University of Tartu
Faculty of Economics and Business Administration

Kärt Viilup

PROFITABILITY FROM MINING BITCOINS: SHOULD YOU STILL ENTER THE BITCOIN MINING COMPETITION? LONG-TERM SIMULATION ANALYSIS OF THE PROFITABILITY FOR A SINGLE MINER

Master's Thesis for the Master of Arts in Economics and Business Administration

Thesis Advisors: Sven Kristjan Bormann, Raul Eamets, PhD

Tartu 2015

Soovitan suunata kaitsmisele ……..
(juhendaja allkiri)

Kaitsmisele lubatud “ “..... 2015. a.

Majandusteooria õppetooli juhataja Raul Eamets ……..
(õppetooli juhataja nimi ja allkiri)

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, põhimõttelised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

……..
(Kärt Viilup)

TABLE OF CONTENTS

1. INTRODUCTION 7

2. BACKGROUND 12

2.1. Bitcoin Network 13

2.2. Transactions 14

2.3. Blocks and Block Chain 16

3. MINING BITCOINS 18

3.1. Mining Options 19

3.1.1. Solo Mining 20

3.1.2. Mining in a Pool: the BTC Guild Mining Pool 21

3.2. Mining Hardware 24

3.3. Mining profitability 26

3.3.1. Difficulty in Mining 27

3.3.2. Volatility 31

3.3.3. Electricity Price 32

4. PROFITABILITY FROM MINING BITCOINS 34

4.1. Methodological approach 34

4.2. Data 36

4.3. Simulation Analysis 38

4.3.1. Estimating Change in Difficulty 38

4.3.2. Revenue from mining in the BTC Guild mining pool 40

4.3.3. Expenditure 47

4.3.4. Profitability from mining Bitcoins 49
5. DISCUSSION 51
6. CONCLUSION 53
REFERENCES 55
APPENDIXES 63
RESÜMEE 64

ACRONYMS

ASIC Application Specific Integrated Circuit

BTC Abbreviation for bitcoin (sometimes also used as XBT)

CPU Central Processing Unit

FPGA Field-Programmable Gate Array

Ghash Giga hash

GPU Graphics Processing Unit

Mhash Mega hash

PPLNS Pay Per last N Shares

Thash Tera hash

DEFINITIONS

Block A record in the blockchain that holds a number of transactions that have occurred in the Bitcoin network. In roughly every 10 minutes the network releases a new block that will be included to the blockchain.

Blockchain A public record of all of the transactions that have taken place in the Bitcoin network in a chronological order. Once a block is validated and included in the blockchain, its permanence is verified.

Difficulty The measure of how hard it is to generate a new blocks in the blockchain. The difficulty is designed to adjust every 2016 blocks (roughly 2 weeks) to balance out the rate at which blocks are created.

Hash rate A measuring unit of the processing power of the Bitcoin network

Mining Process of making computer hardware do numerous mathematical calculations for the Bitcoin network to validate transactions. Through mining new blocks are added to the blockchain.

Miners People who contribute their computers hashing power for the sake of the Bitcoin network. As a reward for mining, in every 10 minutes a new block of new bitcoins is found and the miner who solved the necessary calculation receives the transaction fees of that block plus a certain amount of new bitcoins.

Mining pool Pooling of resources by miners in order to find more bitcoins in a shorter amount of time and thus guarantee a more stable income through the Bitcoin reward system.

Proof-of-work The work that needs to be done in order to find the right hash necessary for solving a block.

1. INTRODUCTION

Bitcoin is the world's first decentralized digital currency. It was introduced in 2008 by a person or a group of people called Satoshi Nakamoto. Since its introduction it has experienced an exponential growth and as of writing this paper, according to Blockchain, there are over 14 million bitcoins in circulation (Total Bitcoins…) and the number is growing daily due to the hard work of numerous people who contribute their computers' power for the sake of the network to mine new bitcoins. As an incentive for mining, in every ten minutes the network releases a block of new bitcoins and all miners hope they are the ones to receive the reward and thus get paid for their mining activities.

The Bitcoin system is a peer-to-peer network that uses proof-of-work to keep a public record of all of the bitcoin transactions. There is no need for a third intermediary between the two partners to clear the transactions and the whole system is built up to be as user friendly as possible (Miers *et al* 2013: 1). In the original paper explaining the network Satoshi Nakamoto brought out that the network is "robust in its unstructured simplicity" (Nakamoto 2008: 8). Even though virtual currencies might sound like a niche subject, Bitcoin has managed to bring the topic into mainstream media and make it relevant for a very large audience. The market capitalization of Bitcoin amounts to over $3.3 billion and is growing steadily (Bitcoin Market…). In many countries there are Bitcoin enthusiasts who work towards introducing and developing the network even more, for example in Estonia the Estonian Cryptocurrencies Association stands for the development of cryptocurrencies in Estonia (Estonian Cryptocurrency…).

The initial purpose of Bitcoin that was brought out in the original paper was to introduce a payment system that would offer an alternative for the currently existing payment systems that require a third party mediator. While also filling that role, the Bitcoin network has grown into something much bigger- there is a whole new industry that is being developed around Bitcoin, offering different services or products that

might be required. One of the industries that have seen a way to profit from the Bitcoin rise is the hardware industry that has brought into the market a completely new device- an Application-Specific Integrated Circuit (ASIC) hardware for mining bitcoins. ASIC hardware is a machine that is solely customized for one use only and in the case of Bitcoins its sole aim is to mine bitcoins as fast as possible (Taylor 2013: 1). The given thesis takes a deeper look into the Bitcoin mining industry to analyze whether the reward system for miners is appealing enough to make the initial investment and enter the market as a Bitcoin miner.

When in the beginning people used their regular computers Central Processing Units (CPU) for mining, then in the recent years in order to actually benefit from mining, a person is recommended to use an ASIC device, otherwise finding a block and getting rewarded for it, which is eventually the aim of most miners, is highly unlikely (Wang, Lo 2014: 4). Due to the fact that miners have rapidly started to upgrade their old mining hardware for newer models in hopes of mining more blocks and earning more money, it is much harder for new interested miners to join the market both because of the high buy in that is the cost of the ASIC device and also because of the risen level of difficulty due to an increased interest in mining and the major advancements mining hardware has gone through. In 2009, the creator of the Bitcoin, Satoshi Nakamoto, asked for the members of the Bitcoin network in a forum to steer clear of such a behavior: "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" (Bitcointalk 2009). Unfortunately Satoshi's ask was denied and the arms race for the best hardware started quickly, moving from Central Processing Units (CPU) to Graphics Processing Units (GPU) to custom Field-Programmable Gate Array (FPGA) systems to custom Application-Specific Integrated Circuit (ASIC) devices (Taylor 2013: 2).

The arms race is not the only thing that might potentially scare off new interested miners. The Bitcoin network is built up the way that in total there will be 21 million bitcoins in circulation and no more. Current calculations expect the network to reach this amount by 2140. As over 14 million bitcoins have already been mined, the mining

of new ones becomes more and more difficult and therefore also less profitable. The expensive hardware, increasing rate of difficulty in mining bitcoins and he lowering price index of Bitcoin all rise a question whether it is actually possible for a miner to earn any profit from this or even more- earn back the initial investment they put into this wildly popular network? This thesis aims to answer the given question from an average miners' perspective.

The aim of the thesis is to calculate whether mining bitcoins is a profitable action for a new miner and analyze how long it would take to pay off the initial investment that was made to purchase the hardware required for mining bitcoins. Even though there are academic works that look at the profitability of mining, it is generally looked at more broadly without bringing out any simulation analyses and only making estimates. There are also several online calculators that estimate how much a miner could earn per day, but these calculators assume the miner to be mining solo, whereas it has already been brought out by many researches that mining solo is no longer a profitable action for an average miner and in order to be successful in mining, it is strongly suggested to join one of the mining pools. The given thesis will take a different approach from the mining calculators in the sense that it will take one of the most popular Bitcoin mining pools and conduct the calculations based on the results of this pool and not the whole network as the mining calculators do. Every step of the payoff function will be explained in depth so that it would be clear which factors affect whether mining bitcoins is profitable or not.

In order to meet this goal, there are many aspects that need to be taken into account and for that, the following research objectives were formulated:

- analyze how a new miner should enter the market;
- analyze which hardware is most suitable for a new miner;
- consider the relative costs related to mining – mainly the price of electricity, as hardware devices consume large amount of electricity;
- analyze how long it would take to earn back the initial investment;
- discuss the future of bitcoin mining and its profitability.

The research method for the given thesis follows the structure similar to several online calculators that help estimate whether a miner is earning profit by inserting all of the necessary parameters into the calculator. It is noteworthy that while several online calculators come to a somewhat similar result, there are still great differences in these results because of the different estimates of parameters necessary for the calculations.

It is known that mining bitcoins has been profitable for a very long time and as many people are still engaged in mining, it indicates they are still in surplus when looking at the reward and the costs needed for earning this reward. Therefore this thesis expects the simulation analysis results to be in surplus when only the operating costs are taken into account. From the rising level of difficulty and the ongoing discussion among the mining community it can also be expected that the profit earned is considerably smaller from what it used to be for example a year ago. Based on that the thesis expects that within the timeframe that is left until the halving of the reward in 2017, it is very likely the reward earned by the miner will not be sufficient to pay off the initial investment and thus can be concluded that it is not profitable for a new miner to enter the market any longer. As mentioned above, there are no mining calculators available that would estimate the earnings based on the results of a mining pool, therefore at this point it is difficulty to even make estimates on how much of the initial investment could be earned back through mining.

The information necessary for making projections about the earnings of a miner is taken from the website of the mining pool that is used in the given analysis- the BTC Guild, which is one of the oldest mining pools with a positive image among miners and which follows a payoff function Pay-Per-Last-N-Shares (PPLNS). The PPLNS payoff function is thought of as one of the most favourable ones for a new miner who does not contribute huge amounts of computing power to the mining pool and therefore it was chosen for the given thesis. A lot of statistics is also taken from Blockchain, which is one the most thorough statistics banks and contains all the information about Bitcoin since it was first introduced. Information about the hardware that is used in the simulation analysis is taken from the homepage of the producer, Butterfly Labs. The information about the electricity price for an average household is taken from Eurostat.

The thesis is structured into three main parts- firstly there is a general introduction to the Bitcoin network. Since the Bitcoin system is very complex and has a lot of details that need to be brought out, this part will introduce everything about the network that is relevant to the topic of the given thesis and lays the groundwork for the following parts. The second part of the thesis takes a more thorough look in the mining industry and everything that is related to mining and miners, such as the hardware that is needed, the factors that play a role on how easy it is to find new bitcoins and the volatility of the currency. The third and the most important part of the thesis comprises of the methodology explanation and the actual analysis on the profitability of mining bitcoins. The third part also includes a discussion that will more thoroughly take a look at the future trends of Bitcoin mining industry.

2. BACKGROUND

A bitcoin can be seen as an electronic token that has no underlying commodity or sovereign currency, and is not a liability on any balance sheet. Bitcoins can only be used within its ecosystem; outside of that system they have no value (Androulaki *et al* 2013:36). Bitcoin also has no legal tender status in any jurisdiction and very little academic literature to describe and analyze this phenomenon. Regardless of the above mentioned the publics' interest towards the topic of Bitcoin is growing steadily and the currency has found many successful supporters such as Richard Branson and Bill Gates (Siciliano, 2014).

Even though Bitcoin might seem like a new-age innovation, the idea of virtual currencies and their benefit over fiat currencies has been discussed already for several decades as brought out by Drehmann *et al*, 2002. Bitcoin is a cryptographic currency and a digital payment system that enables global and secure transactions with a low transaction fee. The magazine Wired describes bitcoin as a "dollar that has a teleporter wrapped around it" (Kaminsky 2013). Bitcoin has its own metric value that is called bitcoin (with lowercase letter "b" and abbreviated as BTC). Another popular abbreviation for the Bitcoin currency is XBT (Bitcoin Symbol…), but throughout this thesis the abbreviation BTC is used. The Federal Bureau of Investigation has defined bitcoin with lower case as a currency and Bitcoin with an upper case as an official protocol and the software called Bitcoin (Federal Bureau of Investigation … 2012: 3) and this rule will also be used in the given thesis.

The founder of Streamin' garage and creator, executive producer and host for Bitcoin game show "Take My Bitcoin" Mike Rotman has said that in his eyes the biggest problem with Bitcoin is that it is really hard to use bitcoins and even harder to understand it (Bundrick 2015). This thought is also supported by Anton Badev and Matthew Chen, who bring out in their research that the Bitcoin scheme is a complex one and that its implementation involves a combination of cryptography, distributed algorithms and incentive driven behaviour (Badev, Chen 2014: 3). Even though when

creating the Bitcoin system Satoshi Nakamoto aimed for the network to be as simple as possible, it is actually much more complex already because of the many terms one has to know in order to grasp the whole system. Because of this complex network, the given section will give an overview of the structure of the network and explain everything regarding Bitcoin that is necessary for the analysis part.

2.1. Bitcoin Network

The Bitcoin network is a peer-to-peer payment network which is operating on a cryptographic protocol and enables its users to make transactions in bitcoins to one-another. There is no central financial authority to control the system. Instead, the control function belongs to the Bitcoin network, which acts as the financial authority by using cryptography to keep control over the transactions and creation of new bitcoins (Decker, Wattenhofer 2014: 1).

The Bitcoin network relies on a public ledger which records all of the transactions in the system. All of the information from the ledger is available to the public as a blockchain, which gives information on all of the transactions that have taken place. The information in the blockchain is organized so that all occurred transactions are put into different blocks with links which lead to the previous block in the list and with that form a chain. Because of that it possible to follow the chain backward to the beginning of Bitcoin history and have a complete record of all transactions which have ever occurred (Kondor *et al* 2014: 3).

The blockchain is maintained by a network of miners, who are compensated in bitcoins for the computing power they put into mining new bitcoins and validating transactions. Bitcoin transactions are protected with cryptographic techniques that ensure only the rightful owner of a Bitcoin address can transfer funds from it. Miners are competing with each other on who's' computer gets to solve the cryptographic search problem first and with that find a new block and earn a reward. A new block consists of 25 new

bitcoins and the transaction fees of users whose transactions were included. When the amount received by the miner is larger than 25 bitcoins, which it usually is, the rest from there are transaction fees.

When Bitcoin mining began, the reward consisted of 50 bitcoins, but the number dropped to 25 bitcoins after 210 000 blocks were mined. Once another 210 000 blocks are mined with the 25 bitcoins reward per block, the reward will again drop by half and remain so for the coming 4 years which is the estimated mining period for the 210 000 new blocks depending on how accurately the mining difficulty manages to control this time period. Mining difficulty is the factor that determines how easy it is to find one new block and it is set based on how much time it took to find the previous block. In an ideal case a block is found in every 10 minutes, if a block is found faster, the difficulty level increases and finding a block will be harder but if it took less than 10 minutes, the difficulty level would lower itself to make sure the next block is found within the 10 minute frame (Eyal, Sirer 2013: 4).

On 13th of April 2015 according to the BitcoinClock, there were 351 902 blocks mined altogether, from where 210 000 were mined with the 50 bitcoins per block reward and 68 098 blocks mined with the 25 bitcoins per block reward. In 141 902 blocks, the reward will again drop by half as it did from 50 to 25 the previous time. BitcoinClock also brought out that there were 1118 blocks mined since the last change in difficulty, therefore in 898 the difficulty of mining bitcoins will again change (Difficulty Change…).

2.2. Transactions

A transaction is defined by the Bitcoin network as an event where one user transfers a certain amount of bitcoins to another user. Because there is no central financial authority to control the system, the transfer is broadcast to the Bitcoin network and collected into a block (Kristoufek 2013: 5). Transactions are not encrypted and therefore it is possible to browse and view every transaction ever collected into a block (Barber *et*

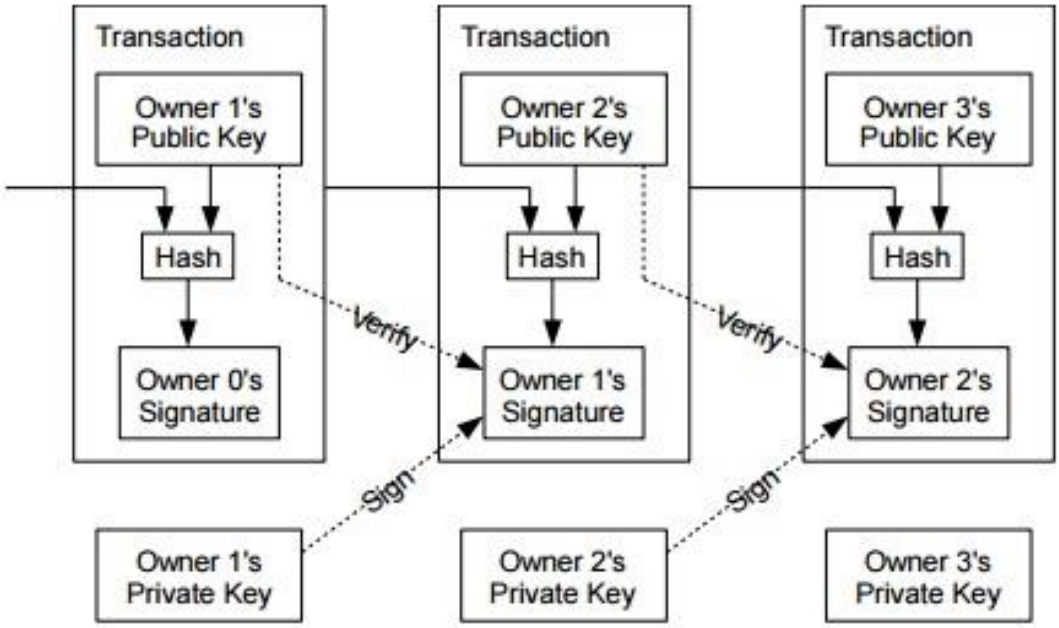
at 2012: 4). All of the transactions that have occurred in the Bitcoin network are collected into a ledger, which in Bitcoin network is called the blockchain, which is essentially a long line of blocks that have information on previous transactions. The blockchain can be viewed by anyone, making it a transparent system.

Before the Bitcoins' eruption, online transactions had always required a trusted third-party intermediary such as PayPal, MasterCard or Visa because of the fear of double spending (Meiklejohn *et al* 2013: 1). Bitcoin solved the double-spending problem by distributing the block chain among all its users via a peer-to-peer network. As all transactions that have occurred are open to the public, it can easily be ensured that the same bitcoins haven't been previously spent.

Transactions on the Bitcoin network are not denominated in any popular currencies as they are on PayPal, but are instead denominated in bitcoins. This makes it a virtual currency in addition to a decentralized payments network. The value of the currency is not derived from gold or government fiat, but from the value that people assign to it. The dollar value of a bitcoin is determined on an open market, just as is the exchange rate between different world currencies (Brito, Castillo 2013: 4)

In order for the transaction to be included into a blockchain, it needs to be validated. This is one of the reasons why the network has terms such as mining and miners. Mining is a process of solving mathematical equations to validate transactions and add these transactions to the blockchain and miners are the people who contribute their computers' or hardware's' time and power to solving these equations. The first miner to successfully solve the necessary equation and authenticate a block (which consists of several transactions) receives a reward of bitcoins after sharing the solution with everybody else in the network by adding the authenticated block to the blockchain. The reward the miner receives consists of new bitcoins released to the circulation plus the transaction fees from the authenticated block.

Figure 1. Structure of Bitcoin transactions



Source: Nakamoto 2008: 2

Figure 1 gives an overview of how transactions work in the Bitcoin network. Each owner transfers the coin to the next owner by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

2.3. Blocks and Block Chain

The Bitcoin blockchain can be seen as the backbone of the Bitcoin network that provides a tamper-proof data structure, providing a shared public ledger open to everybody who is interested (Garay *et al* 2014: 2). The blockchain is built of blocks, which connect all transactions together. Transactions are combined into single blocks and are then verified on average in every ten minutes through mining. Each subsequent block strengthens the verification of the previous blocks, making it impossible to double

spend bitcoins (Böhme *et al* 2015: 216). New blocks are added to the end of the blockchain and can never be changed or removed once written. Each block memorializes what took place in the minutes before it was created.

All of the blocks contain a record of some or all recent transactions and a reference to the block that came immediately before it. Through these activities a chain is formed through which the whole history of Bitcoins can be traced back. The block also contains an answer to a difficult mathematical equation - the answer which is unique to each block. New blocks cannot be submitted to the network without the correct answer and in the process of mining computers solve many mathematical equations to find the necessary answer that solves the current block and add it to the blockchain (Karlstrom 2014: 24).

Finding an answer to the mathematical equation can be seen as a lottery, where many miners are competing to be the first ones to solve the equation and therefore receive the reward for finding it. In order to have greater chances at this lottery, a person should have a powerful hardware that can solve more equations than other mining hardwares. With this there are greater chances that one of the equations the computer solves is the one that is needed for the given block. Every time someone successfully finds a block, they get a reward of 25 bitcoins plus the transaction fees, the blockchain is updated, and everyone on the network hears about it. That’s the incentive to keep mining and keep the transactions working.

The blocks are added to the blockchain in a linear, chronological order. Everyone who is interested can get a copy of the blockchain and therefore gets access to complete information about the addresses and their balances right from the genesis block to the most recently completed block.

3. MINING BITCOINS

Bitcoin mining is the processing of transactions in the digital currency system, in which the records of current Bitcoin transactions, known as a blocks, are added to the record of past transactions, known as the blockchain. Bitcoin mining is done by computers that aim to validate the transactions and find new bitcoins. Miners are the people to whom these mining devices belong and who choose to contribute their devices' computing power to the Bitcoin network (Ala-Peijari 2014: 25). As a reward for their contribution, in every ten minutes the network releases a block of new bitcoins which together with the reward for the transactions that were validated belongs to the miner whose computer was the first to solve the necessary equation. Mining can therefore be seen as a competitive lottery, where all of the computers which are engaged in mining compete to solve the necessary equation and with that earn a reward (Miller 2014: 3). Mining is a specialized and competitive market where the rewards are divided up according to how much calculation is done. Not all Bitcoin users do Bitcoin mining, and it is not an easy way to make money (StartBitcoin 2014).

When originally the mining was done by personal computers then in time mining has become more and more popular and with that the devices have also gone through drastic improvements. Even though it is still possible to mine with a personal computer, it is unlikely that the miner will ever earn a reward for his/her actions as the device is too slow compared to custom made hardware that has been developed with the sole purpose of mining bitcoins.

Miners and mining are an essential part to the Bitcoin network as they are the ones who keep and updated record of transactions and with that avoid the double spending problem. Because of mining, Bitcoin network can operate without having a third intermediary, as miners carry this role.

Another important role the miners fill is controlling the release of new Bitcoins. The Bitcoin network is built up so that the total amount of bitcoins, which is 21 million, will

be released to the market over a certain time period. It is currently estimated that by the year 2140 the Bitcoin network will reach this target. After that the miners will no longer receive new bitcoins as rewards and are only rewarded with the transaction fees they receive from adding a new block to the block chain. The Bitcoin network is also built up so that those people who started mining in an earlier stage will receive a higher reward, as the reward is halved in every 4 years (Babaioff *et al* 2012: 57). When in the beginning, as a reward miners received a block that consisted of 50 bitcoins, then after 4 years the reward halved into 25 new bitcoins per block. The reward is expected to halve again some-time in 2017.

3.1. Mining Options

Before starting to mine, Bitcoin miners have to decide whether they wish to mine in a pool or mine solo. Solo mining is when a miner performs the mining operations alone. All mined blocks are generated to the miner's credit. Mining in a pool means that many miners join their hashing powers to mine bitcoins and then share the reward using one of the payout functions. In case a solo miners' device manages to find a block, all of the 25 bitcoins plus the transaction fees automatically belong to the miner herself/himself. Therefore the reward of solo mining is a lot more appealing. As however there is a great deal of luck in determining which computer first manages to solve the cryptographic search problem and receive the block, then chances of finding a block via solo mining are very small. It is very likely that a user that mines solo does not manage to find a block for years and therefore earns no profit from mining.

Eyal and Sirer from Cornell University bring out that there is empirical evidence that shows that Bitcoin miners behave strategically and form pools in order to decrease the variance of their income rate (Eyal, Sirer 2013: 2). Mining in a pool means that many miners put together their computers' hashing power in order to find new blocks. Different pools have different payout schemes they offer for their miners but usually the pool reward is divided between all of the miners who contributed to finding the block

based on the percentage of hashing power they put into the pool. In a pool, chances of finding a block are much bigger and therefore it guarantees a much more steady income.

3.1.1. Solo Mining

Solo mining is known as going through the process of calculating hashes required for the Bitcoin network individually with the aim of finding a block of bitcoins which's reward will then be solely in the hands of the solo miner. During the process of calculating hashes, miners also validate transactions and with that are rewarded a certain amount of bitcoins per each transaction they validated while looking for a new block. The solo miners also receive the reward for validating transactions solely to themselves. Taking into account that currently the reward for finding a block is worth 25 bitcoins, the reward a solo miner receives is appealing to many.

Solo mining with a constant hash rate *h* and the difficulty level *D* is a Poisson process with $\frac{h}{D*2^{32}}$ as the rate parameter, meaning that it is a continuous-time stochastic process. Mining for a certain time period *t* (e.g. 30 GH/s) results in $\frac{ht}{D*2^{32}}$. The number of blocks found follows the Poisson distribution with (Rosenfeld 2011: 2):

(1) $$\lambda = \frac{ht}{D*2^{32}},$$

So in case a miner would use the ASIC Little Single mining device that produces 30 GH/s (Butterfly Labs) and mine for a day (86 400 seconds) with a difficulty 46717549645 like it was on March 22nd 2015 according to Blockchain statistics and receive a reward of 25 bitcoins per block, then the number of blocks found via mining would be:

(2) $$\frac{ht}{D*2^{32}} = \frac{30000000000*86400}{46717549645*4294967296} = 0.000012918*25 = 0.00032295 \text{ bitcoins}$$

Due to the nature of the mining network it cannot be estimated that every day, every week or year a miner might earn such a reward.

In the beginning of Bitcoin mining everybody used solo mining because it was the only way to mine and even with a device that could not produce a big number of hashing power, it was still possible to find blocks. Once the difficulty started to increase due to the fast pace of hardware development and increased number of miners, it became more and more complicated to find bitcoins up until the point where it did not make sense to mine solo anymore as it was too unlikely that a miner would ever find a block and get a reward for the work they have put into the network. The above calculations show that currently the chances of finding a block via solo mining are very low and the odds are strongly against it.

3.1.2. Mining in a Pool: the BTC Guild Mining Pool

Mining in a pool became popular once the difficulty level of mining new bitcoins rose and it was not as rewarding any more to continue mining solo. A mining pool is the pooling of resources by miners, who share their processing power over a network, to split the reward equally, according to the amount of work they contributed to solving a block. Mining in a pool solved the problem of inconsistent reward- the chances for a pool to find a block to share are much higher than finding a block via solo mining and therefore creating a more steady reward rather than finding a block solo randomly once every few years (Houy 2014: 7). Currently mining in a pool is the only possible way for a small miner to earn any revenue. There are many different pools one can choose from to get the payoff function most suitable for the miner.

The given thesis will use the BTC Guild's pool in the simulation analysis for two main reasons- first of all it is one of the oldest running pools. The BCT Guild was opened already in 2011 in and by the end of 2014 miners of BTC Guild had mined over 32 000 blocks of bitcoins and hold about 5% of the daily bitcoins mined (McCormick 2014). All of this gives credibility that the pool will remain running and earn profit for miners and also certify that the owner of the pool has been honest with the miners when distributing profits earned by the pool. Secondly, the BTC Guild's pool follows the pay-

per-last-N-shares (PPLNS) reward system, which is considered to be one of the safest reward systems for beginner miners. The BTC Guild mining pool has both EU and US based servers.

The BTC Guild charges a 2% fee from all of the mined bitcoins, but as miners also mine Namecoins[1] and validate transactions while mining for new bitcoins, then taken into account the profit earned from these other mining activities, the fee is reduced to approximately 1%. Even though the miners have the chance to claim the transaction fees and Namecoins and have them sent to their accounts, then this thesis expects the miners to leave these items for the mining pool and in exchange reduce the fee to 1%. Because of that the simulation analysis will not be looking at the transaction costs and price of Namecoins but will just reduce the 2% fee to 1%.

The PPLNS reward system for the BTC Guild rewards all open shifts with a sum that is equal to (BTC Guild):

(3) **((Block Value + Transaction Fees) / 10) - Pool Fee (2%)**

In case of this thesis as stated above, the transaction fees are used to lower the pool fee, so the reward system follows this form:

(4) **(Block Value / 10) - Pool Fee (1%)**

The BTC Guild divides all users into a shift in order to make the reward system as honest as possible and to make sure people are interested in joining the mining pool. By dividing the reward found by one shift among ten last shifts, the pool makes sure there is no pool hopping and everybody earns the reward they are supposed to, based on the hashing power they contributed. Even in case one shift does not manage to find a block after contributing the necessary computing power, they still get rewarded from the amount of blocks the other nine shifts found. Pool hopping means that miners join a pool to contribute their computing power only when the expected share value or "luck" is estimated to be greater than 100% and with that cause loss for miners at pools with proportional reward systems because with the pool hoppers their share for reward

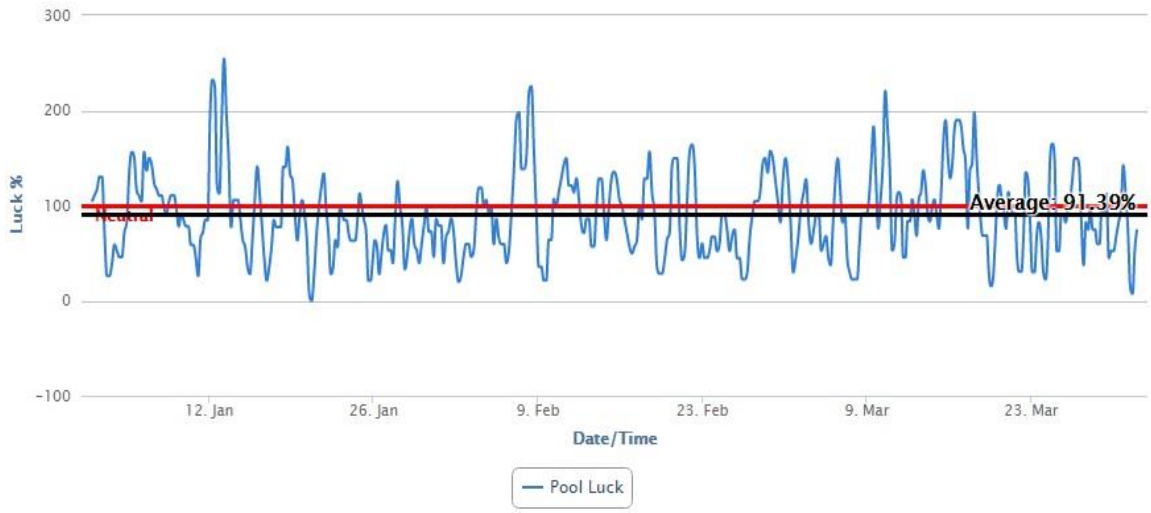
[1] "Namecoin is a decentralized open source information registration and transfer system based on Bitcoin"(Namecoin…).

automatically declines. There are different algorithms and logics experienced miners use for finding a pool with a share value greater than 100% so they can benefit from joining it. (Neighbourhood…2012).

Pool luck is measured in percentages and it shows how easy or difficult it was to find a block compared to other times the pool has found a block. If the luck is above 100% it means that the pool needed fewer shares then expected for the given difficulty. If the luck is below 100%, more shares were needed. The luck shows only history and says nothing about future blocks. Finding block is fully independent on historical events so that e.g. joining the pool only when there is high luck and disconnecting when the luck is low doesn't make any sense. In long term, the luck is always 100% (BitcoinCZ Mining 2015).

The pool luck of the BTC Guild varies greatly similarly with other pools. For the sake of this analysis this thesis will use the three-month average pool luck of BTC Guild, which on the 1st of April was 91.39 %.

Figure 2. Pool luck changes and the average pool luck for three months.



Source: BTC Guild

Pay-Per-Last-N-Shares group's shares submitted by all users into a "shift." Shifts are cut off after a certain number of shares, which increases whenever shifts get too short, or the difficulty gets too high. Once a shift is completed, it is considered an "Open

Shift". After 10 new shifts have completed, the oldest open shift is closed. While a shift is open, any blocks the pool finds are rewarded out to all open shifts (10% of the block per shift). This means that you will continue receiving rewards on completed (open) shifts even if you stop mining. This amount is then split evenly among all shares submitted during the shift (BTC Guild). The system is built up so in order to guarantee more stable revenue for all miners mining in the BTC Guild.

3.2. Mining Hardware

The most important thing in in determining whether a miner is successful and earns a sufficient amount of revenue from mining is the hardware that is used for mining.

In the beginning, using a personal computer and using its Central Processing Unit (CPU) was the most popular way to mine bitcoins. It did not contain any extra expenditure to the miners because they could easily use their own computers for mining. At this time the reward for finding a block was also higher, at 50 BTC, then currently it is only 25 BTC and is expected to drop again in some time. Since then according to Blockchain, the difficulty has also seen a massive increase from 1 190 923 195 in January 2014 to 42 971 662 056 in January 2015 (Rise of…). Because of this, mining new blocks has become more and more time consuming.

Mining with a CPU via the original Satoshi client is how the bitcoin network started. This method is no longer viable now that the network difficulty level is so high. Currently it is likely for a person to never find a single bitcoin using a CPU device. Because mining bitcoins is somewhat similar with a lottery, where many miners compete with each other on whose hardware manages to solve the cryptographic problem the first and therefore gets the reward of 1 block, there are still people who use CPUs for mining. For example high school and college students who can use the electricity from their parents' house or in school without having to pay for it themselves might try their luck in mining by using their own computers and with this have no real expenditure for mining. CPUs have different hashing rates as other hardware types but

an Intel Core 2 Quad Q9650, which is an average, CPU hashes with a rate of 18.67 mega hash per second (Intel Core…) and with this device it would take the miner on average 361694.3 years according to a Bitcoin Mining Profit Calculator to find one block via solo mining (Bitcoin Mining…). Since finding a block has a lot of luck involved as well, it might be that the miner finds a block by mining solo already in a year but the odds are strongly against that.

Soon it was discovered that high end graphics cards were much more efficient at bitcoin mining than CPUs and with that, the CPU bitcoin mining gave way to the Graphical Processing Unit (GPU) mining. GPUs allowed miners to increase the hashing rate over 50 or even 100 times more while consuming far less lower per one unit of work. (Stevenson 2013: 31).

With the rise of GPUs, the arms race for the best mining hardware began. The next hardware to replace the GPUs was Field Programmable Gate Arrays called FPGA. The first FPGA was introduced in June 2011 and already in late 2011 and early 2012 the Bitcoin mining hardware companies such as Butterfly Labs and ZTEX brought the first FPGA devices to the market (Ryder 2012). With the successful launch of these devices, the bitcoin mining hardware landscape gave way to specially manufactured hardware dedicated to mining bitcoins and thus entering a new era in bitcoin mining. Even though the FPGAs did not bring as big of an increase in mining speed, they did reduce the power efficiency of devices greatly thus lowering the cost for electricity. A typical 600 MH/s graphics card consumed upwards of 400w of power, whereas a typical FPGA mining device would provide a hash rate of 826 MH/s at 80w of power. That 5x improvement allowed the first large bitcoin mining farms to be constructed at an operational profit (Stevenson 2013: 33). The era of FPGAs can also be considered as the birth of Bitcoin mining industry because at that time many technology companies such as the above mentioned Butterfly Labs and ZTEX started producing the first devices which's sole aim was to mine bitcoins.

The third generation: the FPGA generation dominated the market for a relatively short amount of time, as in June 2012 the Butterfly Labs already came to the market with an Application Specific Integrated Circuit (ASIC) hardware. At the current point of time, the Bitcoin mining world is solidly in the ASIC era. An ASIC is a chip designed

specifically to do one thing and one thing only, which is to mine bitcoins as fast and efficiently as possible. Unlike FPGA's, an ASIC device cannot be repurposed to perform other tasks, therefore the investment made on an ASIC device can only be used for mining bitcoins and it cannot be programmed to perform anything else. When the development from CPUs to GPUs to FPGAs was relatively fast, then experts assume that in the immediate future there is nothing that would replace ASIC devices.

The power consumption on an ASIC device is the single most important factor of any ASIC product, as the expected useful lifetime of an ASIC mining device is longer than the entire history of Bitcoin mining and also because it is technically impossible to have as big of an increase in hashing speed as it was when the shift from CPU to GPU took place.

3.3. Mining profitability

Getting involved in mining bitcoins is a voluntary option- there is no need to be a miner if a person is interested in the Bitcoin network, one can easily purchase and exchange bitcoins without ever having contributed any hashing power for the sake of the network. Mining however is something the Bitcoin network cannot function without therefore there are incentives to convey people to start mining bitcoins (Raiborn, Sivitanides 2015: 26).

From 2009 to 2013, the bitcoin price experienced an exponential growth that reached its peak in December 2013, when the price of Bitcoin reached $1,128. This price surge was accompanied by a rise in the number of miners joining the bitcoin network, as mining suddenly became a very profitable action. As the number of miners grew, miners went from mining solo to joining pools, in order to share their computational power while maintaining their chances of capturing a reward and earn a more stable return on their investments. Researchers at New York University found that early miners who were using GPU devices broke even on their investment in just under two years in the United

States and the owner of the ASIC miner could have broken even in less than a month (Wang, Lo 2014: 2).

With the growth of miners and the computing power the network had, it quickly had to adjust itself to maintain a situation where only in every 10 minutes and no sooner a block is found from where miners can earn a reward. Due to that mining became less and less profitable up to the point where a new miner needs to make serious calculations whether or not it is still reasonable to enter the market- something like this is new to the Bitcoin mining industry.

3.3.1. Difficulty in Mining

One of the important measures in Bitcoin network is called difficulty. Difficulty is a measure of how hard it is to find a hash below a given target. The Bitcoin network has a global block difficulty and all valid blocks must have a hash below this target. The hash rate is adjusted to the level that on average in every 10 minutes one block would be found. In this ideal speed, 2016 blocks will be discovered every two weeks (Gronwald 2014: 4). After the 2016 blocks have been found, the new difficulty is selected so that if the same average hash rate is maintained, it will take two weeks to calculate the next 2016 blocks. If the new difficulty level is more than two times harder than the current difficulty, then the result is capped to two times harder restrictions on the range of acceptable difficulties/targets are also applied (Böhme *et al* 2014: 2). In recent years the difficulty level has rapidly started to rise because of the increase of miners who have joined the network and also of the hardware revolution that has lead from CPU mining devices to ASIC mining devices. Because of that the growth rate of the difficulty attribute is not fixed, but varies, and it is impossible to draw exact conclusion based on the previous results on how much the difficulty will change.

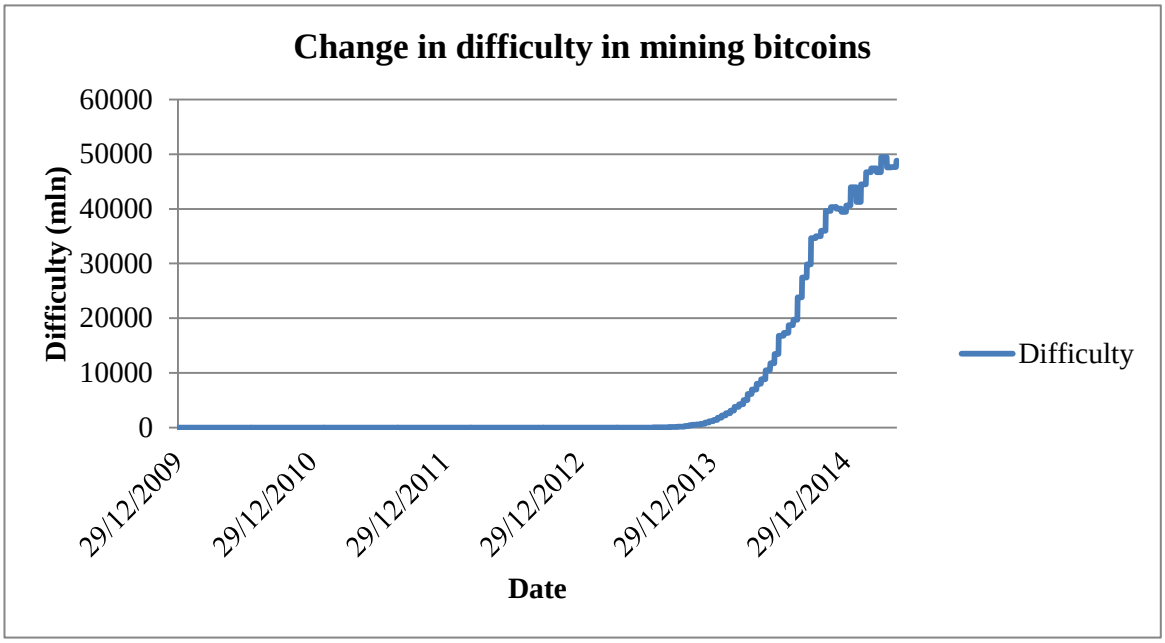
Satoshi Nakamoto brings out that the difficulty varies in order to "compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of

blocks per hour. If they're generated too fast, the difficulty increases." (Nakamoto 2008: 7)

When a computer mines bitcoins, it tries to calculate a hash which is the block's header. The hash starts with a certain number of zeros. The number of zeros is defined by the target. The target is a 256-bit number and is therefore extremely long. The target number is known to all of the Bitcoin users and anyone else interested in the currency. It gets more difficult to mine bitcoins the more leading zeros the hash has got. At the same time the computer is more likely to find a block at a given bitcoin difficulty when it has more computing power. Because of the above mentioned, the key to finding blocks of bitcoins is powerful hardware that can calculate as many hashes as possible in a short amount of time, while being as energy efficient as possible to make sure the miner earns a profit from this process.

The Bitcoin difficulty started out at 1 in the beginning and can never go below that. As mentioned above, in the ideal situation it is expected that a block of bitcoins is found every 10 minutes. With these calculations, it would take two weeks to reach the 2016 blocks when the difficulty change would appear. In case it took fewer days to find those 2016 blocks, the difficulty increases enough to make sure the next 2016 blocks are found in exactly two week time. Since the difficulty change itself is also only an estimate on how long it would take to find the next 2016 bitcoins, it is very likely that the actual period will not be exactly 2016 and there will be a change in difficulty taking place. In case it takes longer to find the 2016 blocks than the estimated two weeks, the difficulty would change. As can be seen from Figure 3, the difficulty in mining bitcoins has been in a growing trend since the beginning of Bitcoin network. This has been due to the massive improvements in the mining hardware that can find new bitcoins much faster. According to TradeBlock statistics, in the last 30 days, the difficulty has increased 4%, in 60 days it has increased 11% and in 90 days, the difficulty has increased 12% in total.

Figure 3. Change in difficulty in mining Bitcoins

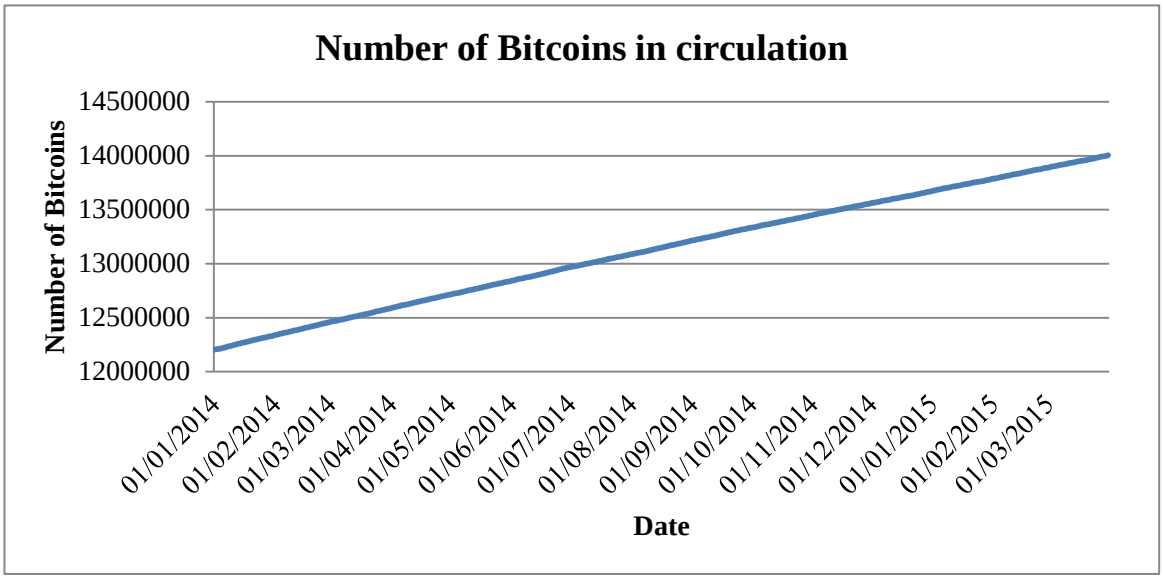


Source: Constructed by the author using statistics from BlockChain

Difficulty is calculated periodically so that every computed hash will lead to a valid block of bitcoins with the probability of$\frac{1}{2^{32}D}$, where *D* stands for the difficulty variable. With this a miner with a hash rate *h*, which in the given thesis is 30 GH/s, in a time period *t* will find on average $\frac{30t}{2^{32}D}$ blocks and her/his payout is $\frac{30tB}{2^{32}D}$, where *B* is stands for the amount of bitcoins in one block (Rosenfeld 2011: 1).

Figure 4 displays the change in the number of Bitcoins in circulation starting from 2014. It shows that the number has been in a stable, constant growth.

Figure 4. Total number of bitcoins in circulation



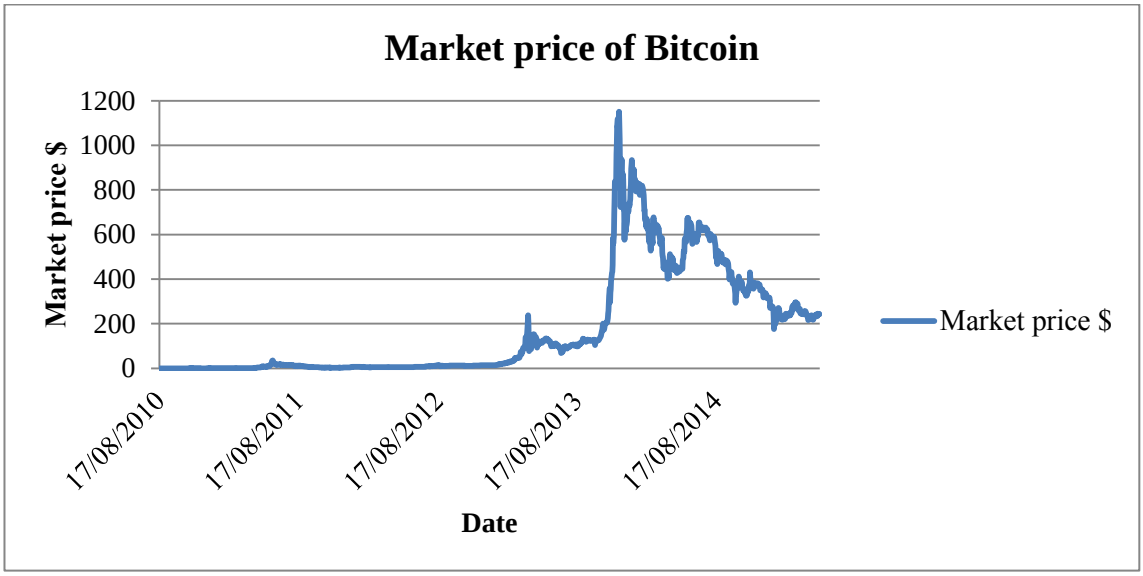
Source: Constructed by the author using statistics from BlockChain

Estimating how much the network mining difficulty will change even in the short term is very hard with any degree of accuracy. There are several methods for forecasting the future difficulty but it is done so only for a short period and no estimates have been made for the change in difficulty over a longer time period. As mining new bitcoins has become much more costly because of the large number of miners and the advanced hardware and its initial purchasing cost, it is very likely that the number of miners will drop and that the mining hardware will not continue to develop in such a fast pace. On top of that, in 141 902 new blocks, the reward for finding a new block will also drop by half, making the mining even less rewarding. With all of this and the lowering price of Bitcoin, the change in difficulty is also expected to drop. As these are all just estimates, it is impossible to actually estimate the change in difficulty over a long period of time. As difficulty still plays an important role in the simulation analysis of this thesis, it has to be taken into account. The average change in difficulty in the last 3 months has been 2.48% in every two weeks and the average since the beginning of 2014 has been 10.94% in every two weeks (Blockchain).

3.3.2. Volatility

With the rise of Bitcoin into mainstream consciousness, the issue that has received the most attention has been the high price volatility of the virtual currency. Skeptics have opined that this volatility will preclude bitcoin from ever replacing traditional fiat currencies given the fluctuating purchasing power inherent in the volatility, while regulators worry that this volatility poses a systemic risk to investors and users and should thus be given enhanced scrutiny (Baek, Elbeck 2014: 30). There is no one right answer to what drives the price of Bitcoin but several researches such as the research by Kristoufek, 2013 and Bouiyour, Refk, 2014 suggests that one possible driver of the Bitcoin prices is its popularity- the increased interest in the currency by the media, connected with a simple way of actually investing into it, leads to an increasing demand and thus increasing prices.

Figure 5. Market price of Bitcoin



Source: Constructed by the author

Figure 5 displays the changes the Bitcoin price has gone through since the value of Bitcoin exceeded zero in 2010. It has been estimated that once Bitcoin has been in the market for a longer period of time, the volatility will eventually start to decrease, which can also be seen from the latest trends in the figure 5. The estimated Bitcoin volatility on 11th of May was 2.28% (Bitcoin Volatility…). The given percentage is a measure of

historical volatility based on past Bitcoin prices. When the Bitcoin options market matures, it will be possible to calculate Bitcoin's implied volatility, which is in many ways a better measure (Dwyer 2014: 87). For comparison to the Bitcoin volatility, the volatility of gold averages around 1.2%, while other major currencies average between 0.5% and 1.0% (Bitcoin Volatility…).

Because the market price of Bitcoin is very difficult to assess in a long run as there is no general agreement on what really drives the price exactly, it cannot be argued for sure that the volatility will lower. In 2014 Foundersgrid asked 50 Bitcoin experts what they think will happen to the price of Bitcoin in the next 12 months. The answers received were very different but a popular belief was that the price of Bitcoin will again skyrocket, whereas figure 5 clearly shows the trend was different and the price has been lowering for a considerable time already. The answers the experts gave and the actual market price of Bitcoin clearly show there is no way of telling what will happen to the market price of Bitcoin over a longer period of time.

3.3.3. Electricity Price

The Bitcoin network is solely reliant on the work of miners who contribute their computers' power to mine new bitcoins and verify transactions. As the network of miners grows, so does the amount of electricity the devices that mine bitcoins use. There have been many estimates to how much energy the network has consumed as a whole. Fred Trotter, a co-founder of data journal and software company Not Only Dev estimated that with the five years that the Bitcoin network has operated, the computers that do the mining have spent over 150,000 mW/h of electricity, which is enough to keep the Eiffel Tower lit for over two and a half centuries (Clenfield, Alpeyev 2014). Forbes brought out that in 2013, bitcoins consumed on average around $15 million worth of electricity each day (Worstall 2013). In reality it is not possible to calculate the exact power consumption of the network as miners use different machines with very different efficiency rates, therefore only estimates can be made as to what is the amount of electricity the bitcoin network requires.

As electricity is an important factor in determining whether or not mining bitcoins is profitable, it can be argued that choosing the right location has a big impact on the results. The right location for mining is somewhere where the cost for electricity is as low as possible. However the location cannot only be determined solely by the price of electricity. As the machines intended for mining are supposed to mine full time day and night they also create a lot of excess heat and that might require fans and air conditioners to cool down the devices in case the hardware is situated in a warmer climate. It is also important to choose a location where there is no electricity blackouts occurring that would stop mining.

Estonia fits to many of the criteria that were brought out above- it has an affordable electricity price that is lower than the average electricity price average consumers pay within the European Union. It also has a climate that is suitable for mining as the temperatures are low enough and blackouts are very rare, due to which one can be certain a mining device can run 24 hours a day to make sure the miner earns maximum profits.

4. PROFITABILITY FROM MINING BITCOINS

4.1. Methodological approach

This chapter introduces the methodological approach the given thesis uses in the simulation analysis in order to realize the revenue earned from mining bitcoins over a longer period of time and also to determine whether mining bitcoins in the given simulation analysis can be seen as a profitable activity. In order to analyze the above situation, the thesis uses quantitative data from Blockchain Bitcoin database and BTC Guild. In estimating the payout function of the mining pool, theory and research by Rosenfeld 2011 will be used.

The empirical part of the thesis follows the structure similar to a Bitcoin mining calculator that aims to estimate whether or not a miner is earning a profit from her/his actions. The difference between the mining calculators and the thesis is that when calculators do the same calculations as the thesis will, they estimate the miner to mine solo- e.g. they receive proportional reward for their hashing power contribution and do not benefit from others findings. Research by Eyal *et al*, 2013 suggests that in order to earn profit, miners behave strategically and form mining pools. The thesis will use the total hashing power of the mining pool instead of the whole network together with the blocks found by that pool and compares it to the individual's proportion and how much the miner will get a reward for that.

There are multiple different online calculators that allow the user to estimate if they are making a profit or not. Some of the calculators take into account the change in difficulty and some only provide instantaneous calculations. The estimated expected Bitcoin earnings a calculator gives are based on a statistical calculation using the values entered and do not account for difficulty and exchange rate fluctuations and pool efficiency. Therefore the results calculated by using any of these calculators does not firstly provide long term estimates and secondly does not take into account the pool efficiency

which is one of the most important determiners in how many Bitcoins a miner earns per day.

The results these mining calculators can vary greatly depending on how much they estimate the change of difficulty to be at a given time period, what are the transaction fees, etc. Table 1 gives an overview of some of the most popular online mining efficiency calculators available and the results they provided.

Table 1. Results from different online mining calculators

Calculator	**Daily profit $**	**Break Even**	**Link**
Calculator 1	-0.001	never	https://bitcoinwisdom.com/bitcoin/calculator
Calculator 2	-0.270	never	http://www.coinwarz.com/cryptocurrency
Calculator 3*	0.070	not given	https://alloscomp.com/bitcoin/calculator
*Note on the calculator that it does not attempt to extrapolate difficulty or price changes and provides only instantaneous calculations			
Calculator 4	-0.250	no break-even in first year	https://tradeblock.com/mining/
Calculator 5	0.043	not given	http://bitcoin.web-share.nl
Calculator 6	-0.260	never	http://www.vnbitcoin.org/bitcoincalculator.php

Source: Constructed by the author using data from the websites provided in the table

The formula given below shows how most mining calculators estimate the income a miner receives from mining.

$$(5)\ \frac{User's\ Hashrate}{Total\ Hashrate} \times \frac{(Reward + Transaction\ fees)}{600s} \times 86400s = Income\ (BTC)$$

User's Hash rate is the hash rate an individual contributes to the mining process, *Total Hash rate* is the combined has rate of all of the miners, *Reward* is the amount of bitcoins that are included in one block that the solver of the equation gets as a reward

and on average in every 10 minutes one miner receives this award, which is 600 seconds. Currently there are 25 bitcoins per one block. *Transaction fees* are part of the reward that the miner receives and these are the transaction fees the miner validated when trying to find a new block. Users are free to offer any amount as a transaction fee, but miners prioritize transactions based on the size of the reward therefore the transactions with bigger rewards get validated sooner. Usually transaction fees sum up to between 0.01 and 0.25 bitcoins per one block. As there are 86400 seconds in one day then the *Income (BTC)* shows how much a miner would earn in one day.

The outcome formula consists of the fixed costs and operating costs. Similarly to online mining calculators, the thesis does not take into account the depreciation of the mining hardware. On the operating costs side there is the cost of electricity, which is the biggest factor in determining whether it is a cost. Fixed costs are the costs the miner spends on shipping and buying of the hardware.

The analysis is divided into three parts where the first part looks at the earnings one might expect from mining, the second part looks at the expenditures a miner has to take into account. With these two parts it is possible to put together an estimate on the profitability from mining Bitcoins, which is the third part. The profit function for mining bitcoins in one second is given below.

(6) $$Profit = Mining\ reward - Electricity\ cost - Hardware\ cost$$

4.2. Data

The current analysis investigates whether mining bitcoins in a BTC Guild mining pool with an ASIC Little Single miner is profitable for the miner and tries to estimate the time the miner needs to start earning a profit from her/his investment. The statistics concerning the mining pool are taken from the official webpage of BTC Guild. The hardware that is used in the given thesis is an ASIC mining device Little Single by Butterfly Labs, which is one of the biggest producers of Bitcoin mining hardware. Based on the research by Wang and Lo at New York University and also the common

belief of the Bitcoin mining community, ASIC miners are the only ones worth considering for a serious miner thinking about entering the market. Firstly, ASIC devices are solely developed for mining bitcoins and as the level of difficulty of mining bitcoins has gone through a tremendous rise since the launch of the virtual currency and will continue to rise, it has been brought out by many miners that personal computers and other hardware are too weak to mine bitcoins and ASIC devices are needed to earn an actual profit from mining. Secondly, there is no programming needed to start mining with an ASIC device- it will automatically start to mine once plugged in.

The price of ASIC Little Single hardware by Butterfly Labs is $1263.9. The price is taken from one of the biggest online marketplaces- Amazon, where on 28th of March the device was for sale for $1263.9 including shipping worldwide (appendix 1). The thesis chose to use the ASIC Little Single device due to its affordable price. Even though many ASIC devices can mine several times more of giga hashes per second, the initial investment would also be much more expensive. The data about electricity prices is taken from Eurostat.

The statistics from BTC Guild that are used for this simulation analysis are from 3rd of March until the 31st of March. Based on this statistics it is calculated how many of the 10 shifts that start mining for bitcoins per day actually find bitcoins and the average result is used. The analysis also calculates the daily payoffs for the period of March 3rd until March 31st to see how much the result differs from the average monthly result. Unfortunately the BTC Guild does not provide exact statistics on pool luck, which means that for all calculations the average pool luck for a three month period is used, which on April 1st was 91.39%.

The analysis will use several Bitcoin market prices from different time periods to see how the payoff would change in time as Bitcoin is known for its volatility and therefore there might be a scenario where mining Bitcoins will result in a loss due to a low market price or a scenario where in a short time it is possible to earn back the money spent on the mining device and make a profit from mining Bitcoins.

4.3. Simulation Analysis

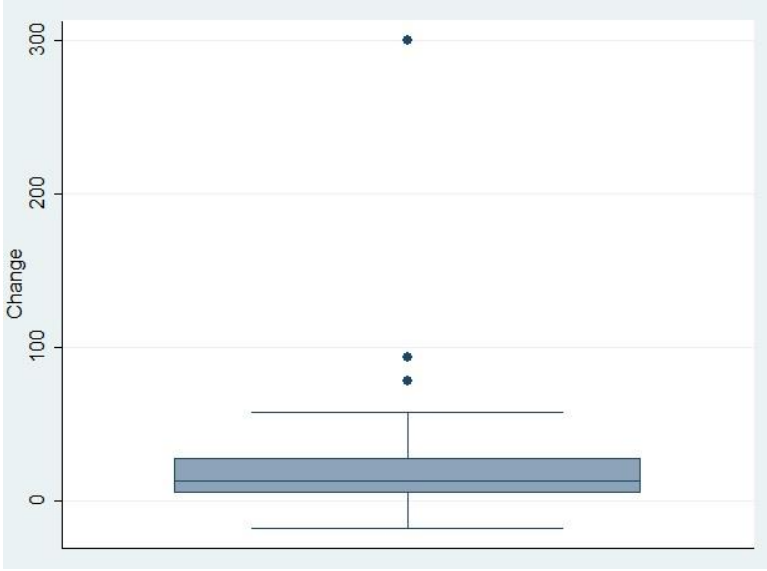
4.3.1. Estimating Change in Difficulty

The importance of difficulty in mining bitcoins is essential, as it is one of the key factors determining whether it is profitable to mine bitcoins or not. Up until now, the difficulty has seen a rapid growth but it is not known how and with what speed the difficulty will continue to grow. Even though there are many ways to best make future predictions, then for something as new as mining bitcoins, there is no research available on what would be the proven best method of estimating long term or even short term changes in difficulty. After the block reward will halve from 25 blocks, it is already impossible to see what impact it will have on the market. Currently there are still 141 902 blocks to be mined with the 25 bitcoins per block reward.

The block reward miner receives in case the hardware successfully solves the necessary equation halves in every 210 000 blocks, which is approximately 4 years. When currently the reward is at 25 bitcoins per block then it is widely expected that the next halving will take place already in 2017. It is expected that fewer Bitcoins will be mined going forward as network complexity reaches a higher level. Because of this, the thesis will estimate the change in difficulty only until 2017, as the situation will change completely at that stage and it is impossible to assess the magnitude the reward halving will have on the price of the Bitcoin and the mining industry.

The average change in difficulty in the last 3 months (first quarter of 2015) has seen a growth of 2.96% in every two weeks and the average since the beginning of 2014 has grown 10.94% in every two weeks. The overall change in difficulty since its eruption has seen an average growth of 18.76% in a two week period. There are however three extremum points that can be seen from figure 1 that are much larger than others, growing up to 300% change in only two weeks. Removing these tree points lowers the average change to 16.12% which is still a far bigger change than those that have occurred in the end of 2014 and 2015. The huge difference in these numbers gives idea of how unwieldy it is to estimate the change in difficulty over a period of time.

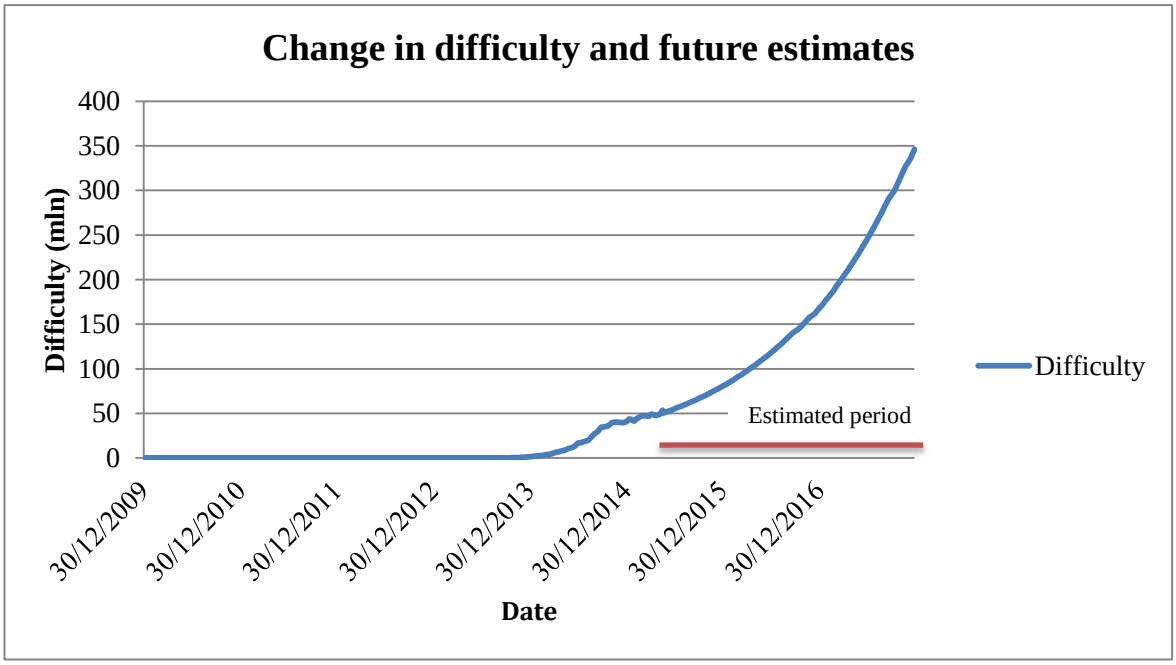
Figure 1. Extremums in difficulty change



Source: Constructed by the author

The simulation analysis will use the average difficulty of 2.96% for future estimates because the trend of difficulty has been lowering not only in 2015, but saw a decrease already in 2014. There can be many reasons for that- for example the fast paced development of mining hardware or the higher price of Bitcoins which made miners use more of their hardware to mine bitcoins and more attractive for new miners to enter the market.

Figure 2. Historic changes in difficulty and future estimates



Source: Constructed by the author

Figure 2 shows both the historic data of change in difficulty plus the estimates for future changes until the end of 2017 with the average change of 2.96% growth in every two weeks-time.

4.3.2. Revenue from mining in the BTC Guild mining pool

BTC Guild is a mining pool which offers proportional Pay-per-last-N-shares (PPLNS) based rewards, where a persons' reward is equal to the block value, multiplied by her/his valid shares submitted during the round. The pool is run off the donations of users which are taken from the individual user's reward when a block is calculated. BTC Guild stands out from other mining pools because of the amount of information that is shared with the miners and public, which is considerably larger than the amount of info shared by many other pools.

The given analysis uses the statistics of March 2015 to determine the average number of blocks mined per day and the average hashing speed. The data is taken on a daily basis exactly at 6:11 PM. Table one displays data used in the analysis. The speed column shows the whole speed of the mining pool in tera-hashes per second. One tera-hash (Thash) equals 1000 giga-hashes (Ghash) and 1000000 mega-hashes (Mhash). Since BTC Guild is one of the biggest and most renowned mining pools with lots of contributors and a considerable overall hashing speed, every day they manage to find several blocks of bitcoins. There can only be an integer number of blocks but as this simulation analysis will look at the daily average based on the statistics of March, the average number of blocks is not an integer. In a real life situation it would not be possible to mine something other than an integer number of blocks.

Table 2. Statistics from BTC Guild for March'15

Date	Speed (TH/s)	Little Single % of speed	Blocks mined	Block value	Total value per day
03/03/2015	14351	0.00021	5	25.15	125.73
04/03/2015	14408	0.00021	6	25.09	150.56
05/03/2015	15317	0.00020	4	25.17	100.70
06/03/2015	16065	0.00019	6	25.10	150.58
07/03/2015	15374	0.00020	4	25.08	100.33
08/03/2015	15787	0.00019	3	25.06	75.18
09/03/2015	15785	0.00019	8	25.19	201.51
10/03/2015	15945	0.00019	10	25.14	251.39
11/03/2015	16265	0.00018	7	25.04	175.27
12/03/2015	16796	0.00018	5	25.11	125.57
13/03/2015	16647	0.00018	7	25.11	175.80
14/03/2015	16626	0.00018	7	25.11	175.75
15/03/2015	16474	0.00018	9	25.08	225.71
16/03/2015	16414	0.00018	11	25.10	276.05

17/03/2015	17060	0.00018	10	25.10	251.05
18/03/2015	17219	0.00017	11	25.11	276.24
19/03/2015	18128	0.00017	3	25.18	75.55
20/03/2015	16864	0.00018	6	25.09	150.52
21/03/2015	16901	0.00018	7	25.13	175.93
22/03/2015	17006	0.00018	5	25.13	125.67
23/03/2015	16820	0.00018	5	25.08	125.41
24/03/2015	16425	0.00018	3	25.08	75.24
25/03/2015	16684	0.00018	8	25.07	200.56
26/03/2015	16598	0.00018	7	25.15	176.06
27/03/2015	16328	0.00018	7	25.09	175.64
28/03/2015	16215	0.00019	6	25.09	150.54
29/03/2015	15824	0.00019	6	25.08	150.46
30/03/2015	15353	0.00020	4	25.10	100.40
31/03/2015	16089	0.00019	5	25.06	125.32
Average	**16268**	**0.00018**	**6.38**	**25.11**	**160.16**

Source: Constructed by the author using statistics from BTC Guild

One block consists of exactly 25 new bitcoins that are mined and then launched to the circulation. While mining new bitcoins, the miners also validate transactions that have occurred between the users of bitcoin. Based on how many transactions are validated, miners who collect a block also receive a bonus for validating transactions and adding them to the block chain. This bonus is different for all blocks as it is related to the number of transactions that have occurred. Blockchain gives information that in March 2015, there were on average 673.17 transactions per block for what on average miners earned 0.11 BTC per mined block a day. It is common for mining pools to collect the money received from transactions validated for running the mining pool. In the case of BTC Guild, the pool does not keep the transaction fees but instead charges a 2% fee of mined bitcoins. However, as mentioned above, the pool has estimated that the amount

of transaction fees and Namecoins will on average reduce the pool fee to 1% and this thesis uses this estimate. Therefore in the analysis the transaction fees are not included in the calculation and instead the pool fee is lowered to 1%.

Based on table 2 it can be seen that on average there are 6.38 blocks mined every day, making the daily average total value of bitcoins mined 159.48. Every day the BTC Guild earns 0.68 bitcoins from transaction fees plus the 1% fee they receive from all of the miners' revenue.

All of the blocks that are found are divided by 10, so that 10 of the pools that started last would earn an equal share even if their pool did not manage to find any blocks. Since there are 6.38 blocks found per day on average and the BTC Guild's average pool luck according to the statistics of three months is 91.39, the pay-out for an average day would be:

(7) **(Block Value / 10) - Pool Fee (1%)**

(8) $$\left((\mathbf{159.48} \div \mathbf{10}) - \mathbf{1}\%\right) * \mathbf{0.9139} = \mathbf{14.43}$$

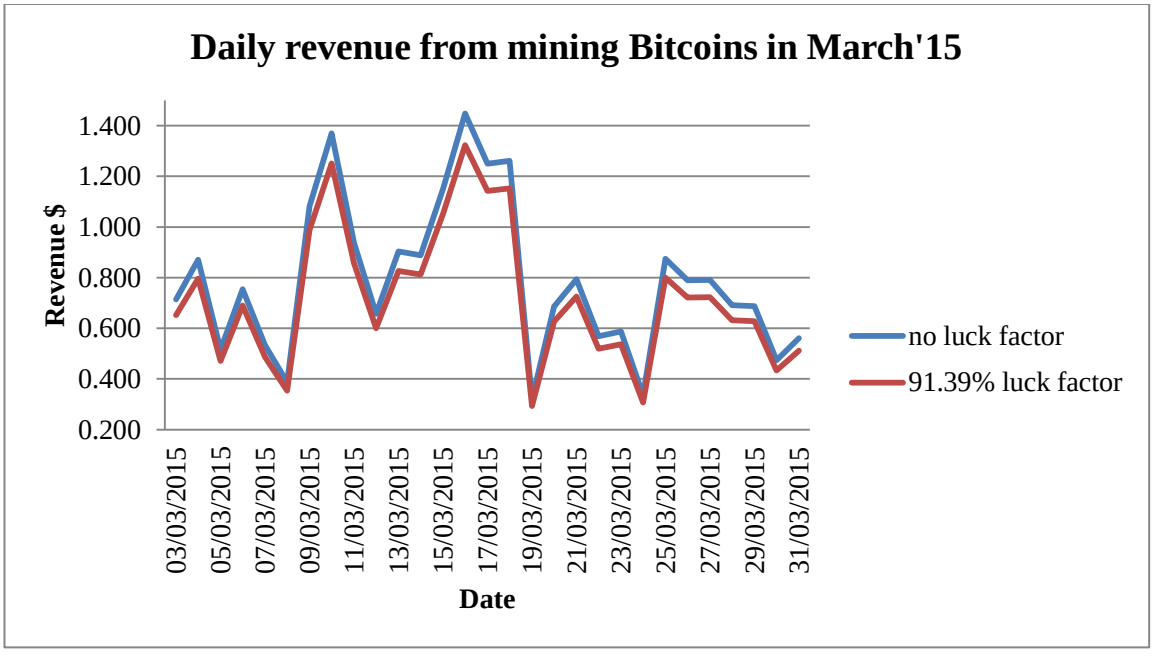
Because the analysis is making long term estimates about the profitability of mining bitcoins, the pool luck will be 100% instead of 91.39%, as the pool luck is taken into account only in short term estimates. With this the daily pay-out grows from 14.43 to 15.79 bitcoins.

This 15.79 is the amount of bitcoins one shift receives per day on average. In order to find out how much each miner receives individually, the amount of hashing power they put into mining is taken into account and each miner receives proportionally the amount they are supposed to from the hashing power they put into work. The ASIC Little Single that is used in the simulation analysis hashes 0.03 TH/s. Table 2 displays the hashing speed of the period under consideration which is on average 16267.86 TH/s, therefore the ASIC Little Single with its 0.03 TH/s forms on average 0.00018% of the pools whole speed and therefore the user of ASIC Little single miner would receive 0.00018% of bitcoins one shift receives. The miner with the given hardware would therefore earn on average revenue of 0.0027 bitcoins per day.

On 1st of April 2015 Coindesk valued the price of Bitcoin to be at 246.55 dollar. With this price the revenue earned per day from mining a bitcoin would be 0.621 dollars.

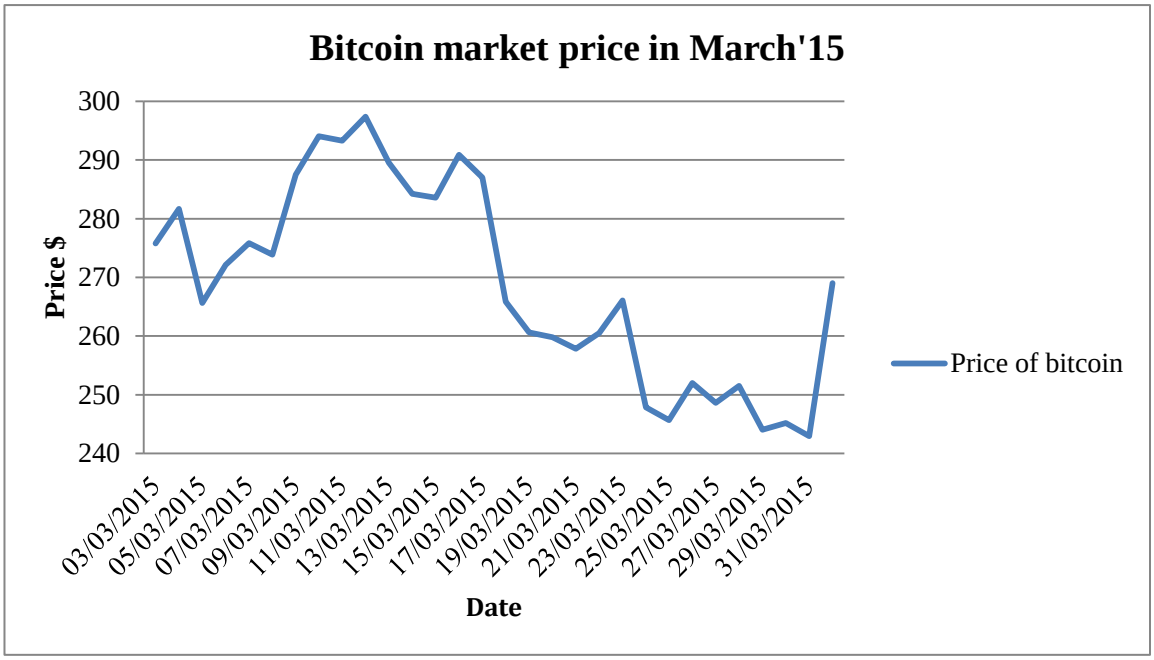
Because Bitcoins are very volatile and their price can change rapidly, the revenue might go through drastic changes even in a short amount of time. Below is a daily revenue analysis for March 2015 with the pool luck included and excluded as for a short term analysis such as monthly analysis, pool luck is an important factor but for a long term analysis determining when the initial investment will be paid off it is irrelevant. Due to the fact it was not possible to get daily information on how the pool luck was changing during the given period, all of the calculations use the 3 month average luck 91.39%. Figure 3 clearly displays that the revenue is in a constant change and no day is similar to the previous one. In comparison to figure 3, figure 4 displays the daily basis market price of Bitcoins in March 2015 to give a graphic overview of the trend. The figures are different as the market price of Bitcoin is only one of the factors behind the revenue.

Figure 3. Daily revenue from mining Bitcoins in March'15



Source: Constructed by the author

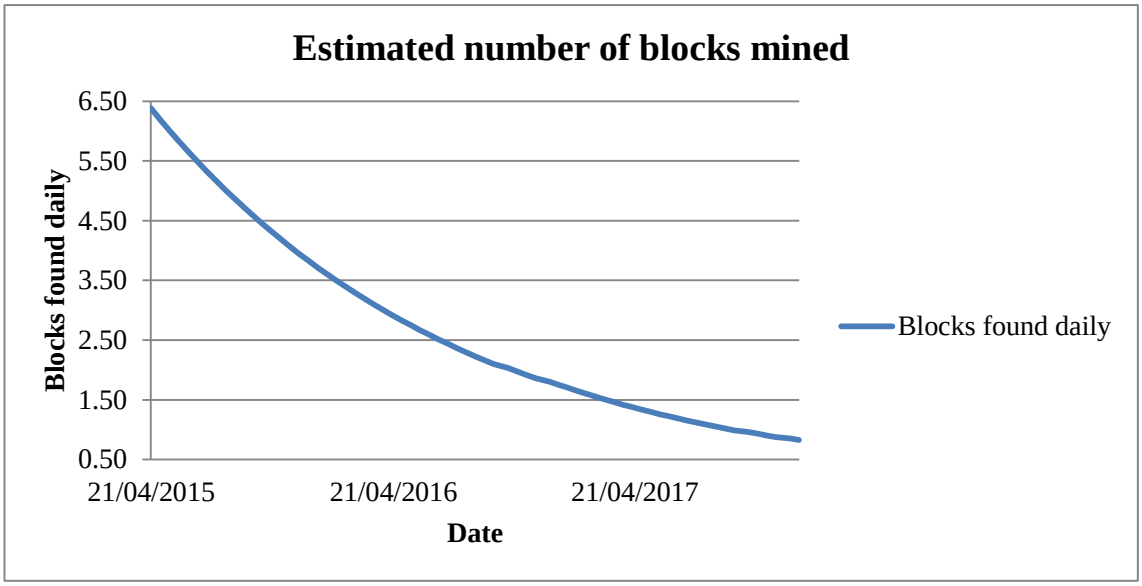
Figure 4. Bitcoin market price in March'15



Source: Constructed by the author

As the above analysis looks at the average revenue based on one month, then in order to look at the revenue over a longer period, the difficulty change also has to be taken into account, as it makes mining for new bitcoins more and more difficult therefore lowering the revenue in case other parameters remain the same. The difficulty change that will be used in the analysis is 2.96% for a two week period. This 2.96% means that in every two weeks it will become 2.96% more difficult to mine for these 6.38 blocks, therefore in a case where the hashing power of the network, the individual contribution and the amount of blocks found in a day would remain the same and only difficulty would change, in every two weeks the pool would find 2.96% less of the blocks it found in March. Figure 5 displays the estimated number of blocks found with the 2.96% difficulty change.

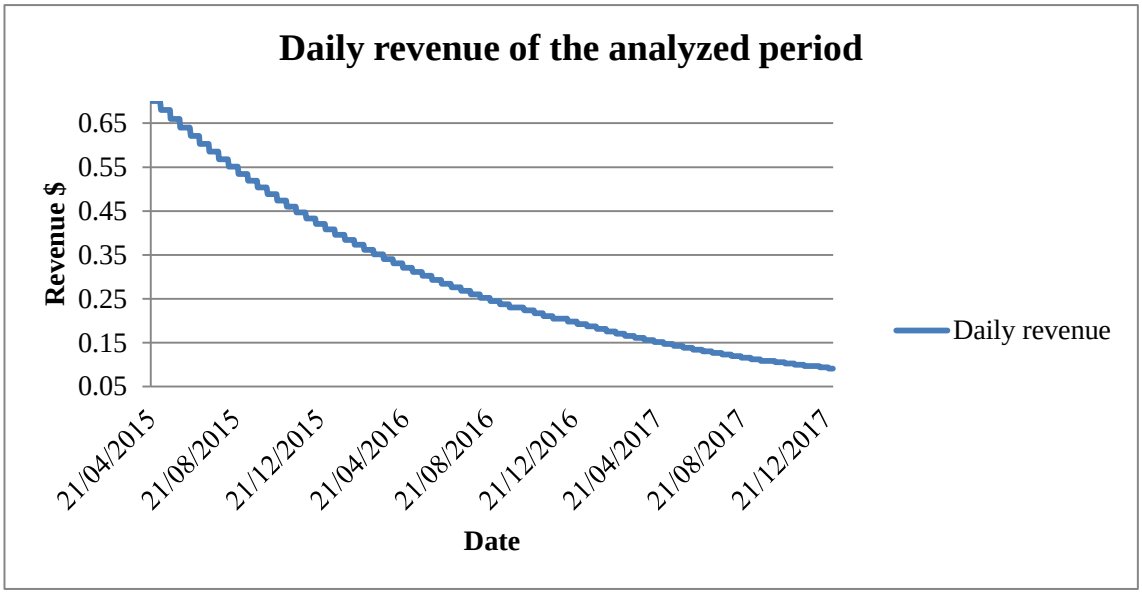
Figure 5. Estimated number of blocks found daily until the end of 2017



Source: Constructed by the author

Because the Bitcoin reward will halve in every 210 000 blocks, and there are over 140 000 blocks halved with the 25 bitcoins per block reward, then it is estimated that sometime in 2017 the reward will halve again. Due to the fact that there are no clear estimates to how this halving will change the mining industry, the analysis will be conducted only until the end of 2017. During that time the daily revenue will go through a considerable change and drop from 0.7 dollars to 0.09 dollars as can be seen from figure 6, which displays the daily revenue changes in the analysed period.

Figure 6. Daily revenue change in the analysed period



Source: Constructed by the author

During the period given in figure 6, the individual mining with an ASIC Little Single device will earn cumulative revenue of 293.42 dollars, making the average daily revenue 1.19 dollars. This estimate is on the basis that the price of Bitcoin will remain at 246.55 dollars per Bitcoin as it was valued by Coindesk on 1st of April 2015.

4.3.3. Expenditure

There are two expenses that need to be taken into account when calculating the profitability of a mining hardware- the purchasing price of the hardware and the cost of electricity. The purchasing price is a fixed cost and in this analysis it is 1263.9 dollars including also the price for shipping. The operating cost is the cost of electricity that is spent on keeping the mining device running throughout the day.

The electricity price that the analysis uses is the electricity price charged to final consumers. The price used is defined by Eurostat as follows: "Average national price in Euro per kWh without taxes applicable for the first semester of each year for medium

size household consumers (Consumption Band Dc with annual consumption between 2500 and 5000 kWh) (Eurostat 2015). In Estonia household users need to pay a 20% tax on electricity (Estonian Tax…2015). Table 2 displays the electricity prices to the end user both in 2013 and 2014, in the analysis only the statistics from 2014 will be used and it is displayed in the table for mere comparison basis. The prices are converted to dollars with the conversion rates of the European Central Bank on 1st of April 2015. In 2015, the Estonian end user paid 0.169 dollars per kW/h of electricity.

Table 2. Price of electricity average household end user in euros and dollars

Year	Without tax (€)	With tax (€)	Without tax ($)	With tax ($)
2013	0.135	0.162	0.145	0.174
2014	0.131	0.157	0.141	0.169

Source: Constructed by the author using data from Eurostat and European Central Banks

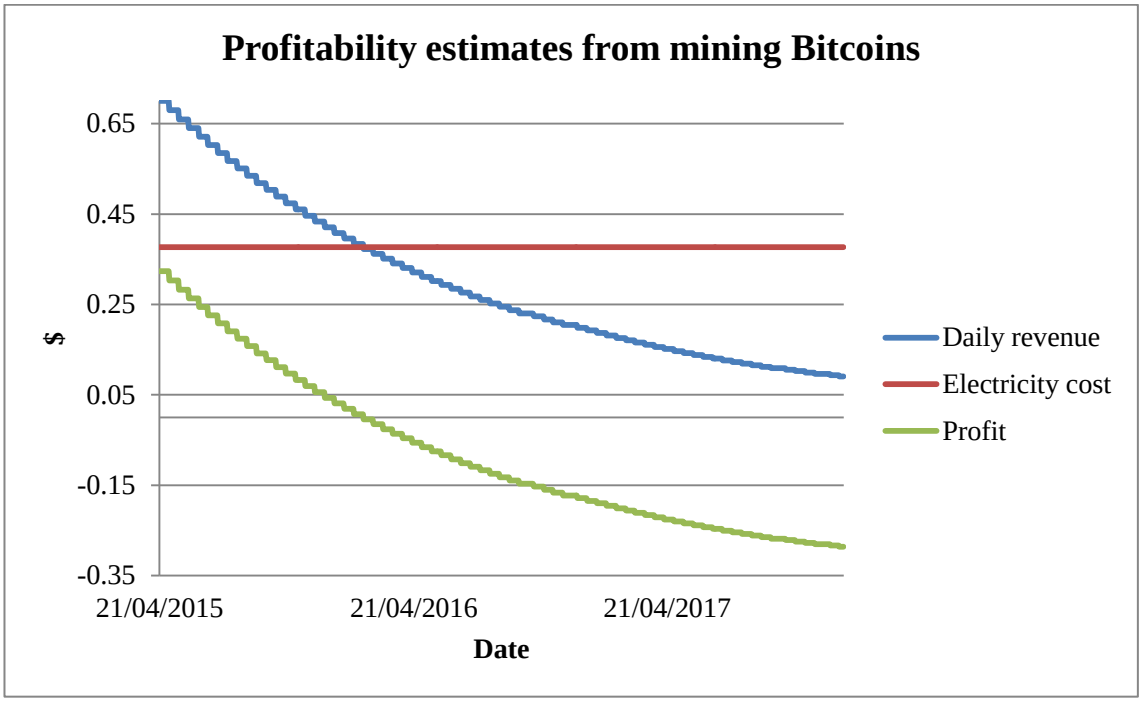
The analysis expects the mining device to be running non-stop all day consuming on average 0.093 kW/h, therefore per day the ASIC Little Single machine consumes approximately 2.232 kW/h. With the average price of $0.169 per kW/h, in one day the ASIC machine consumes $0.377 worth of electricity. The average daily profit excluding fixed costs and with the Bitcoin market price on April 1st 2015 would then be $0.244 on average in the month of March 2015.

Due to change in difficulty, the revenue is estimated to decrease in every two weeks; the amount of electricity the device consumes will however remain the same. The thesis will not estimate the change in the price of electricity and will use the same price for electricity throughout the analysis.

4.3.4. Profitability from mining Bitcoins

Figure 7 displays the profitability estimates from mining Bitcoins without the fixed costs. As can be seen, then in the first part of 2016 the mining already becomes unprofitable and starts to earn loss, which increases even more every time the difficulty factor increases. As a result of this analysis, the mining activities should be stopped on 9th of February 2016.

Figure 7. Profitability estimates from mining Bitcoins



Source: Constructed by the author

By the time the mining activities become unprofitable, the Little Single machine would have earned its user revenue of $44.25, which is only around 3.5% of the investment that has to be made in order to purchase the mining device. Based on that it can be concluded that mining in a current situation is not profitable and one of the factors needs to change notably- either the market price of Bitcoin, the price of electricity or the difficulty factor. Because however the price of Bitcoin is very volatile and exactly a year ago on April 1st 2014 the market price of Bitcoin was $479.51, estimates for the

profitability cannot be made solely based on the price of Bitcoin at one point of time and different scenarios must be looked at.

With the price of $479.51 the mining activities should be stopped at 10th of January 2017 and up until that time the without taking into account the initial investment, a miner would have earned a profit of $241.17, which is already considerably bigger from the profit that a miner would earn with the current Bitcoin market price. Nevertheless even when the market price would be $479.51 instead of $246.55, it would still not be enough to pay off the initial investment. In order for the miner to pay of the initial investment and earn no overall profit from mining activities, the market price should be $1370 throughout the period. This market price however seems unrealistic as currently the market price has reached its highest value of $1124.76 on 29 November 2013, the price subsequently dropped into the $200-$300 range (Wang, Lo 2014: 2).

As a result of the simulation it can be thus said that it will not be profitable for a new miner to enter the market in case there is no dramatic increase in the Bitcoin market price. The only way to still make profit off mining is in case the price of electricity would be diminished for example through renewable energy or in case the mining hardware would come at a very affordable price e.g. in case the miner would be able to build the mining hardware on his/her own. For an average miner however to whom the electricity is not free and who does not possess the ability to build the hardware and has to buy it, it does not make sense to enter the mining market at this point.

5. DISCUSSION

Bitcoin, a modern day virtual gold, has managed to do something in its mere 6 years of existence no virtual currency has before- take this topic into mainstream media. With the increased media attention the virtual currency has received, it also sparked the interest of many people. This attention can be seen as the core leader behind the exponential growth the currency has seen. The booming market price Bitcoin went through made people became more interested in the process of mining bitcoins, as it seemed like an easy way to earn money without having to do much work. When in the beginning mining really was a very profitable action, then recent trends show otherwise because due to the increased number of miners the Bitcoin network started to adjust itself to make sure the reward time scale would remain its current level.

Mining was a very profitable action for a very long time because of the high Bitcoin market price and low level of difficulty. However both of these factors have changed drastically with a relatively short time to a situation where new miners need to critically assess whether to enter the market as a miner or not and current miners to evaluate when to turn off their mining hardware as it is no longer profitable to keep it running and consume electricity.

The high hardware prices and the falling market price of Bitcoin are not the only things miners need to take into account when estimating their returns. Because of the Bitcoin reward system, in every new 210 000 blocks the reward for finding a block halves. The reward started out with a 50 bitcoin reward per block and halved into 25 once 210 000 blocks were found. As can be seen from the results of the above analysis, due to the increased level of difficulty and market price of Bitcoin, the mining activities can already be seen as non- profitable for a new miner who has to make the initial investment and buy the mining hardware, then when the reward halves again to 12.5 bitcoins per block, it becomes non-profitable to those miners as well, who started

mining in the earlier stages and have managed to earn back the money for their initial investment.

Although as a reward, miners also receive transaction fees, they are currently voluntary by the rules the network has set, they cannot compensate for the difference that is caused by the halving of the reward. Even in a situation where the transaction fees would be made obligatory for all, this would not be enough to cover the difference caused by the halving in case there is no substantial growth in the percentage the transaction fee forms from the payment. This percentage however needs to remain low as otherwise there would be no incentive to make transactions in Bitcoins in case the transaction fees exceed those of banks. The raising of transaction fees would also go against the initial idea behind the Bitcoin network which was to offer a global and secure platform with low transaction fees.

Because mining plays an essential role in the Bitcoin network, it is vital for the existence of the virtual currency that the miners have an incentive to keep on mining to validate transactions and release new bitcoins to the market. When the market reaches a point when it is no longer profitable to mine bitcoins even for a person whose initial investment has already been paid off, the network needs to restructure itself to make it appealing again. The need to restructure the Bitcoin network has also been brought out in a research by Kroll *et al* 2013. Even though there have been some ideas on how to restructure the network in order to keep it still appealing, these have only remained as small suggestions and most likely the topic will remain unpopular up until the point the reward actually halves and mining becomes unprofitable for a majority of the mining community.

There are many possibilities as to what might happen with Bitcoin. In case the market price would again start to rise and achieve a high enough level, it might be sufficient enough for miners to receive most of their rewards as transaction fees and not through newly launched bitcoins. There is also a possibility to restructure the reward system and increase the amount of bitcoins miners receive as a reward in one block. Another possibility is that the Bitcoin network will just slowly cease to exist or remain in the interest of a very small group of enthusiasts in case the market price continues to drop and no changes are done to the reward system.

6. CONCLUSION

Bitcoin is the world's first virtual currency system that was proposed as an alternative to fiat currencies. It has provided an innovative solution to the problem of double spending through the usage of peer-to-peer network. There is no third intermediary in the Bitcoin network and it is solely run by people who are interested in it and are willing to contribute their computers for the sake of the network. In order to make sure enough people are willing to contribute their computers power for the Bitcoin network and become a miner, there are incentives one can receive through mining bitcoins. Due to the falling trend of the market price of Bitcoin and the increased difficulty in finding new blocks and thus earning a reward for mining, it is no longer certain whether the mining market is appealing enough for a newcomer.

The given thesis analysed whether mining Bitcoins is a profitable action from an average miners' perspective. Even though there are mining calculators available online that try to estimate the profitability of mining, the calculators calculate the possible reward of the miner from the percentage of how much the miners' computer contributes to the whole network. In the given thesis however it is expected that the miner is mining in a pool and the contribution of the miner's hardware is compared to the overall contribution and reward of the mining pool and not the whole network. This approach is also supported by many researches that bring out that mining pools are the best for new and small miners.

As a result of the simulation analysis it can be concluded that even though mining was a very profitable action some years ago, then due to the increased difficulty and the high hardware prices, it is not profitable for a new miner to enter the market any longer, as the expected reward would only cover around 3.5% of the initial investment. The only considerable way to earn from mining at this current state is for miners who already possess mining hardware and have already earned this investment back and now only need to cover the cost of electricity from the revenue they earn from mining.

Due to the halving of the mining reward some time in 2017, mining might become non-profitable also for the miners who have entered the mining market sooner and don't need to invest in hardware anymore as with the halved reward they might not earn enough to cover for the electricity their hardware's' consume from the reward they earn. This is something the Bitcoin network needs to find answers to as mining is essential to the Bitcoin network and without it cannot exist.

In the beginning of the thesis five research objectives were set to meet the goal of the thesis and know whether it is still profitable for a new miner to enter the market. All of the objectives were successfully addressed and the research method was designed similar to online calculators with the exception of changing the whole network's contribution in the mining calculators with the contribution of the chosen mining pool. As a result the thesis found that in the given situation it is not profitable for a new miner to enter the market, as the overall profit would only be $44.25, which covers only 3,5% of the initial investment. In order for the market to become appealing again for new miners, considerable changes have to take place in order for mining to become profitable enough to cover for the initial investment that is the price of the mining hardware.

REFERENCES

1. **Ala-Peijari, O**. Bitcoin The Virtual Currency: Energy Efficient Mining of Bitcoins. Aalto University, 2014, 81 p. [https://aaltodoc.aalto.fi/bitstream/handle/123456789/14102/master_Ala-Peijari_Ossi_2014.pdf?sequence=2] 15.01.2015

2. **Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S**. Evaluating User Privacy in Bitcoin. - Sadeghi, & Ahmad-Reza (Ed.), Financial Cryptography and Data Security, 2013, pp. 34-51.

3. **Babaioff, M., Dobzinski, S., Oren, and S., Zohar, A**. On Bitcoin and Red Balloons. - ACM New York, NY, USA, 2012, 56-73 pp. [http://research.microsoft.com/pubs/156072/bitcoin.pdf] 18.04.2015.

4. **Badev, A., Chen, M**. Bitcoin: Technical Background and Data Analysis. - Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board, Washington, D.C. 2014, 104 p. [http://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf] 02.02.2015.

5. **Baek, C., Elbeck, M**. Bitcoins as an Investment or Speculative Vehicle? A First Look. – Applied Economics Letters, 22:1, 2014, pp. 30-34.

6. **Barber, S., Boyen, X.,Shi, E., and Uzun, E**. Bitter to Better — How to Make Bitcoin a Better Currency. – A.D. Keromytis (Ed.): FC 2012, LNC 7397, 2012, [https://crypto.stanford.edu/~xb/fc12/bitcoin.pdf] 24.04.2015.

7. Bitcoin Market Capitalization. Blockchain.
[https://blockchain.info/charts/market-cap]. 10.02.2015.

8. Bitcoin Mining Calculator 1. BitcoinWisdom.
[https://bitcoinwisdom.com/bitcoin/calculator]. 05.02.2015.

9. Bitcoin Mining Calculator 2. CoinWarz.
[http://www.coinwarz.com/cryptocurrency]. 05.02.2015.

10. Bitcoin Mining Calculator 3. Alloscomp.
[https://alloscomp.com/bitcoin/calculator]. 05.02.2015.

11. Bitcoin Mining Calculator 4. TradeBlock.
[https://tradeblock.com/mining/]. 05.02.2015.

12. Bitcoin Mining Calculator 5. Bitcoin Mining Calculator.
[http://bitcoin.web-share.nl/]. 05.02.2015.

13. Bitcoin Mining Calculator 6. Bitcoin Mining Profitability Calculator.
[http://www.vnbitcoin.org/bitcoincalculator.php]. 05.02.2015.

14. Bitcoin Mining Profit Calculator.
[http://jblevins.org/btcmpc/]. 01.04.2015.

15. Bitcoin Pool Luck. BitcoinCZ Mining.
[https://mining.bitcoin.cz/proposal/detail/72/] 01.04.2015.

16. Bitcoin Symbol. Bitcoin wiki.
[https://en.bitcoin.it/wiki/Bitcoin_symbol]. 10.02.2015.

17. Bitcoin Volatility Index.
[https://btcvol.info/]. 25.03.2015.

18. Beginner's Guide to Mining Bitcoins. Start Bitcoin. [http://startbitcoin.com/] 12.05.2015

19. **Brito, J., Castillo, A**. Bitcoin A Primer for Policymakers. Mercatus Center at George Mason University, 2013. [http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf] 22.02.2015

20. BTC Guild. [https://www.btcguild.com/index.php?page=support&section=howamirewarded] 29.03.2015.

21. **Bundrick, H**. 2015 Bitcoin Forecast: Industry Insiders Predict What's Next for the Virtual Currency. - Inside Bitcoins, 1 January 2015. [http://insidebitcoins.com/news/2015-bitcoin-forecast-industry-insiders-predict-whats-next-for-the-virtual-currency/28228] 10.02.2015

22. Butterfly Labs. [https://products.butterflylabs.com/]. 01.04.2015.

23. **Buyuiyour, J., Selmi, R**. What Does Crypto-currency Look Like? Gaining Insight into Bitcoin Phenomenon. – MPRA Paper, 2014.

24. **Böhme, R., Brenner. M., Moore, T., Smith, M**. Game-Theoretic Analysis of DDos Attacks Against Bitcoin Mining Pools. Financial Cryptography and Data Security, 2014, pp. 72-86. [http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_16.pdf].19.04.2015.

25. **Böhme, R., Christin, N., Edelma, B., Moore, T.** Bitcoin: Economics, Technology, and Governance. - Journal of Economic Perspectives, Vol. 29, Issue 2, 2015.

26. Bitcoin Market Price. Coindesk.
[http://www.coindesk.com/]. 01.04.2015

27. **Clenfield, J., Alpeyev, P**. The Other Bitcoin Power Struggle. - Bloomberg Business. 24 April 2014.
[http://www.bloomberg.com/bw/articles/2014-04-24/bitcoin-miners-seek-cheap-electricity-to-eke-out-a-profit] 29.03.2015.

28. **Decker, C., and Wattenhofer, R**. Information Propagation in the Bitcoin Network. - Peer-to-Peer Computing (P2P), IEEE Thirteenth International Conference, 2013, 10 p.
[http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf] 01.05.2015.

29. Difficulty Change. Tradeblock.
[https://tradeblock.com/mining/]. 01.04.2015.

30. Difficulty Change. Bitcoin Clock.
[http://bitcoinclock.com/]. 01.04.2015.

31. **Drehmann M., Goodhart C. and M. Krueger**. (2002) "The challenges facing currency usage: will the traditional transaction medium be able to resist competition from the new technologies?." Economic Policy, 17(34), page 193-228.

32. **Dwyer, G**. The Economics of Bitcoin and Similar Private Digital Currencies. – Journal of Financial Stability, 2015, pp. 81-91.

33. Estonian Cryptocurrency Association.
[http://www.kryptoraha.ee/]. 04.05.2015.

34. Estonian Tax Rates. Estonian Tax and Customs Board.
[http://www.emta.ee/index.php?id=3274] 05.02.2015.

35. Eurostat Electricity Prices by Type of User 2003 – 2014. Eurostat. [http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=ten00117]. 05.02.2014.

36. **Eyal, I., Sirer, E**. Majority is not Enough: Bitcoin Mining is Vulnerable. Department of Computer Science, Cornell University. 04 November 2013, 17 p. [http://arxiv.org/pdf/1311.0243v2.pdf] 25.03.2015.

37. Federal Bureau of Investigation Directorate of Intelligence. Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity. 24 April 2012. [http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf] 10.02.2015.

38. **Garay, J., Kiayias, A., Leonardos, N.** The Bitcoin Backbone Protocol: Analysis and Applications. Univeristy of Athens, 2014.

39. **Gronwald, M**. The Economics of Bitcoins- Market Characteristics and Price Jumps. – Center for Economic Studies & Ifo Institute, Working Paper No. 5121, 2014.

40. **Houy, N.** The Bitcoin Mining Game. -GATE Groupe d'Analyse et de Théorie Économique Lyon-St Étienne, Working Paper No. 1412, 2014.

41. Intel Core 2 Quad Q9650 Data. Intel. [http://ark.intel.com/products/35428/Intel-Core2-Quad-Processor-Q9650-12M-Cache-3_00-GHz-1333-MHz-FSB]. 01.04.2015.

42. **Kaminsky, D**. Let's Cut Through The Bitcoin Hype: A Hacker-Enterpreneur's Take. – Wired Magazine, 05 March 2013. [http://www.wired.com/2013/05/lets-cut-through-the-bitcoin-hype/] 25.03.2015

43. **Karlstrom, H**. Do Liberitarians Dream of Electric Coins? The Embededness of Bitcoin. – Distinktion: Scandinavian Journal of Social Theori, Vol. 15, Issue 1, 2014, pp. 23-36.

44. **Kondor, D., Posfai, M., Csabai, I., Vattay, G**. Do the Rich Get Richer? An Empirical Analysis of the Bitcoin Transaction Network. - PLoS ONE 9(2): e86197. doi:10.1371/journal.pone.0086197, 2014, 10 p.

45. **Kristoufek, L.** Bitcoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. Scientific Reports, 2013.

46. **Kroll, J., Davey, I., Felten, E**. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. – Princeton University, 2013, 21 p. [https://www.cs.princeton.edu/~kroll/papers/weis13_bitcoin.pdf] 26.04.2015.

47. **McCormick, J**. BTC Guild Bitcoin Mining Pool Review. 2014. [http://bitcoinsinireland.com/btc-guild-bitcoin-mining-pool-review/] 10.02.2015.

48. **Meiklejohn S., Pomarole M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G., and Savage, S.** A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. - University of California, San Diego George Mason University, 2013, 13 p. [http://conferences.sigcomm.org/imc/2013/ papers/imc182-meiklejohnA.pdf] 24.04.2015.

49. **Miers, I., Garman, C., Green, M., and Rubin, D**. Zerocoin: Anonymous Distributed E-Cash from Bitcoin.- Security and Privacy (SP), 2013 IEEE Symposium, 2013, pp. 397–411 [http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6547123] 26.04.2015.

50. **Miller, A.,** Anonymous Byzantine Consensus from Moderately-Hard puzzles: A Model for Bitcoin. – University of Central Florida, 2014.

51. **Nakamoto, S**. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008, 9 p. [https://bitcoin.org/bitcoin.pdf] 22.02.2015.

52. Namecoin definition. Namecoin. [http://namecoin.info/].10.02.2015.

53. Neighborhood Pool Watch. [http://organofcorti.blogspot.com/2013/05/131-bitminter-and-luck.html] 02.03.2015.

54. **Raiborn, C., Sivitanides, M**. Accounting Issues Related to Bitcoins. – Journal of Corporate Accounting & Finance, Volume 26, Issue 2, 2015, pp.25-34.

55. **Rosenfeld, M**. Analysis of Bitcoin Pooled Mining Reward Systems. 17 November 2011, 50 p. [https://bitcoil.co.il/pool_analysis.pdf] 10.02.2015.

56. Rise of Difficulty. Blockchain. [https://blockchain.info/charts/difficulty]. 01.04.2015.

57. **Ryder, G**. All About Bitcoin Mining: Road To Riches Or Fool's Gold? - Toms Hardware, 09 June 2013. [http://www.tomshardware.com/reviews/bitcoin-mining-make-money,3514-5.html] 10.02.2015.

58. Siciliano, L. Bring on Bitcoin: why Richard Branson and Bill Gates support the currency. – The Telegraph, 8. October 2014. [http://www.telegraph.co.uk/finance/currency/11148160/Bring-on-Bitcoin-why-Richard-Branson-and-Bill-Gates-support-the-currency.html]. 25.03.2015.

59. **Stevenson, J.** Getting Started with Litecoin (after Bitcoin). eBook, 2013, 81 p.

60. **Taylor, M**. Bitcoin and The Age of Bespoke Silicon. University of California, San Diego, 2013. 10 p. [http://cseweb.ucsd.edu/~mbtaylor/papers/bitcoin_taylor_cases_2013.pdf] 22.02.2015.

61. Total Bitcoins in Circulation. Blockchain. [https://blockchain.info/charts/total-bitcoins]. 25.03.2015.

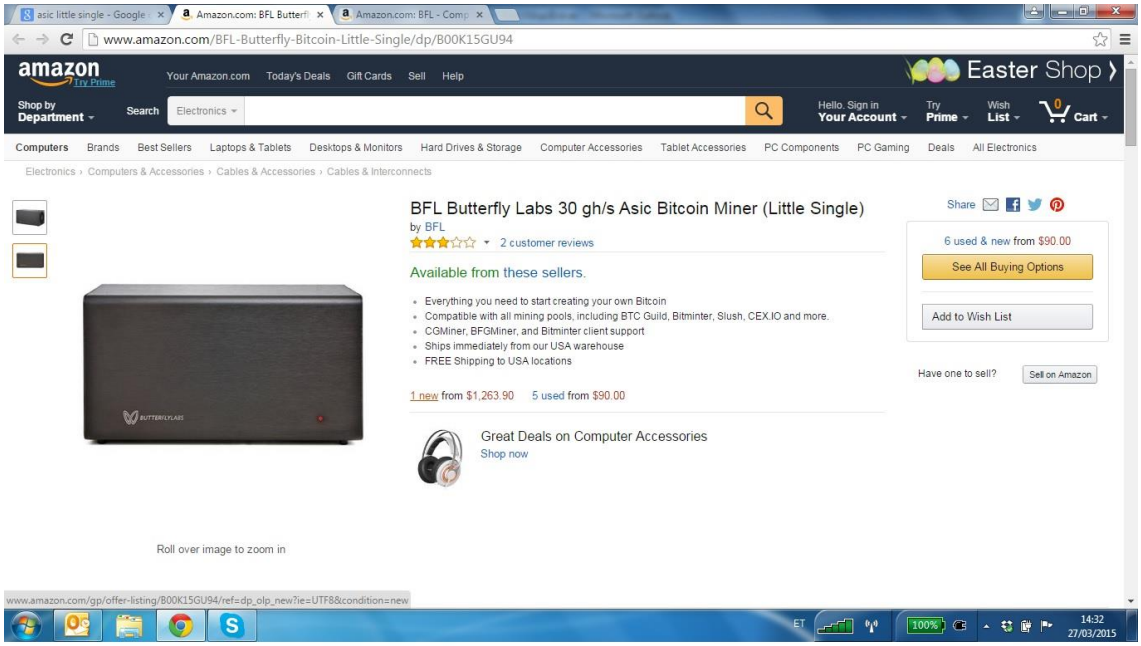
62. **Wang, C., Lo, S.** Bitcoin as Money? – Current Policy Perspectives, No. 14-4, 2014.

63. **Worstall, T**. Fascinating Number: Bitcoin Mining Uses $15 Million's Worth Of Electricity Every Day. - Forbes Magazine. 12 March 2013. [http://www.forbes.com/sites/timworstall/2013/12/03/fascinating-number-bitcoin-mining-uses-15-millions-worth-of-electricity-every-day/] 29.03.2015.

64. 50 Bitcoin Experts Reveal (Guess) What Bitcoin Will Be Trading At Within The Next 12 Months. Founders Grid. [http://foundersgrid.com/bitcoin-price] 12.05.2015

APPENDIXES

Appendix 1. A screenshot with the price of the mining hardware used in the simulation analysis



RESÜMEE

BITCOINIDE KAEVANDAMISE KASUMLIKKUS:
KAS ON KASUMLIK ALUSTADA BITCOINIDE KAEVANDAMIST?
PIKAAJALINE SIMULATSIOONIANALÜÜS BITCOINIDE KAEVANDAMISE KASUMLIKKUSEST ÜKSIKU KAEVANDAJA JAOKS.

Kärt Viilup

Bitcoin on maailma esimene krüptoraha, mis tegutseb täielikult ilma kolmanda osapoole vahenduseta. Bitcoini süsteem loodi 2008 aastal Satoshi Nakamoto poolt selleks, et inimestel oleks turvaline platvorm raha ülekandmise jaoks ilma tasumata suuri pankade vahendustasusid valuuta konverteerimiseks. Bitcoini süsteem toimib täielikult tänu Bitcoini võrgustikule, kus kõik liikmed on võrdsed. Selleks, et antud võrgustik saaks toimida ilma kolmanda osapoole abita, mängib Bitcoini võrgustikus olulist rolli nö. kaevandus. Bitcoinide kaevandamine hõlmab enda all bitcoinide transaktsioonide vahendamist ning kinnitamist. Lisaks sellele toodaks kaevandamisega turule ka uusi bitcoine, kuna süsteem on üles ehitatud selliselt, et kogu raha ei ole mitte koheselt turul, vaid seda kaevandatakse pidevalt juurde, kuni saab täis 21 miljoni bitcoini piir. Kaevandamise eest omistab süsteem automaatselt preemiaks kindla summa bitcoine koos vahendustasudega.

Bitcoinide teema on aktuaalne eelkõige seetõttu, et sellega on seotud äärmiselt suur hulk inimesi kas siis läbi kaevandamise, võrgustikku investeerimise või lihtsalt kasutamise kaudu. 2015 aasta algul oli kõigi ringluses olevate bitcoinide turuväärtus üle 3.3 miljardi dollari, mis teeb antud teema ja selle tuleviku relevantseks väga paljudele ning kuna just bitcoinide kaevandus on see, mis tagab süsteemi elujõulisuse tuleb veenduda, et inimestel on piisavalt suur motivatsioon kaevandamisega tegeleda.

Kaevandamisega saab tegeleda igaüks, kellel on selleks vajalik riistvara. Kui varasemalt oli võimalik bitcoine edukalt kaevandada ka tavalise arvutiga, siis mitmete põhjuste koosmõjul on nüüdseks kaevandamine võimalik vaid selleks spetsiaalselt loodud riistvara abil. Kuigi endiselt on võimalik kaevandada ka vaid tavalise arvutiga nagu seda tehti Bitcoini algusajal, siis enam ei tasu see ära, kuna seadme võimsus on liiga väike, et bitcoine edukalt kaevandada.

Kuna bitcoini turuväärtus on pidevas languses ning kaevandamine on muutunud märksa raskemaks, on muutunud küsitavaks kaevandamise äratasumine isegi võimsama riistvaraga. Kui aga kaob ära võimalus teenida kaevandamisega piisavalt suur preemia, et ära tasuda nii elektrikulu, mida riistvara tarbib kui ka riistvara soetamise maksumus, kaob inimestel huvi kaevandamise vastu. See omakorda aga seab küsimärgi alla terve Bitcoini võrgustiku toimimise, sest ilma kaevanduseta ei valideeri keegi transaktsioone ning ei too uusi bitcoine turule. Antud magistritöö analüüsis, kas uue kaevandaja jaoks on turg piisavalt atraktiivne ning on võimalus sealt kasumit teenida Selleks, et saada vastus püstitatud küsimusele, analüüsis antud töö viite olulist aspekti bitcoinide kaevandamise juures- viisi, kuidas uus kaevandaja peaks turule sisenema, millist riistvara kasutama, milliseid kulusid kaevandustegevuse juures eeldama, analüüsima kui kaua kuluks aega esialgse investeeringu ehk siis riistvara ostmisest tuleneva summa tasumiseks ning analüüsima bitcoinide kaevandamise tulevikku.

Turule sisenemiseks on uuel kaevandajal kaks võimalust- kas kaevandada üksi või liituda kaevandamise jaoks loodud koguga, mille puhul panevad mitmed kaevandajad oma riistvara võimsuse kokku, et koos bitcoine kaevandada ning siis preemia omavahel ära jagada. Mitmed analüüsid on välja toonud, et üksinda kaevandamine ei tasu end enam ära, kuna kaevandamise raskusaste on tõusud liiga kõrgeks, seetõttu oleks keskmisele alustavale kaevandajale kõige õigem liituda kaevandajate koguga. Antud töö kasutab oma analüüsides BTC Guildi kogu statistikat, kuna tegu on ühe kõige hinnatuma kaevandajate koguga.

Kulud, mida kaevandaja kandma peab on nii elektrikulu, mis seadmele kulub kui ka riistvara soetusmaksumus, mis antud töö puhul on $1263.9 koos saatmiskuludega. Selleks, et kaevandaja saaks öelda, et ta teenib kaevandamisega kasumit peab ta olema

suuteline tasuma teenitud preemiatega ära ka riistvara soetusmaksumuse ning seetõttu on kasumlikkuse hindamine pigem pikaajaline tegevus.

Simulatsioonianalüüsi tulemusena selgus, et tänu tõusvale kaevandamise raskustasemele muutub kaevandamine 2016 aasta esimeses pooles kahjumlikuks tegevuseks, kuna elektrikulu mida seade tarbib ületab preemia, mida kaevandaja oma tegevuse eest oodata võib. Analüüsis kasutatavate andmete põhjal, mis pärinevad märtsist 2015 võib öelda, et kaevandaja teenib läbi kaevandamise päevas käivet $0.621, kulutades seejuures elektrile päevas $0.377 seega arvestamata riistvara soetusmaksumust oleks kaevandaja märtsis 2015 teeninud päevas kasumit keskmiselt $0.244 päevas.

Bitcoini süsteem on üles ehitatud selliselt, et iga 10 minuti tagant leiaks üks kaevandajatest uue bloki bitcoine. Juhul, kui antud blokk leiti varem kui 10 minutiga, muutub süsteemi raskustase veendumaks, et uus blokk leitakse just 10 minutiga. Kuigi raskustase võib ka väheneda, näitab trend, et see pigem suureneb. Sellest tulenevalt peab pikaajalises analüüsis võtma arvesse ka raskustaseme muutust, mis 2015 aasta andmete põhjal on 2.96% iga kahe nädala tagant. Sellest tulenevalt võib öelda, et 2016 aasta alguseks jõuab süsteem antud näitajatega olukorda, kus saadud preemia on väiksem elektrile kulunud rahast ning seega ei tasu kaevandamine end enam ära. Analüüsi tulemusel on selleks ajaks kaevandaja, kes kasutab ASIC Little Single riistvara, suutnud teenida $44.25, mis katab ära vaid 3.5% investeeringust mis tuleb teha, et antud riistvara soetada.

Antud töö simulatsioonianalüüsi tulemusena saab öelda, et bitcoinide kaevandamine pole atraktiivne uute kaevandajate jaoks ning tõenäoliselt juba 2016 aastal saabub punkt, kus kaevandamine pole enam kasulik ka nende kaevandajate jaoks, kes kauem kaevandusega tegelenud ning juba varasemalt teeninud tagasi riistvara soetamiseks tehtud kulu. Kuna kaevandamine on Bitcoini süsteemi jaoks äärmiselt oluline tegevus, tuleb tõenäoliselt mingil hetkel seda restruktureerida veendumaks, et süsteem välja ei sure.

Soovitusi kuidas süsteemi restruktureerida on mitmeid, kuid Bitcoini võrgustik pole hetkel ühelegi rekonstrueerimisplaanile reageerinud, kuna kaevandamine teatud

olukordades on endiselt kasumlik tegevus näiteks juhul, kui elektrikulud puuduvad ja kasutatakse taastuvenergiat. Selleks, et tõuseks tõsisem diskussioon Bitcoini tuleviku üle, tuleb tõenäoliselt ära oodata aeg, millal bitcoinide kaevandamine ei ole enam enamuse jaoks kasumlik, sest alles siis hakkab see teema huvi pakkuma piisavale hulgale inimestest, et sellest tulenevalt ka midagi muuta.

Tulenevalt sellest, et Bitcoin on uus fenomen, mille volatiilsus on äärmiselt kõrge ning puudub üleüldine trend nii hinnas kui kaevandamisraskuses on alati võimalik, et bitcoini turuhind tõuseb piisavalt palju, või et kaevandamise raskustase langeb piisavalt et kaevandamine tasuks ära ka ilma struktuuri muutmata. Kuna Bitcoini tuleviku prognoosimine on äärmiselt keerukas tegevus millega siiamaani pole eksperdid väga hästi hakkama saanud, ei osata ka antud hetkel ennustada, kas on tulevikus vaja süsteemi restruktureerida või muutuvad vajalikud parameetrid ise piisavalt, et kaevandamine uuesti kasumlikuks muuta, nii turul juba tegutsevatele kaevandajatele kui uutele kaevandajatele, kes kaaluvad turule sisenemist.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, _____Kärt Viilup_____,
(*autori nimi*)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
PROFITABILITY FROM MINING BITCOINS: SHOULD YOU STILL ENTER THE BITCOIN MINING VOMPETITION? LONG-TERM SIMULATION ANALYSIS OF THE PROFITABILITY FOR A SINGLE MINER
,
(*lõputöö pealkiri*)

mille juhendaja on _____Sven Kristjan Bormann, Raul Eamets, PhD_____,
(*juhendaja nimi*)

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **19.05.2015**