Title: **Bitcoin Mining 101**

Author: **Eduardo Santos**

Date: **11/06/2021**

Contents

1. Introductory Note

This assignment focus on Bitcoin mining, and will answer the following questions:

- What is Bitcoin mining?
- How does Bitcoin Mining work?
- Is mining Bitcoins worth it?
- What do I need to mine bitcoins?

2. Summary / Abstract

This assignment's objective is not to explain what Bitcoin or other cryptocurrencies are, as it assumes that that is already known.

Instead, it is related to Bitcoin mining, trying to explain it in the simplest possible way, so that anyone can understand how it works and, if wanted, can start to mine Bitcoins right away.

3. Framework

Bitcoin's evolution is something that we cannot ignore, since it has been extremely spoked about since April of 2011, time on which its value exploded, with a gain of 3200% within three short months.

Since the explosion of Bitcoin and other cryptocurrencies, there is one question that has undoubtedly been on most of investor's mind, as well as any person that is curious about this subject, and that question is: "How can I mine Bitcoin and is it worth it?"

This question is the main premise for this assignment.

4. Bitcoin Mining

4.1. What is Bitcoin Mining?

Bitcoin mining is the process of updating the ledger of Bitcoin transactions known as the Blockchain. This process is usually performed by computers with a lot of processing power, such that they are able to calculate in a way that we humans could not, at least by hand.

The expression ”Bitcoin mining” derives from an analogy relating to how people physically mine materials in the real world. We can think of it like this, mining is the process of extracting finite resources from our planet, this is much like Bitcoin mining, which put simply is the process of extracting finite Bitcoins through the Bitcoin network. So how does that work?

4.2. How does Bitcoin Mining work?

By definition, Bitcoin mining is the process of generating new Bitcoin by solving algorithmic puzzles. The people who solve these puzzles on the Bitcoin network are referred to as Miners.

These miners highly advanced computers that are able to run complex mathematical algorithms, ultimately this algorithms are really just a long series of numeric values that, when ordered correctly, result in the puzzle being solved, this puzzle is nothing more nothing less than a 64-digit number (hash).

When a miner solves a puzzle, they are rewarded in Bitcoin. The amount of Bitcoin a miner receiver upon completion of a puzzle is referred to as the *Bitcoin reward per block*, because, whenever a puzzle is solved, it adds a new block onto the Bitcoin blockchain, which in turn affects the whole network.

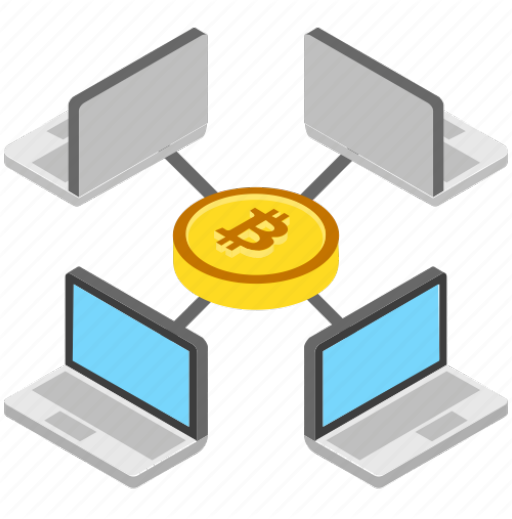

Figure 1: Bitcoin Mining

4.3. The Mining Model

Considering a miner that has the following fraction of the total mining hashrate:

$$0 < p \leq 1$$

That miner's earnings come from the block rewards of his validated blocks. On average, the number of blocks per unit of time that he is able to mine successfully is proportional to his hashrate - p;

The time the miner takes on average to successfully mine a block - t_0 - is given by the formula:

$$t_0 = \frac{\tau_0}{p}$$

Where τ_0 is the time the network takes on average to validate a block (10 min).

Now, lets consider the following variable:

$$T - \text{time between blocks mined by the miner}$$

Given the properties of the hash function, we can conclude that mining is a Markov process - memoryless. This makes easy to show from this property that T follows an exponential distribution:

$$f_\tau(t) = \alpha e^{-\alpha t}$$

Where

$$\alpha = \frac{1}{t_0} = \frac{1}{E[T]}$$

Considering that:

$$t = 0 - \text{instant on which the miner starts mining}$$

$$T_1 - \text{time needed to mine the first block}$$

$$T_2, ..., T_n - \text{inter-block mining times}$$

Then Markov property tells that $T_1, T_2, ..., T_n$ are independent and are all identically distributed following the same exponential law. This means that the time needed to discover n blocks is given by:

$$S_n = T_1 + T_2 + ... + T_n$$

Were S_n follows the e n-convolution of the exponential distribution, giving a Gamma distribution with parameters (n, α):

$$f_{S_n}(t) = \frac{\alpha^n}{(n-1)!} t^{n-1} e^{-\alpha t}$$

With cumulative distribution:

$$F_{S_n}(t) = \int_0^t f_{S_n}(u)du = \sum_{k=0}^{n-1} \frac{(\alpha t)^k}{k!}$$

Finally, we can conclude that, if $N(t)$ is the process counting the number of blocks validated at time $t > 0$ and $N(t) = maxn \geq 0; S_n < t$, then we have:

$$P[N(t) = n] = F_{S_n}(t) - F_{S_{n+1}}(t) = \frac{(\alpha t)^n}{n!} e^{-\alpha t}$$

With $N(t)$ following a Poisson law with mean value αt. This proves that mathematics of Bitcoin mining with validation based on proof of work, are Poisson distributions.

4.4. The impact of mining in the Blockchain

The Blockchain refers to the decentralized ledger that records all Bitcoin related transactions worldwide, whenever a transaction is made, or new Bitcoin is added to the network, the ledger is updated and a new block is added to the chain. This means that each block related to an update in the ledger, either due to a transaction, or the addition of new Bitcoin.

Therefore, when a puzzle is solved and a Bitcoin has been generated, the ledger is updated, this results in a new block being added to the chain, hence the name *reward per block*. Not only does mining allows the miner to produce and earn Bitcoins, it is also an essential activity that allows the ledger of transactions upon which Bitcoin is based to be maintained.

Now that we understand how people mine and how does this influences the Blockchain, how much are miners rewarded when they solve a puzzle?

The reward per block was 50 Bitcoin, back in 2008, however, the rewards is halved every 210 000 blocks that are solved. Blocks are solved at an average of one block every 10 minutes, this means that the reward per block halves around every 4 years. The most recent halving occurred in July of 2020, meaning that the current reward per block is 6.25 Bitcoin.

All recent reports state that there is roughly 18 million Bitcoin currently in circulation, However, we can cross-reference this figure by following this calculation:

$$(50x210000) + (25x210000) + (12.5x210000) + (6.25x210000) = 18375000$$

By calculating this number, we are able to confirm that there are at least 18 375 000 Bitcoin in circulation as of July 2020.

So how does the formula of halving the Bitcoin reward after each 210 000 puzzles solved, effect the long-term generation of Bitcoin? When Bitcoin was created, there were many stipulations enforced by specific coding, one of this rules is that the total number of Bitcoin must be limited and therefore have a finite supply. The cap was set so that, when the final puzzle is solved, there would only ever be a cumulative amount of 21 million Bitcoins. By following the same logic that we applied how much Bitcoin is currently in circulation, we can also estimate when the last Bitcoin will be mined.

The main factor to consider is that the reward is halved once in every 4 year increment, so the final mining date can be determined as follows: In 2008, the initial reward was 50 Bitcoin per block. So, to find out

when Bitcoin will be depleted, we just need to keep on halving 50 until we reach 0, meaning that there is no reward per block because there is no Bitcoin left to be mined. 50 can be halved 33 times before it reaches 0, and there have been 3 halvings already. This means that there are 30 halvings remaining before Bitcoin has been depleted.

As a halving occurs every 4 years, we can multiply 30 by 4 to find out how long it will be until the final Bitcoin will be mined. The answer to this is 120 years, meaning that the final Bitcoin will be mined inn 2140.

But, if there is already 18 million out of 21 million Bitcoin in circulation, within 12 years of the first Bitcoin being mined, why will it take 120 years to mine the last 3 million?

This is due to the reward per block halving 4 years, the rate at which new Bitcoin is generated drastically decreases. When the final division takes effect, miners will only be rewarded 0.00000001 Bitcoin per block, this means that when the last puzzle is solved, and the final Bitcoin is mined in 2140, no more Bitcoin can ever be generated.

Linking back to the metaphor we used before, this is equivalent to all the mines on this planet being drained and, consequently, the planet Earth being depleted of the limited finite resources that it once had.

So, if this is the case, why isn't everyone mining now, in order to get Bitcoin while reward per block is still considerably high? We will talk about that on the next section.

4.5. Is Bitcoin mining worth it?

When Bitcoin was created, a very specific set of rules were implemented to allow for sustained mining. These rules abide by the following characteristic: The more mining power the network has, the harder it is to solve the puzzles that the system generates.

There is a positive correlation between mining power and the system's mining difficulty. In other words, the more miners there are on the system trying to solve the puzzle, the harder it will be for them to do so. This means that the algorithmic puzzles are a self-adjusting mechanism.

The rule of the adjustment works in parallel, so if there are less miners working on the puzzle, it will be easier to solve. In essence, this creates an equilibrium between the mining power and mining difficulty.

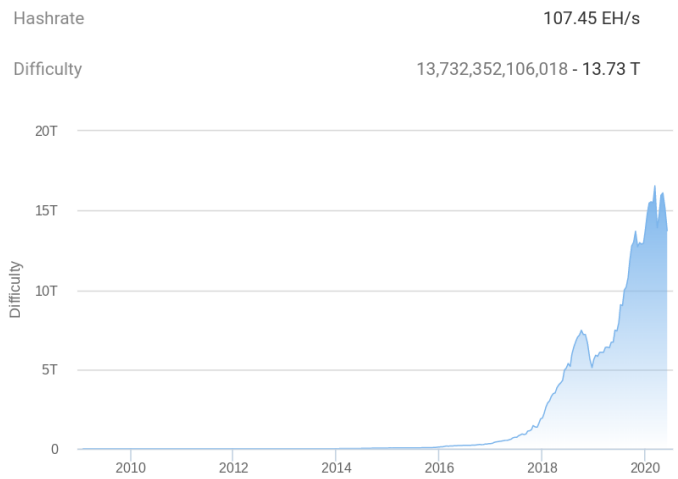

Figure 2: Bitcoin Mining Difficulty Graph

As the years have passed, Bitcoin has evolved from an emerging to an established market. Consequently, the mining capability has excelled exponentially due to the saturation of miners looking to solve puzzles and earn Bitcoin. This means that, over time, more miners have begun utilizing the most powerful and advanced technology, creating very high barriers to entry for new miners.

So, how do these rules allow for sustained mining?

These rules dictate the rate at which puzzles can be solved, it is because of these rules that a puzzle is solved, on average, every 10 minutes, and, therefore, allows the reward per block to consistently halve every 4 years. This means that, before the first halving even took place, it was already dictated how often new Bitcoin would be added to the system.

Because there is only a finite amount of Bitcoin to be mined, the implementation of these rules regulates the rate at which new Bitcoin is generated, allowing the process to be sustained for a predetermined period of time. Due to the restricted time in which new Bitcoin is distributed, the supply is limited for a prolonged duration, and, therefore, results in Bitcoin being less subject to inflationary pressure from centralized banks and governments.

But why is Bitcoin less subject to inflation then money from centralized institutions?

As we've seen previously, Bitcoin is finite, whereas money is unlimited in quantity, because it is reproducible. Governments and banks can print more money whenever they want, and this is a significant cause of inflation. When more money is printed, the value of the currency itself decreases, when a currency decreases in value, and inflation has taken effect, people often only talk about prices rising, however, the reality of this is that, due to an increase in the supply of money, its value has fallen, causing a decline in purchasing power, meaning that we are able to buy less with the same amount that we could before. In summary, we need more money to buy something that costs less in the past.

To mine Bitcoins, there are a lot of factors we depend on:

- Hashrate
- Bitcoin reward
- Mining difficulty
- Electricity cost
- Power consumption
- Pool fees
- Bitcoin's price
- Difficulty increase per year

4.5.1. Hashrate

In bitcoin's case, a Hash is the puzzle we previously mentioned that a miner has to solve. The Hashrate is a miner's hardware performance, and it means the number of guesses to the right solution a miner can make per second.

The Hashrate is usually measured in:

- **MH/s** - Mega Hash per second (Mega = 10^6)
- **GH/s** - Giga Hash per second (Giga = 10^9)
- **TH/s** - Thera Hash per second (Thera = 10^{12})
- **PH/s** - Peta Hash per second (Peta = 10^{15})

4.5.2. Bitcoin reward

This represents the number of Bitcoins generated when a miner finds a solution to a puzzle. As mentioned before, the current reward per block is 6.25 Bitcoin.

4.5.3. Mining difficulty

The mining difficulty is measured by a number that represents how hard is to mine Bitcoins at a specific time. This number takes into consideration the amount of mining power at that specific time.

4.5.4. Electricity cost

To calculate if mining Bitcoins is profitable, we need to our electricity cost, this value comes in our monthly electricity bills, and can be quite high due to the electricity needed to power the miner, as well as to cool it, because of the high temperatures it can reach.

4.5.5. Power consumption

The power consumption can vary from miner to miner, that's why we need to find the power consumption for our specific miner, in order to calculate his profitability.

Power consumption is usually measured in W^1s.

[1] Watt

4.5.6. Pool fees

We can think of mining as a competitive game, this game happens between all the current miners on the network.

Even if we have a good and expensive mining system, we are in disadvantage against profession mining farms. To mitigate this disadvantage, we have something called mining pools.

Mining pools, as the name suggests, are groups of miners that work together and combine their mining power in order to compete more equitably. If the pool is the fastest to solve the puzzle, the earning are spread between the pool members, depending on how much each one of the miners contributed.

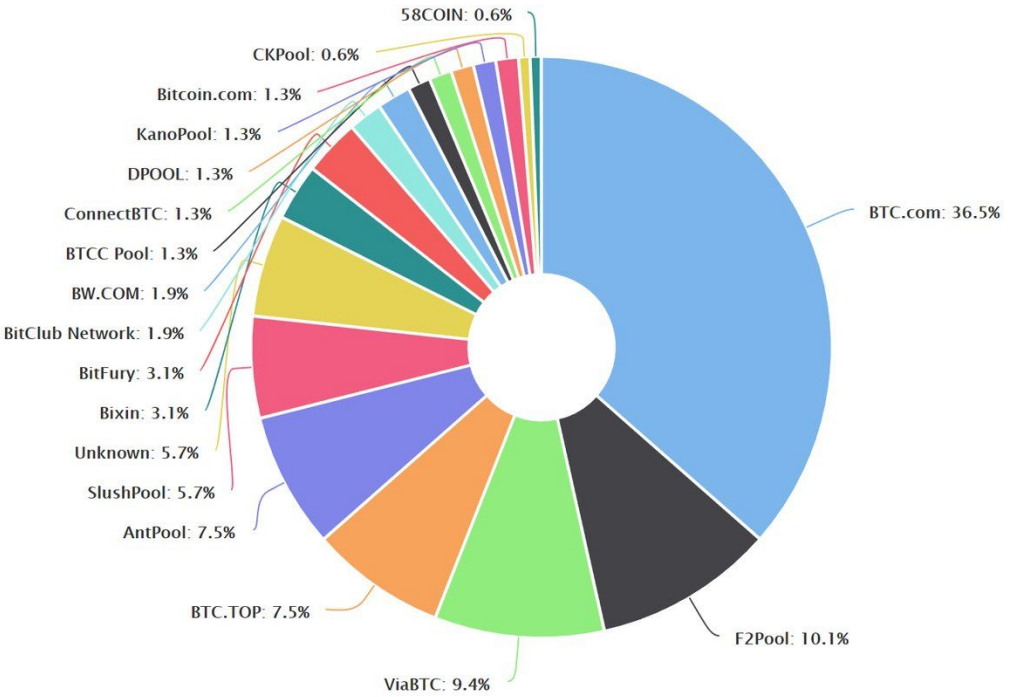

Figure 3: Largest Bitcoin Mining Pools

4.5.7. Bitcoin's price

Because of the volatility of Bitcoin's price, it is almost impossible to know wether it will be profitable. And this uncertainty has a significant impact on profitability.

Figure 4: Bitcoin's Price Over The Last Year

4.5.8. Difficulty increase per year

The rate of miners joining the network, as well as the difficulty to mine in the future, it's quite unpredictable. This is why it is very difficult to say if mining Bitcoin is profitable.

Despite that, and having the value of the previous topics' variables, we are able to calculate how many Bitcoins we can earn a month, using an online Bitcoin mining calculator.

4.6. What do I need to mine bitcoins?

4.6.1. Bitcoin Mining Software

There are 4 types of Bitcoin mining software:

- CPU mining
- GPU mining
- FPGA mining
- ASIC mining

4.6.1.1 CPU mining

CPU[2]s are made to be suitable for rapid switching from task to task. However, CPUs are not very well prepared for repetitive and long mathematical calculations. They can do math, as inside every CPU is one or more ALU[3]s. However, GPU[4]s have much more ALUs than CPUs and because of that, they can do large amounts of mathematical work in a greater quantity, if we compare both.

CPU mining was initially allowed in Bitcoin client's initial versions but the hashrate of the network grew too much for CPU mining to be considered profitable. The option was therefore removed from the core Bitcoin client's user interface.

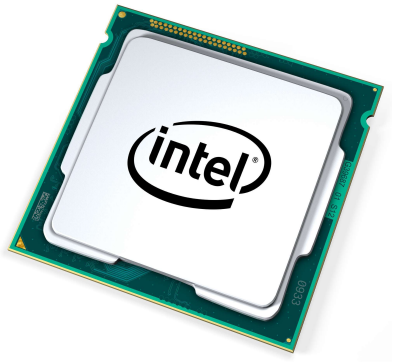

Figure 5: CPU Example

4.6.1.2 GPU mining

GPU is a part of the video rendering system of a computer. It assists with the rendering of 3D graphics and visual effects so that the CPU doesn't have to.

GPU Mining is faster and more efficient than CPU mining.

A GPU is like a CPU, but there are important internal differences that make them suited toward their special tasks. Making GPUs best suited for Bitcoin mining.

Figure 6: GPU Example

[2]Central Processing Unit
[3]Arithmetic/Logic Unit
[4]Graphics Processing Unit

4.6.1.3 FPGA mining

FPGA[5]s is a hardware that can be configured to run a set of calculations. It works like a GPU, but it can be at most 100 times faster. It typically consume very small amounts of power with relatively high hash ratings. Making it more efficient than CPU and GPU mining.

Figure 7: FPGA Example

4.6.1.4 ASIC Mining

ASIC[6]s are pieces of hardware specifically designed for mining Bitcoins, and it can not do anything else.

In the current days, ASIC miners are the standard when it comes to mining.

Figure 8: ASIC Example

[5]Field Programmable Gate Array
[6]Application-Specific Integrated Circuit

4.6.2. Step-By-Step Guide

To mine Bitcoins, there are a few main steps that we should follow:

1. Calculate Profitability
2. Get a Miner
3. Open a Bitcoin Wallet
4. (Opcional) Enter a Mining Pool
5. Install a Mining Software
6. Start Mining

4.6.2.1 Calculate Profitability

Calculate profitability using an online Bitcoin mining calculator to find out if, in our case, mining Bitcoins is worth it. If it is, then we can get to the next step, if not, maybe we should not enter this business.

4.6.2.2 Get a Miner

This step is very important, like all of them. We need to be very careful when choosing a miner, in order to choose something that fits our budget, as well as be the best option we can afford when it comes to the relation price/efficiency.

Here are some of the best Bitcoin miners, in the present days:

- **Bitmain AntMiner S5**
- **Bitmain AntMiner S7**
- **Bitmain AntMiner S9**
- **AntMiner T9**
- **AvalonMiner 741**
- **Bitmain AntMiner L3+**
- **Bitmain AntMiner D3**
- **Dragonmint T1**
- **WhatsMiner M3X**
- **Avalon6**

4.6.2.3 Open a Bitcoin Wallet

In order to store our mined Bitcoins, we will need a Bitcoin Wallet. This is the most secure way too do so.

A list of the best Bitcoin/cryptocurrency wallets and its features can be found here.

4.6.2.4 (Opcional) Enter a Mining Pool

We have already talked about the benefits of entering a mining pool, and this could be an option. But, before deciding to enter one, we first need to see of that is something that we really want and if we can benefit from joining one, and this decision should be taken considering some aspects, like what fees does the pool charge for mining/withdrawal, how frequently does the pool actually wins the competition and solves the puzzle, etc.

4.6.2.5 Install a Mining Software

Without the correct software, our hardware will nor be of much use. Here are the best programs for mining Bitcoin:

- **CGminer**
- **BFGminer**
- **EasyMiner**
- **MultiMiner**

4.6.2.6 Start Mining

After completing the previous steps, connect your miner to your computer, and configure your mining software with your pool's credentials, after all set, you are ready to mine!

4.7. Conclusion

With this assignment, we were able to understand what Bitcoin mining is, as well as all the different factors that make this possible. Now, we have a clearer idea about this subject, making the decision of whether we want to mine Bitcoins or not easier and more thoughtful.

Bitcoin mining isn't for everyone, but it is possible to earn money and to make a profitable business from this.

References

[1] Bitcoin. *Bitcoin*. [Accessed 05/07/2021]. URL: https://bitcoin.org/en/.

[2] 99 BITCOINS. *What is Bitcoin Mining and How Does it Work?* [Accessed 05/07/2021]. URL: https://99bitcoins.com/bitcoin-mining/.

[3] CryptoTrader.Tax. *The 10 Best Bitcoin Mining Hardware Machines 2021*. [Accessed 07/07/2021]. URL: https://cryptotrader.tax/blog/best-bitcoin-mining-hardware.

[4] Ricardo Pérez-Marco Cyril Grunspan. "The mathematics of Bitcoin". In: (2020). DOI: hal-02486029f.

[5] Ethan. *Crypto Mining 101: Calculating Profitability*. [Accessed 05/07/2021]. URL: https://medium.com/london-blockchain-labs/mining-101-calculating-profitability-7df1ff064279.

[6] Forbes. *An Overview Of Mining: CPU, GPU And ASIC*. [Accessed 07/07/2021]. URL: https://www.forbes.com/sites/theyec/2020/07/23/an-overview-of-mining-cpu-gpu-and-asic/.

[7] Guru99. *BEST Crypto Wallets: Top 20 Bitcoin Wallets App for 2021*. [Accessed 07/07/2021]. URL: https://www.guru99.com/best-bitcoin-cryptocurrency-wallets.html.

[8] Software Testing Help. *Top 10 BEST Bitcoin Mining Software [2021 RANKINGS]*. [Accessed 07/07/2021]. URL: https://www.softwaretestinghelp.com/bitcoin-mining-software/.

[9] Investopedia. *Bitcoin Mining*. [Accessed 05/07/2021]. URL: https://www.investopedia.com/terms/b/bitcoin-mining.asp.

[10] Investopedia. *How Does Bitcoin Mining Work?* [Accessed 05/07/2021]. URL: https://www.investopedia.com/tech/how-does-bitcoin-mining-work/#:~:text=Bitcoin%5C%20mining%5C%20is%5C%20the%5C%20process,extremely%5C%20complex%5C%20computational%5C%20math%5C%20problems..

[11] Bitcoin Mining. *How Bitcoin Mining Works*. [Accessed 05/07/2021]. URL: https://www.bitcoinmining.com/.

[12] Bitcoin Wiki. *Mining*. [Accessed 07/07/2021]. URL: https://en.bitcoin.it/wiki/Mining.

[13] Bitcoin Wiki. *Why a GPU mines faster than a CPU*. [Accessed 07/07/2021]. URL: https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU.