardware\\_comparison](https://litecoin.info/Mining_hardware_comparison) there is no possibility to mine on SHA256 within price range around 1000 USD with soon (or even later) return of initial investment. Mining Bitcoins (SHA256) on non-ASIC devices is not profitable and mining digital currencies based on scrypt algorithm is still profitable. (uraymeiviar, 2014)

Disadvantage of the GPU mining is that you have to put the graphic card in some computer so there is need to think that GPU is the only thing to be bought but the CPU, motherboard, RAM, memory medium for running OS and power supply. Keyboard, mouse and monitor are required for mining so it is omitted in this thesis and for setup spare monitor and keyboard will be used. For the miner to be most profitable and have low initial cost there are only two components that matters. First you need a GPU that is profitable and second component is efficient power supply.

Other components to get the miner (computer) running are irrelevant and could be some low cost (budget) they just need to work properly.

### 5.1.1 Hardware searching

Albert Einstein said, *“If I had one hour to save the world, I would spend 55 minutes defining the problem and only five minutes finding the solution.”* (Einstein, 2011) This part of the thesis took a very long time because there are many various computer parts and many retail sellers.

#### 5.1.1.1 GPU

Graphic card is the most important part of the miner as it determines how fast it is possible to find (theoretically) new blocks. This speed is measured in kHash/second in scrypt-based mining and in MHash/s for SHA256 mining algorithm. Hashing is done only in graphic core and graphic memory so that is why all other computer components are irrelevant.

According to hardware research the best options for mining on GPUs are cards from ATI (AMD) than from nVidia. These two graphic cards core manufacturer have different architecture and ATI's cards are 3 to 5 times faster for hashing job (in scrypt and SHA256).

*Firstly, AMD designs GPUs with many simple ALUs/shaders (VLIW design) that run at a relatively low frequency clock (typically 1120-3200 ALUs at 625-900 MHz), whereas Nvidia's microarchitecture consists of fewer more complex ALUs and tries to compensate with a higher shader clock (typically 448-1024 ALUs at 1150-1544 MHz). Because of this VLIW vs. non-VLIW difference, Nvidia uses up more square millimeters of die space per ALU, hence can pack fewer of them per chip, and they hit the frequency wall sooner than AMD which prevents them from increasing the clock high enough to match or surpass AMD's performance. This translates to a raw ALU performance advantage for AMD:*

*AMD Radeon HD 6990: 3072 ALUs x 830 MHz = 2550 billion 32-bit instruction per second*

*Nvidia GTX 590: 1024 ALUs x 1214 MHz = 1243 billion 32-bit instruction per second*

Secondly, difference between these two manufacturers is that AMD cards are able to work with 32-bit integer right rotating operations in one hardware instruction but Nvidia cards has to emulate it through three hardware instructions. (Tom van der Woerdt, 2013)

Top winning cards in this category were: ATI Radeon R9 290x, R9 280x, R9 270x, ATI Radeon HD 7870, HD 7850 or 7970. It was chosen according to their hashrate, power consumption and price. These parameters are different among graphic card manufacturer so in table are listed mean values.

**Table 2: Modern GPUs comparison**

GPU	kHash/s	Power consumption (W)	Price in CZK
R9 270x	380	150	5000
R9 280x	700	300	7500
R9 290x	750	450	15000
HD 7850	360	130	5000
HD 7870	400	200	5300
HD 7970	750	270	9000

The Multiple criteria decision method with points was used to determine the most profitable GPU. According to the first table points were distributed by its impact to mining. The winner from the table is supposed to be the one that has lower points and the biggest value in “hash rate total”.

**Table 3: Multiple criteria decision**

GPU	Hashrate	Power consumption	Price in CZK	How many cards	Sum points	Multiply points by number of GPU	Hash rate total
R9 270x	4	2	1,5	3	10,5	31,5	1140
<b>R9 280x</b>	2	4	3	2	11	22	1400
R9 290x	1	6	5	1	13	13	750
HD 7850	5	1	1,5	3	10,5	31,5	1080
HD 7870	3	3	2	3	11	33	1200
HD 7970	2	5	4	2	13	26	1480

Winner, for the most profitable GPU, is **ATI Radeon HD R9 280x**. Because if there is money in the budget could be spent on two of those graphic cards and there would be still money left for other computer parts.

#### *5.1.1.2 Power supply*

Efficient and quality power supply is very important for mining because the mining rig is supposed to run 24 hours a day for as long as possible. Because two graphic cards R9 280x were chosen and they have the power consumption around 600 watts together the power supply has to be at least 650W because 600W is only for GPUs but CPU, motherboard and RAM are consuming some power too (it should be definitely less than 100W).

Some manufacturers are producing power supply that they put label 600 Watts on it but the power supply is not enough strong to produce 600W or the efficiency could be under 50% so 600W power supply could consume 1kW electricity. For this purposes there is certification 80 Plus – that mean if some power supply is able to fulfill some criteria it could be certified and it is not easy to meet this criteria and if power supply success in the testing the manufacturer is happy that he can use this logo certification. 80 Plus certifies products that have more than 80% energy efficiency and this is very important for computers that runs 24/7.

Standard energy cost in Czech republic is 5 CZK per kW/hour but if you have better tariffs you could have lower costs. The mining rig will be placed in the place where energy is not for free and it cost around 5 CZK per 1 kW/hour. Suppose that 600W PSU with 50% energy efficiency were bought (estimated price 1300 CZK) and mining rig will be running 24/7. Because the PSU is only 50% energy efficient it will consume 900W energy. Final cost will be 4,5 CZK per hour – 108 CZK per day and 3240 CZK per month. Second option is to buy much more efficient power supply – suppose we bought 600W PSU with 80% energy efficiency and cost were 3000 CZK. The PSU will consume 720W because of 80% energy efficiency and one hour mining will cost 3,6 CZK – one day 86 CZK and cost for one month mining would be 2592 CZK. Difference between theses PSUs running 24/7 is 650 CZK per month so if the mining will be more than 3 months it is better to buy more expensive PSU with at least 80% energy efficiency.

According to the Internet research about power supplies one of the best PSU for mining (or just running 24/7) is from Corsair manufacturer and it is named GS700. Unfortunately GS700 is no longer available so his successor was chosen – **Corsair RM850**. This PSU is 850W so there is possibility to add one more 280x graphic card in future and it is certified with 80 Plus Gold (that means 90% power efficiency). This PSU cost approximately 3000 CZK.

#### **5.1.1.3 Rest of components**

As it was mentioned before – rest of the computer part could be low-end models that are inexpensive. These components are just to make GPUs running.

#### **5.1.1.4 Motherboard**

Two GPUs with power consumption 600W and one PSU 850W so there is reserve for one more 280x card for future. PSU is 850W but every 80 plus certified PSUs have overload test so this PSU could work on 120% - that is 1020W. Graphic cards are supposed to be in PCIe 16x slots that means that motherboard has to contain at least three PCIe 16x slots and because every modern powerful graphic card is heating when working, they are fitted with coolers that exceeds more than one slot on motherboards (suppose standard ATX format) – GPUs are with double slot coolers – PCIe slots on MB cannot be exactly under each other, they have to be spaced one slot from each other.

With these parameters the cheapest motherboard is currently **MSI Z77A-G45** according to heureka.cz and its price is 2300 CZK.

#### **5.1.1.5 CPU**

Suppose MSI Z77A-G45 motherboard have been chosen and it needs a CPU. Socket of this MB is Intel LGA 1155 and the cheapest processor according to heureka.cz is **Intel Celeron G1610 @ 2.6 GHz**.

#### **5.1.1.6 RAM, HDD, flash drive**

MB that was chosen also needs RAM and slots on the MB are DDR3 type. The cheapest memory for it is currently **Kingston KHX1333C9D3B1K2** with price 1300 CZK. It is 4GB kit (2 x 2GB). Actually mining rig should have at least 2 GB RAM to get running but in RAM kit is better ratio between price per GB.



For running operating system Windows we need to have HDD or SSD, currently it is still cheaper to use some normal hard drive – the cheapest is for 1200 CZK in SATA 2 slot. If mining rig will be running on Linux it is possible to use flash drive – price 300 CZK for 16 GB.

Somebody could say that computer must be in some case but graphic cards are going to heat a lot and case would just make air flow much worse so it is better to leave motherboard with GPUs outside the case. Motherboard that has been chosen is without buttons on MB that are for start or restart of the system, in standard conventional way it doesn't matter because buttons are on PC case but without case it is only possible to start the system by creating short-circuit on designated pins. Short-circuit is done by connecting these two pins together with some conductive thing – like screw driver.

### 5.1.2 Building mining rig

Computer components were chosen and ordering them was the next thing to do. Components were bought through czc.cz e-shop and final costs were 22 500 CZK.

Table 4: Used components

Component name	Price in CZK
ATI Radeon R9 280x	15 000
Corsair RM850	3 000
MSI Z77A-G45	2 300
Intel Celeron G1610 @ 2.6 GHz	900
Kingston KHX1333C9D3B1K2	1 300
USB flash drive 16 GB	300
<b>Total price</b>	<b>22 800</b>

All components are compatible and fit in the designed slots on the motherboard so connecting these parts is easy as building a cube from LEGO blocks. Time duration for accomplishing this quest was around 15 minutes.

## 5.2 Software setup

The mining rig has been successfully built and was able to boot BIOS – that means all the computer parts are operational.

Next step was to find the operating system for mining. There are two options and both have been tested. First option is to use Linux as the operating system and the second is Microsoft Windows. There is no correct answer for what is better – these systems are different and everyone possesses something special that the other doesn't.

Table 5: Linux vs. Windows mining

OS	Linux	MS Windows
<b>Price</b>	Free	Licensed
<b>Monitoring</b>	SSH, mining stats	No default SW
<b>Stability</b>	Stable	More stable
<b>Users</b>	For advanced users	For amateurs
<b>OS storage</b>	USB flash drive (4 GB)	HDD

### 5.2.1 Linux mining

Linux operating systems are mostly for more advanced computer users (it is not Windows and works differently). There are many advantages for example Linux could be controlled remotely via SSH (command line via network) but in need it could posses RDC (remote desktop connection that is used in Windows for remote control).

Linux is mostly distributed as an open-source SW and there are many Linux distributions (Debian, Ubuntu, Opensuse, Backtrack...). Because Linux is an open-source some advanced programmers have created Linux distributions that are exactly for mining purposes. First linux distribution for mining purposes was BAMT (Big A Miner Thing) and was created for mining SHA256 hash algorithm on GPUs with CGminer. It is not efficient to mine SHA256 on GPUs so some programmers recreated BAMT ([guiminer.net/bamt](http://guiminer.net/bamt)) to work with scrypt hash algorithm and named it SMOS Linux ([www.smos-linux.org](http://www.smos-linux.org)). SMOS linux is free for usage but there is only a donation procedure that every day for three minutes miner will be mining for

developers of this Linux but this donation may be easily removed (even developers accept that, it is just turned on by default).

Linux OS is possible to run from a USB flash drive (in case of SMOS 4 GB is required). To run SMOS there is a little guide for start:

- I. Download SMOS at [www.smos-linux.org](http://www.smos-linux.org)
- II. Suppose we downloaded SMOS to Windows OS and we need to create USB stick with SMOS. In Windows we need special program for creating bootable flash drive with Linux, recommended program is Win32diskimager that is free and available at <http://sourceforge.net/projects/win32diskimager/files/latest/download>
- III. Start Win32diskimager. Select the downloaded IMG file and target device, and click Write.
- IV. When it is finished, remove USB drive and put it in mining rig.
- V. Start the mining rig and set in BIOS booting from flash drive – if successful mining rig boot to SMOS Linux

When running SMOS Linux the setup for miner could be done without monitor attached directly to mining rig – it is possible through SSH if we know the IP address of the mining rig (could be discovered through a router, dhcp server or network discovery program). In script mining it is mandatory to do setup of graphic cards that are used. It will be detailed discussed in chapter Mining optimization. For now suppose successful finish as login through SSH to mining rig.

### 5.2.2 Windows mining

Building a mining rig that will run on Microsoft Windows is slightly different than on Linux based rig because Windows has to be installed on HDD or SSD unit and they cannot run from cheap flash drive.

Windows always has to be licensed because it is a proprietary software of Microsoft. Because CULS (ČZU) offers free Microsoft products to their students through Dreamspark premium accounts the student version of Windows have been used (totally free). There are three versions of Windows – Win XP, Win 7 and Win 8. Choosing Windows XP is not very smart because it's a 13 year old system and in April 2014 there will be no support for this system. Windows 8 boots to Metro GUI instead of classic desktop environment as Win 7 and many users hate that. Windows

8 and Windows 7 are almost the same and work the same so the choice is what is user-friendly. Windows 7 were used because of empirical experience and because they boot to desktop environment by default.

Windows is an operating system for many various types of people and for many user types. All the programs designed for mining have to be installed otherwise mining on GPU just will not start. Suppose that installation of Windows 7 64-bit on HDD was successful, all security updates were installed and system is fully operational. It is goof to set automatic login because when the system will reboot by unpredictable reason it will not ask for login credentials. For mining 24/7 the system has to be set to never go to sleep or hibernation because the system will be in idle (no mouse movement or keyboard activity) and the default option is that computer will sleep after 30 minutes in idle.

#### **5.2.2.1 GPU drivers and SDK**

Windows 7 has some generic drivers for GPUs – that means that for showing info on screen it works just fine but for mining is required (the newest) drivers and SDK from manufacturer. Driver is just piece of software that connects hardware with operating system and these drivers are free to use and for downloading too. Drivers for GPUs were available at [www.amd.com](http://www.amd.com). Because this GPU driver is just for managing GPU in standard way and mining is still unconventional the APP SDK has to be downloaded and installed too.

*AMD Accelerated Parallel Processing (APP) SDK technology is a set of advanced hardware and software technologies that enable AMD graphics processing cores (GPU), working in concert with the system's x86 cores (CPU), to execute heterogeneously to accelerate many applications beyond just graphics. This enables better-balanced platforms capable of running demanding computing tasks faster than ever, and sets software developers on the path to optimize for AMD Accelerated Processing Units (APUs). (AMD - ATI Technology, 2013)*

#### **5.2.2.2 Mining program**

Installing the driver and APP SDK has been successful and time for choosing and installing program for mining is in order. There are many programs for mining – some of them have a lot of in common and some works very differently. Most

recommended and discussed is CGMiner. There are many versions of this mining program – the most stable version is 3.7.2 and it is the last CGMiner version that supports GPU mining (version 4.0 is available from February 2014 but doesn't support GPU). CGMiner is program that is free and available at <http://ck.kolivas.org/apps/cgminer/>. There is no need to install this program; it runs from folder without installation.

### 5.2.2.3 System monitoring

If the mining rig is mining and hasve some connected monitor (display) – rendering the images to the monitor could cause that the one graphic card will run a little bit slower so it is better to unplug monitor after Windows is fully set up. In the future it may be necessary to connect to that rig and troubleshoot or just to check temperatures of graphic cards or current work in CGMiner. For this purpose is the best way TightVNC it is a free program available at [tightvnc.com/download.php](http://tightvnc.com/download.php). The built in Remote desktop in Windows is messing with GPUs when they are mining so it is better to use TightVNC.

If everything was installed properly the best way to prove it is to reboot the system and check if some errors come up – in this case they did not.

## 5.3 Solo mining

Bitcoin is the first digital decentralized currency; it was created so that miners will do the hard work instead of some banks. Satoshi Nakamoto expected that there will be a lot of miners and everyone will work solo but working solo when the hashrate of the network is very high and still climbing is like winning the lottery to find new blocks. Average time to find new block is in this formula:

$$\text{average time (seconds)} = \frac{(\text{current difficulty}) * (2^{32})}{\text{hashrate}}$$

With 1 giga hashrate in bitcoin network it would take in average over 1000 years to find new block so it is a better chance of winning in lottery.

Solo mining is efficient only in the new digital currencies where the hashrate is still low and it is not so hard to find new blocks. There is no way how to determine if this new currency will be successful and mining solo in Litecoin network is just unprofitable.

## 5.4 Pool mining

*Pooled mining is a mining approach where multiple generating clients contribute to the generation of a block, and then split the block reward according to the contributed processing power. Pooled mining effectively reduces the granularity of the block generation reward, spreading it out more smoothly over time.* (Nanotube, 2014) Mining in pool are simply many people together that mine as one user and the reward for the block is distributed by some factors (there are many reward systems).

The idea of mining in pool came from Czech guy named Marek Palatinus (in bitcoin community known as Slush), because in the early ages of Bitcoin the hashrate of the network started to grow when it became popular and it was very unpredictable how fast you will find new blocks. Slush made the first pool mining ever (released in December 2010) and it is still operational on <http://mining.bitcoin.cz/>.

Work for miners, in earlier time, has been distributed over Getwork protocol but it was very inefficient and consumed a lot of resources of server where the pool software was running. Getwork protocol was based on HTTP request. Over some time miners were starting to mine in pool because you would get your “average” money for your hashrate and mining stopped being a lottery. Because Getwork protocol was inefficient Slush designed a new protocol called Stratum and distributed it with an open-source license (March 2013).

*In a simplified manner, Stratum is a line-based protocol using plain TCP socket, with payload encoded as JSON-RPC messages. That's all. Client simply opens TCP socket and writes requests to the server in the form of JSON messages finished by the newline character \n. Every line received by the client is again a valid JSON-RPC fragment containing the response.* (Slush, 2013)

### 5.4.1 Reward system

As pool mining was getting popular a new reward system was designed and implemented in pools. There are currently over 10 rewarding systems. About some rewarding methods it is not possible to say which one is better over some different rewarding method but there are also rewarding methods that have been proven to be very inefficient during some time.

#### *5.4.1.1 Proportional*

The proportional system is perhaps the simplest pooled mining reward system, and the one that, intuitively, seems to best capture the principles of pooled mining. In this system, payments are calculated based on a division to rounds, where a round is the time between one block found by the pool to the next. At the end of every round, when a block is found and the pool receives a reward of a block, the operator keeps a fee of  $f \cdot B$ , and  $(1 - f) \cdot B$  are distributed among the miners, in direct proportion to the number of shares they submitted during this round. If a miner submitted  $n$  shares in this round, and the total number of shares submitted to the pool during this round is  $N$ , then his payout for this round will be  $n / N \cdot (1 - f) \cdot B$ .

This reward method has proven to be inefficient because it doesn't expect some dishonest miners and because of that honest miners are less rewarded.

#### *5.4.1.2 PPS*

Each share receives a fixed reward known in advance. This is the ultimate low - variance, low - maturity simple method, but has the highest risk for the operator, and hence lower expected returns than other methods and risk of collapse if not managed properly. It is currently only moderately attractive, but is the way of the future - it will be the most widely used method when the infrastructure to offer it with low fees is established.

#### *5.4.1.3 PPLNS*

Block rewards are distributed among the last shares, disregarding round boundaries. In the accurate implementation, the number of shares is determined so that their total will be a specified quantity of score (where the score of a share is the inverse of the difficulty). Most pools use a naive implementation based on a fixed number of shares or a fixed multiple of the difficulty. The share-variance can be reduced at the cost of increased maturity time, but there is no way to decrease the long-term pool-variance. All implementations cannot be hopped using traditional methods. However, only the accurate implementation is hopping-proof against difficulty adjustments. This rewarding method belongs to one of the best for mining on one pool 24/7.

## 5.5 Pool & currency decision

Choosing a pool and which digital coins are going to be mined is one of the important factors of how much money could be received in the future. There are many online calculators that calculate how much money you receive during some period of time. Nobody knows the future and it is hard to predict what is going to be in one month (the digital currency could be dismissed or the price could just get lower and lower but because nobody knows the future it may be exactly the opposite. One of the most favorite calculators is available at <http://dustcoin.com/mining>. One could choose a time interval that is interesting, and then choose the hashrate and even the price for electricity and power consumption. Nobody is an oracle to predict the future so for mining on short term basis (returning initial investment as soon as possible) the best way is to calculate for period of time as one day (24 hours). In this figure the hashrate of two GPUs together that were selected is 1400 kHash/s. Price and power consumption is omitted.

### Cryptocoin Mining Information







Coin	Algo	Difficulty	Price	Ratio	Revenue	Profit
			BTC	vs. BTC or LTC	Coins / Day	USD / Day
 <b>Bitcoin</b>	SHA-256	3815723798	1.00000000	100.00%	0.00018	\$0.12
 <b>Litecoin</b>	scrypt	3636.52	0.02480045	100.00%	0.387	\$6.35
 <b>PPCoin</b>	SHA-256	99555079	0.00536441	82.33%	0.0283	\$0.10
 <b>Dogecoin</b>	scrypt	1002.003	0.00000157	114.88%	7027	\$7.28
 <b>Namecoin</b>	SHA-256	3070377120	0.00570823	1.42%	0.00046	+\$0.00
 <b>Feathercoin</b>	scrypt	230.275	0.00036140	92.05%	24.5	\$5.86

Table 6: Bitcoin vs. Altcoins [source: dustcoin.com]

This figure is comparison of a few currencies, every SHA256 coin is calculated to Bitcoin and scrypt coins are calculated to Litecoin. In the last column is information about **profit** per 24 hours (without power consumption). If mining Bitcoin on two 280x GPUs the profit per day is 0.12 USD and it is very bad but if mining LTC the profit would be 6.35 USD and it is good. According to this figure the best currency for now is **Dogecoin** with 7.28 USD profit per day. It is should not



be called profit yet because it was calculated only by money received (estimated) and that is named revenue.

Mining in pool means that many users are connected in one node that mine solo – that means that bigger pools with higher hashrates have more probability to find new blocks more often.

**Table 7: Dogecoin pools**

Net %	Hashrate	Miners	Pool
<b>24.7%</b>	22923mh/s	23102	Dogehouse.org
<b>15.3%</b>	14141mh/s	11836	Fast-pool.com
13.1%	<b>12131mh/s</b>	<b>7402</b>	<b>Multipool.us</b>
<b>6.0%</b>	5568mh/s	4942	Doge.hashfaster.com
<b>5.4%</b>	4962mh/s	4567	Suchcoins.com

If there is some entity in the network that has hashrate over 51% it could confirm their transactions and doesn't need the rest of 49% of the network. This is one of the most dangerous potential threads in pooled mining. To avoid that it is better to mine at some lower hashrate pools and support them.

Multipool.us was chosen because it has the third best hashrate (sometimes it is on second position) in mining DOGE and it supports many other digital currencies to mine so if DOGE will stopped to be the most profitable currency it is much easier to switch on different currency within one pool than creating registration to other pool and then start mining. Multipool.us also supports multi currency mining – that means that they have sophisticated system that may switch to most profitable currency in real time and when it will stop being most profitable it will change to mine different currency. The profitability is calculated each minute and according to its decision the pool would make decision. Mining just one currency is simpler than maintaining a lot of different currencies because there is a need to have for every digital currency a different wallet and with multipool there is a big probability that more than 10 types of wallets would be required. It is possible to use online wallets for example at Cryptsy exchange but these online coin storages are more likely to be hacked and robbed than the wallets on a computer. DOGE currency was chosen to start with and changing to a different currency is not hard on multipool.us.

## 5.6 Miner optimization

In script mining there are a lot of settings that must be set up for each different GPU manufacturer and settings for each GPU model could be different. ATI and NVidia are only companies to develop and create graphic cores but different manufacturers like Sapphire, MSI, Asus... makes the rest of the card and set up clock of the core, memory clock, how many memory would the graphic card has etc. Each model has a little different name in this case these cards were chosen **MSI R9 280X GAMING 3GB / Radeon R9 280X**. For determining the best setting for the GPU is best to visit [https://litecoin.info/Mining\\_hardware\\_comparison](https://litecoin.info/Mining_hardware_comparison) and search the exact model. Setting for the GPU on this page doesn't have to work the same way for you because it depends even a little on the CPU, MB but mainly on which operating system is in use. If wrong setting has been entered the miner will restart from time to time or just freeze, it is very unlikely that the card would be destroyed (if it wasn't overclocked to crazy extreme values). Appropriate settings for this card is to use cgminer 3.7.2, overclock the core to 1100 MHz, memory clock to 1500 MHz and setting for mining to “-g 2 -w 256 --thread-concurrency 24000”. Overclocking in cgminer is possible by writing “-gpu-engine 1100” and for memory clock “-mem-clock 1500” overclocking this way is possible because of the APP SDK that were previously installed. Values for mining settings is very different among GPUs and the “-g 2” stands for GPU thread, “-w 256” is work size and thread concurrency is shortly like the capacity of doing multiple things at the same time. Total cgminer setup for this rig is:

```
timeout /t 30
```

```
setx GPU_MAX_ALLOC_PERCENT 100
```

```
setx GPU_USE_SYNC_OBJECTS 1
```

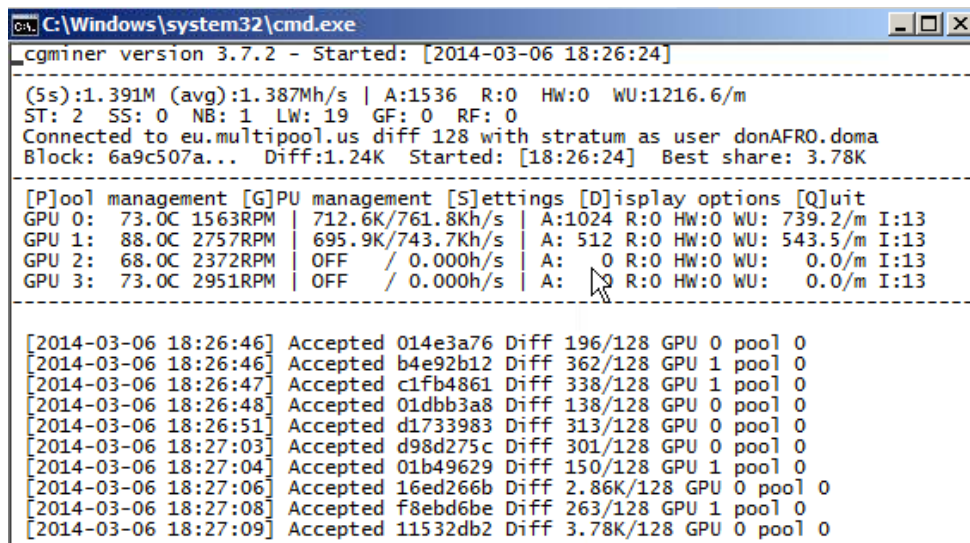
```
cgminer --script -o stratum+tcp://eu.multipool.us:3352 -u donAFRO.doma -p  
prase --failover-only -o stratum+tcp://doge.hashfaster.com:3339 -u  
donAFRO.doma -p prase -I 13 -g 2 -w 256 --thread-concurrency 24000 -gpu-  
engine 1100 -mem-clock 1500
```

This text is supposed to be stored in .bat file (script usage in Windows) and the best way to mine 24/7 is save this file to Startup folder because in case that mining rig reboots the mining script will continue. Password for miners is irrelevant because this credential is registered in some pool that is locked to some pay out

address and if somebody knows this password is not important. If multipool.us will fail there is also a set of secondary mining pools at doge.hashfaster.com.

Overclocking the card may harm the card so it is done on own risk only and mostly the warranty is violated by it, but overclocking the card is good to get bigger hashrate but it consumes a little bit more power.

Miner was setup properly and it was time to start mining. When the mining process start one could notice of heating of GPU because they started working on 100% (possibly on 110% if overclocked). It is more likely if the miner stay “live” for 24 hour that it could make it for longer time, if improperly settings were chosen it should be obviously sooner than in 24 hours. Even with perfect settings many other things could go wrong for example the PSU doesn’t handle the load for 24/7 or GPU may overheat because of very bad airflow, cgminer is clever program that expect overheating and in default if GPU temperature exceeds 95 degrees (Celsius) the rig will reboot or when the temperature is approaching to the maximum value the program load the GPU with less work to prevent the high temperature.



```
C:\Windows\system32\cmd.exe
cgminer version 3.7.2 - Started: [2014-03-06 18:26:24]
-----
[Ss]:1.391M (avg):1.387Mh/s | A:1536 R:0 HW:0 WU:1216.6/m
ST: 2 SS: 0 NB: 1 LW: 19 GF: 0 RF: 0
Connected to eu.multipool.us diff 128 with stratum as user donAFRO.doma
Block: 6a9c507a... Diff:1.24K Started: [18:26:24] Best share: 3.78K
-----
[P]ool management [G]PU management [S]ettings [D]isplay options [Q]uit
GPU 0: 73.0C 1563RPM | 712.6K/761.8Kh/s | A:1024 R:0 HW:0 WU: 739.2/m I:13
GPU 1: 88.0C 2757RPM | 695.9K/743.7Kh/s | A: 512 R:0 HW:0 WU: 543.5/m I:13
GPU 2: 68.0C 2372RPM | OFF / 0.000h/s | A: 0 R:0 HW:0 WU: 0.0/m I:13
GPU 3: 73.0C 2951RPM | OFF / 0.000h/s | A: 0 R:0 HW:0 WU: 0.0/m I:13
-----
[2014-03-06 18:26:46] Accepted 014e3a76 Diff 196/128 GPU 0 pool 0
[2014-03-06 18:26:46] Accepted b4e92b12 Diff 362/128 GPU 1 pool 0
[2014-03-06 18:26:47] Accepted c1fb4861 Diff 338/128 GPU 1 pool 0
[2014-03-06 18:26:48] Accepted 01dbb3a8 Diff 138/128 GPU 0 pool 0
[2014-03-06 18:26:51] Accepted d1733983 Diff 313/128 GPU 0 pool 0
[2014-03-06 18:27:03] Accepted d98d275c Diff 301/128 GPU 1 pool 0
[2014-03-06 18:27:04] Accepted 01b49629 Diff 150/128 GPU 1 pool 0
[2014-03-06 18:27:06] Accepted 16ed266b Diff 2.86K/128 GPU 0 pool 0
[2014-03-06 18:27:08] Accepted f8ebd6be Diff 263/128 GPU 1 pool 0
[2014-03-06 18:27:09] Accepted 11532db2 Diff 3.78K/128 GPU 0 pool 0
```

Figure 18: cgminer output

First two GPUs in the output are R9 280x from this thesis and the rest is R9 270x that has been added later and are not discussed in this thesis. From the output it is easy to see current temperature of GPUs cores (78 and 91 Celsius degrees), the second card is more hot because is close to the other GPU that blocks a

little the fan and there is also lower airflow. Both of the cards are hashing at 700 kHash/s.

## 5.7 Electricity costs and investment return

Calculating electricity consumed is a little bit tricky because there is not easy way to determine it without Wattmeter. Because the electricity cost doesn't have to be calculated precisely it is enough to calculate estimated electricity cost. Suppose our mining rig consumes 600W and PSU is 90% energy efficient. Power consumption =  $600 * 1.1 = 660$  W. Power cost per 1 kWatt/hour is 5 CZK. One hour mining on rig with two 280x cost  $660/1000 * 5 = 3.3$  CZK – 24 hour mining cost is  $24 * 3.3 = 79$  CZK. Estimated revenue from mining DOGE is 7.28 USD = 145 CZK. The net profit for one day mining DOGE is  $145 - 79 = 66$  CZK (per month 1980 CZK).

Mining DOGE has been started at the end of December 2013 and duration time has been 2 month. During that time almost 400 000 DOGE has been mined by two GPUs 280x. From experience it is better to wait as long as possible to sell the digital currency because from empirical evidence more money would be obtained. Suppose DOGE were sold now (March 2014), today's price per one DOGE is 0.00000157 BTC, trading it to BTC would be 0.62 BTC for 400 000 DOGE and converting BTC to USD would be  $0.62 * 645$  USD = 430 USD and converting USD to CZK is 8500 CZK. For mining DOGE for two months the net profit would be 8500 CZK closing today, it is a little bit more than one third of the initial investment – that means that estimated and calculated today the initial investment would be back exactly in 6 months and after this six months. Is this a successful business? Yes, it is.

## 6 Conclusion

Aim of this bachelor thesis was supposed to analyze the first digital and decentralized currency Bitcoin, how it works, an analysis of the mining process and last but not least to compare Bitcoin to different digital currencies that are based on Bitcoin. The practical part of this thesis was focused on the mining process that is necessary for all digital currencies.

Entering a digital currency analysis was confusing for the first time because Bitcoin network is a very sophisticated software but during this analysis many questions on how the Bitcoin could work have been answered in order. Comparing Bitcoin to alternative digital currencies was easy to understand because all the alternative currencies are based on Bitcoin. A deep analysis of Bitcoin was not possible because it is a very complex system and it would exceed the extent of the bachelor thesis.

The practical part was focused on building a mining rig and to be an active member of the mining process in digital currencies. It was found that mining is a profitable business with the potential of initial investment return from 4 to 6 months and there are no limits for the size of the initial investment. During the practical part Dogecoin currency has been mined because it used to be the most profitable digital currency at the moment.

Mining resulted in a successful business with money return in six months. Profitability of mining depends on the current hashrate, power consumption and cost, on current market prices and many other factors but if mining would stop being profitable it is still possible to use the hardware for something else (for example to crack passwords) or the components could be sold and because every component was new and with a two year warranty or more the price could be different by one fourth (it sounds bad but in computer equipment it is not). The mining rig was built with two graphic cards but there is still one slot available for one GPU – power supply is supposed to handle another Radeon R9 280x by power consumption and with connectors without some reductions.

Bitcoin can't be shut down by some government or anybody else because it is completely decentralized. Many people say that the Bitcoin is a “bubble” and over

some time it will be forgotten, this bachelor thesis was also supposed to inform the community about Bitcoin and see its positive future and that mining is really a great business.

## 7 References

**AMD - ATI Technology. 2013.** [Online] January 2013.  
<http://developer.amd.com/tools-and-sdks/heterogeneous-computing/amd-accelerated-parallel-processing-app-sdk/>.

**Bitcoin Charts. 2013.** [Online] 2013.  
<http://bitcoincharts.com/charts/volumepie/>.

**Caldwell, K. 2014.** Payment system for Electronic commerce. [Online] 2014.  
<http://kcrona.tripod.com/ecomch11/cash.htm>.

**Casascius. 2012.** Bitcoin News Feed. [Online] December 2012.  
[http://bitcoin.gw.gd/spip.php?page=archive&id\\_rubrique=23&date=2012-11-25](http://bitcoin.gw.gd/spip.php?page=archive&id_rubrique=23&date=2012-11-25).

**Einstein, Albert. 2011.** The work institute. [Online] May 2011.  
<https://workinstitute.com/One-Hour-to-Save-the-World>.

**eMansipater. 2011.** Stackexchange. [Online] September 2011.  
<http://bitcoin.stackexchange.com/questions/148/what-exactly-is-mining>.

**Laszlo. 2010.** Bitcoin forum. [Online] March 2010.  
<https://bitcointalk.org/index.php?topic=137.0>.

**Moore, Shirley. 2013.** [Online] December 2013.  
<http://svmoore.pbworks.com/w/file/fetch/71304148/Hash-DSS.pdf>.

**Muljadi, Paul. 2012.** [Online] 2012.  
[http://books.google.cz/books?id=x\\_8l5aBAJ2gC&dq=Cryptographic+hash+functions+have+many+information+security+applications,+notably+in+digital+signatures,+message+authentication+codes+\(MACs\),+and+other+forms+of+authentication.+They+can+also+be+used+as+ordinary+hash+functions,+to+index+data+in+hash+tables,+for+fingerprinting,+to+detect+duplicate+data+or+uniquely+identify+files,+and+as+checksums+to+detect+accidental+data+corruption.+Indeed,+in+information+security+contexts,+cryptographic+hash+values+are+sometimes+called+\(digital\)+fingerprints,+checksums,+or+just+hash+values,+even+though+all+these+terms+stand+for+more+general+functions+with+rather+different+properties+and+purposes.&source=gbs\\_navlinks\\_s](http://books.google.cz/books?id=x_8l5aBAJ2gC&dq=Cryptographic+hash+functions+have+many+information+security+applications,+notably+in+digital+signatures,+message+authentication+codes+(MACs),+and+other+forms+of+authentication.+They+can+also+be+used+as+ordinary+hash+functions,+to+index+data+in+hash+tables,+for+fingerprinting,+to+detect+duplicate+data+or+uniquely+identify+files,+and+as+checksums+to+detect+accidental+data+corruption.+Indeed,+in+information+security+contexts,+cryptographic+hash+values+are+sometimes+called+(digital)+fingerprints,+checksums,+or+just+hash+values,+even+though+all+these+terms+stand+for+more+general+functions+with+rather+different+properties+and+purposes.&source=gbs_navlinks_s).

**Nanotube. 2014.** Bitcoin It. [Online] February 2014.  
[https://en.bitcoin.it/wiki/Pooled\\_mining](https://en.bitcoin.it/wiki/Pooled_mining).

**Osmosis.** Weusecoins - Your portal into the world of Bitcoin. [Online]  
<http://www.weusecoins.com/en/questions>.

**Satoshi, Nakamoto. 2009.** bitcointalk.org. [Online] December 2009.  
<https://bitcointalk.org/index.php?topic=12.msg52#msg52>.

**Schwartz, David. 2012.** Stackexchange. [Online] 2012.  
<http://bitcoin.stackexchange.com/questions/148/what-exactly-is-mining>.

**Slush, Palatinus, Marek. 2013.** Slush's pool. [Online] March 2013.  
<http://mining.bitcoin.cz/stratum-mining>.

**—.** 2013. Trezor - The Bitcoin Safe. [Online] 2013.  
<http://www.bitcointrezor.com/faq/>.

**Southurst, Jon. 2013.** Coindesk. [Online] November 2013.  
<http://www.coindesk.com/peter-thiel-claims-bitcoin-potential-change-world/>.

**Steven, Levy. 1994.** E-Money (That's What I Want). *Wired*. [Online] December 1994. <http://www.wired.com/wired/archive/2.12/emoney.html>.

**Tom van der Woerdt. 2013.** bitcoin Stack Exchange. [Online] April 2013.  
<http://bitcoin.stackexchange.com/questions/9854/why-do-amds-gpus-mine-faster-than-nvidias>.

**uraymeiviar. 2014.** Reddit. [Online] January 2014.  
[http://www.reddit.com/r/BitcoinMining/comments/1uoy4b/sha256\\_with\\_asic\\_compared\\_to\\_scrypt\\_with\\_gpu/](http://www.reddit.com/r/BitcoinMining/comments/1uoy4b/sha256_with_asic_compared_to_scrypt_with_gpu/).



## 8 Supplements

### 8.1 List of tables

Table 1: Alternative currencies comparison .....	29
Table 2: Modern GPUs comparison .....	32
Table 3: Multiple criteria decision .....	32
Table 4: Used components.....	35
Table 5: Linux vs. Windows mining .....	36
Table 5: Bitcoin vs. Altcoins [source: dustcoin.com].....	42
Table 7: Dogecoin pools .....	43

### 8.2 List of figures

Figure 1: First noted transaction in Bitcoins [Source: bitcointalk.org] .....	12
Figure 2: CPU [source: intel.com].....	15
Figure 3: GPU [source: ati.com].....	16
Figure 4: FPGA card modified for bitcoin mining [source: enterpoint.co.uk].....	16
Figure 5: Avalon miner [source: gizmodo.com.au].....	17
Figure 6: Mining hardware development [source: thegenesisblock.com].....	17
Figure 7: Multibit symbol [source: multibit.org].....	19
Figure 8: Electrum symbol [source: electrum.org].....	20
Figure 9: Mt. Gox logo [source mtgox.com] .....	22
Figure 10: Bitcoin logo [source: bitcoin.org] .....	25
Figure 11: Litecoin logo [source: litecoin.org].....	25
Figure 12: Peercoin logo [source: peercoin.org] .....	26
Figure 13: Namecoin logo [source: wikimedia.org].....	26
Figure 14: DOGE meme [source: dogecoin.com] .....	27
Figure 15: Dogecoin logo [source: dogecoin.com] .....	27
Figure 16: Quark coin logo [source qrk.cc].....	27
Figure 17: Auroracoin logo [source auroracoin.org].....	28
Figure 18: cgminer output .....	45

### 8.3 Acronyms, abbreviations and symbols

<b>ALU</b>	Arithmetic Logic Unit
<b>ASIC</b>	Application Specific Integrated Circuit
<b>AUR</b>	Auroracoin
<b>BAMT</b>	Big A Miner Thing
<b>BIOS</b>	Basic Input Output System
<b>BTC</b>	Bitcoin
<b>CPU</b>	Central Processing Unit
<b>DOGE</b>	Dogecoin
<b>EUR</b>	European currency
<b>GB</b>	GigaByte
<b>GPU</b>	Graphical Processing Unit
<b>LTC</b>	Litecoin
<b>MB</b>	Motherboard
<b>Mhash</b>	Megahash
<b>MS</b>	Microsoft
<b>NMC</b>	Namecoin
<b>NSA</b>	National Security Agency
<b>OS</b>	Operating system
<b>PPC</b>	Peercoin
<b>PPLNS</b>	Pay Per Last N Shares
<b>PPS</b>	Pay Per Share
<b>PSU</b>	Power Supply
<b>QRK</b>	Quarkcoin
<b>RAM</b>	Random Access Memory
<b>RDC</b>	Remote Desktop Connection
<b>SHA256</b>	Secure Hashing Algorithm
<b>SSH</b>	Secure Shell Connection
<b>USD</b>	American currency

### 8.4 Used software

- BAMT
- SMOS Linux
- Win32diskimager
- Cgminer 3.7.2
- Google Chrome
- TightVNC
- MS Windows 7 – student license via Dreamspark
- MS Word, Excel, PowerPoint

## 8.5 Used Hardware

- ATI Radeon R9 280x / MSI R9280XGAMING3G
- Corsair RM850
- MSI Z77A-G45
- Intel Celeron G1610 @ 2.6 GHz
- Kingston KHX1333C9D3B1K2
- A-DATA USB flash drive 16 GB
- HDD Western Digital 320 GB SATA II