May 2019

Analysis of Bitcoin Cryptocurrency and Its Mining Techniques

Suman Ghimire

ANALYSIS OF BITCOIN CRYPTOCURRENCY AND ITS MINING TECHNIQUES

By

Suman Ghimire

Bachelor of Electronics and Communication Engineering
Tribhuvan University, Nepal
2016

A thesis submitted in partial fulfillment
of the requirement for the

Master of Science in Engineering-Electrical Engineering

Department of Electrical and Computer Engineering
Howard R. Hughes College of Engineering
The Graduate College

University of Nevada, Las Vegas
May 2019

UNLV | GRADUATE COLLEGE

Thesis Approval

The Graduate College
The University of Nevada, Las Vegas

April 12, 2019

This thesis prepared by

Suman Ghimire

entitled

Analysis of Bitcoin Cryptocurrency and Its Mining Techniques

is approved in partial fulfillment of the requirements for the degree of

Master of Science in Engineering-Electrical Engineering
Department of Electrical and Computer Engineering

Henry Selvaraj, Ph.D.
Examination Committee Chair

Shahram Latifi, Ph.D.
Examination Committee Member

Mei Yang, Ph.D.
Examination Committee Member

Laxmi Gewali, Ph.D.
Graduate College Faculty Representative

Kathryn Hausbeck Korgan, Ph.D.
Graduate College Dean

ABSTRACT

Bitcoin is a peer-to-peer digital, decentralized cryptocurrency created by an individual under pseudonym Satoshi Nakamoto. In fact, it is the first digital, decentralized currency. Several developers and organizations have explored the importance of digital cryptocurrency and the concept of the blockchain. Bitcoin is assumed to be one of the secure and comfortable payment methods that can be used in the upcoming days. The backbone of Bitcoin mining is the concept of the blockchain, which is assumed to beone of the ingenious invention of this century. The blockchain is the collection of blocks that are linked together in such a way that the hash of the previous block is contained in the present block. Any change of information in any blocks in a blockchain result in an error on the whole blockchain. Bitcoins are generated by a process called mining, where miners solve a complex mathematical puzzle. The miners are competing with each other to mine the Bitcoin as fast as possible and claim the reward.

The mining of Bitcoin requires very high computation power. Since miners are solving the complex mathematical puzzle through hardware, they need to be fast in order to be the first solving the block. The miner who successfully solves the block gets rewarded with Bitcoin. Mining can be done by a single person, or it can be done by pool, where a bunch of miners combines in a network to mine a single block. Single mining, also referred to as solo mining is difficult since the difficulty of Bitcoin mining is increasing every day. Pool mining is another option for those who have fewer resources for mining.

We propose an efficient way of mining Bitcoin by analyzing several results through self-experiment, online exchange market data, real-time Bitcoin block data, different mining pools' efficiency data and much more. Several factors are needed to be taken into consideration during mining because we may never mine a single Bitcoin even if we invest thousands of dollars on mining Bitcoin.

ACKNOWLEDGMENT

I would like to express my sincerest gratitude to my thesis advisor Dr. Henry Selvaraj for his continuous support, invaluable constructive criticism, motivation, encouragement, and guidance throughout my work. I feel fortunate to get the opportunity to work under his supervision.

Besides, my advisor, I would also like to thank my advisory committee members; Dr. Laxmi Gewali, Dr. Mei Yang, and Dr. Shahram Latifi for accepting to be on the committee and providing valuable comments and allocating their precious time in reviewing my work.

I am also grateful to Howard R. Hughes College of Engineering, University of Nevada, Las Vegas for providing me a learning opportunity through Graduate Assistantship.

I am equally grateful to all my family members, my parents Mr. Ramesh Ghimire and Mrs. Gita Ghimire, and my brother Sulav Ghimire. Also, I would like to thank all of my friends who helped me directly and indirectly throughout my thesis work.

SUMAN GHIMIRE

University of Nevada, Las Vegas

May 2019

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

BTC	: Bitcoin
POW	: Proof of Work
ATM	: Automated Teller Machine
USD	: United States Dollar
ASD	:Australian Dollar
INR	: Indian Rupees
NPR	: Nepalese Rupees
ECDSA	: Elliptic Curve Digital Signature Algorithm
SHA-256	: Secure Hash Algorithm-256
CPU	: Central Processing Unit
GPU	: Graphics Processing Unit
FPGA	: Field Programmable Gate Array
ASIC	: Application Specific Integrated Circuit
H/S	: Hash per Second
MH/S	: Mega hashes per second
TH/S	: Tera hashes per second
PH/S	:Peta hashes per second
EH/S	: Exa hashes per second
DDoS	: Distributed Denial of Service

Chapter 1

INTRODUCTION

1.1 Preview

Bitcoin (also known as BTC) is a cryptocurrency created by Satoshi Nakamoto and released in 2009 [1]. Satoshi Nakamoto is not the real name of Bitcoin creator; instead, it is the pseudonym. Bitcoin is a distributed, decentralized, peer-to-peer virtual cryptocurrency. Since Bitcoin is a virtual cryptocurrency, it does not have any shape and size like the currencies we use today and is stored in Bitcoin wallets which are created to store virtual currencies. Bitcoins can be transferred to each other using the Bitcoin address. Since its inception, it has grown both in popularity and its use. There are three different ways to get Bitcoin. One way is to buy them from an exchange, which is the process of converting local currency to Bitcoin. The other way is to get it from Bitcoin ATM that are installed on several places around the world and the other way is to mine them. The main protocol lying behind the Bitcoin is blockchain which is truly an innovative invention of this century. Bitcoin is created by the process called mining [1]. The individual who mines Bitcoin are called miners. The Bitcoin network is operated and secured by miners. Bitcoin can be used as a replacement for physical money in terms of buying and selling goods. It can be purchased, sold and even exchanged for other physical currencies.

Since the introduction of Bitcoin in 2009, it has grabbed attention from numerous sectors mainly targeting business, industry and academic sector. With a market capitalization of $88,604,642,423 USD and more than 300,712 aggregate numbers of confirmed transactions per day (March 2019), Bitcoin is considered to be the most successful cryptocurrency to date.

1.2 Motivation

With the introduction of Bitcoin and the technology that lies within it, there are tremendous opportunities explored by various people in different sectors such as consumers, developers, marketeers, etc. Many organizations have started working on mining Bitcoin which serves as a virtual currency as a replacement of fiat currencies. Several countries including USA, Japan, China, and Australia, started using Bitcoin as one of their payment methods in restaurants and stores [1]. The way of generating new Bitcoins is known as Bitcoin mining. Since there is a limited number of Bitcoins (21 Million), the numbers of Bitcoins left to be mined are getting less day by day. As of now, there are approximately 17.7 Million Bitcoins have been mined, and 3.5 Million Bitcoins are left to be mined. The motivation to know more about Bitcoin and the technical aspect of generating Bitcoin evolves from the ever-increasing interest of people in Bitcoin and its implementation on different sectors.

1.3 Objectives

The main objectives of this research work are listed below:

- To know more about mining options and the ways to reduce longevity in mining time.
- To explore better ways to mine, reducing the cost and improving the performance.
- To know about the existing algorithms behind proof of work, which is a critical factor in mining Bitcoin.
- To study the details of the process in mining and technical difficulties existing in the mining process and come up with a better solution.

1.4 Organization

This report consists of five chapters,

Chapter 1-Introduction: This chapter deals with the introduction of the thesis work, motivation, and the objective of the thesis work.

Chapter 2-Background: This chapter contains a literature review on Bitcoin Cryptocurrency and its mining process. This chapter also deals with different mining techniques used at present.

Chapter 3 Literacy Review: This chapter describes the software use, problem identification, and methodology used in the thesis.

Chapter 4 Analysis and Proposed Solution: This chapter presents the graphs of data collected over several simulation results and the analysis.

Chapter 5 Conclusion and Future Work: This chapter concludes the thesis with collected results, and discusses shortcoming, and future work.

Chapter 2

BACKGROUND

Digital currencies have gained massive popularity these days. Bitcoin is the most popular digital currency having a total market capitalization of USD 71,882,552,340. It is the decentralized, distributed, peer-to-peer virtual currency also known as a cryptocurrency [2]. The creator of Bitcoin is known under the pseudonym, Satoshi Nakamoto. Satoshi Nakamoto's identity remains a mystery to date. Since it is decentralized cryptocurrency, it does not have a centralized control as the bank have. It does not depend on any third party to transfer the amount from user to user. It allows users to transfer money over the internet as easy as sending an email without having any middleman in between.

2.1 Centralized System

As the name implies, centralization is the concentration of control of an activity or organization under a single authority. The currencies that we are using these days are fiat currencies which are transferred among the people under a centralized system. Whenever two parties want to transfer a certain amount of money, then it has to go through a third party which initiates the process and verifies the transaction. If user A, wants to transfer currency to user B, then user A initiates the process, then the third party (in this case, a supposed bank), receives the transaction notification, checks for the authenticity of the transaction and then finally approves it if the data are correct. After approval, the amount is transferred to user B. For this process, the bank takes a lot of time and a certain amount as a transaction fee.

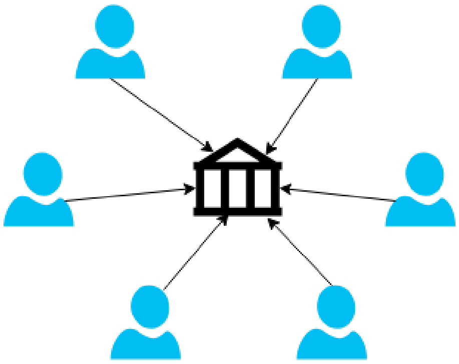


Figure 1: Centralized System.

2.2 Decentralized System

The work that maintains Bitcoin transaction is distributed and shared among each node or “peer” in the network. Moreover, that means data does not have to pass through any central server or hub. Here each user is connected on a Bitcoin network and has a public ledger of every transaction. The users themselves verify the transactions and approve the transaction if the transaction is valid. If all the users on the network having the public ledger of transaction approve on its authenticity, the amount is transferred from user A to user B. This does not require much time and has very minimum transaction fee compared to centralized system.

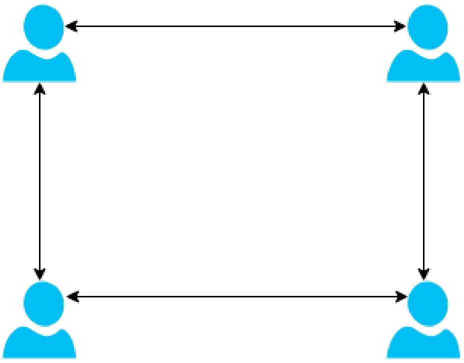
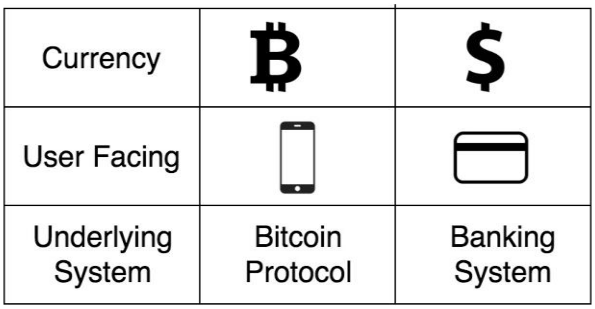


Figure 2: Decentralized System

2.3 Bitcoin System vs. Current System



Currency	₿	$
User Facing	📱	💳
Underlying System	Bitcoin Protocol	Banking System

Figure 3: Bitcoin System Vs. Current System.

Bitcoin system is different from the current system. From the figure 3, we can see how Bitcoin is different from the regular banking system. The current system uses the banking system which is a centralized system. It accepts currency (USD, ASD, NPR, INR, etc.) as a payment method. However, the bitcoin protocol uses the decentralized system and accepts virtual currency (Bitcoin) as a payment method. The protocol that lies behind Bitcoin and other cryptocurrencies is the blockchain [3].

2.4 History of Bitcoin:

- Early 2009: Nakamoto mined the first-ever Bitcoin. The first block that is mined is termed as the "Genesis block." [4]
- October 2009: New Liberty Standard publishes a Bitcoin exchange rate that establishes the value of a Bitcoin at US$1 = 1,309.03 BTC, using an equation that includes the cost of electricity to run a computer that generated Bitcoins. [4]
- May 22, 2010: Laszlo Hanyecz bought pizza in exchange for 10,000 Bitcoins. Today it's worth is $39,304,700 USD. [5]
- February 2011: 1 BTC worth USD 1 [4]
- March 2013: the value of all Bitcoins in circulation hit $1 billion.
- February 2015: The Bitcoin price reached $262. Sets at all-time high.

- December 2017: Bitcoin surpasses all-time highest price USD 18,000 [4]
- As of now, the price has dropped and it is USD 4,050 [6]

The market capital growth chart shown in Figure 4 shows the increase of Bitcoin value per USD. [6]

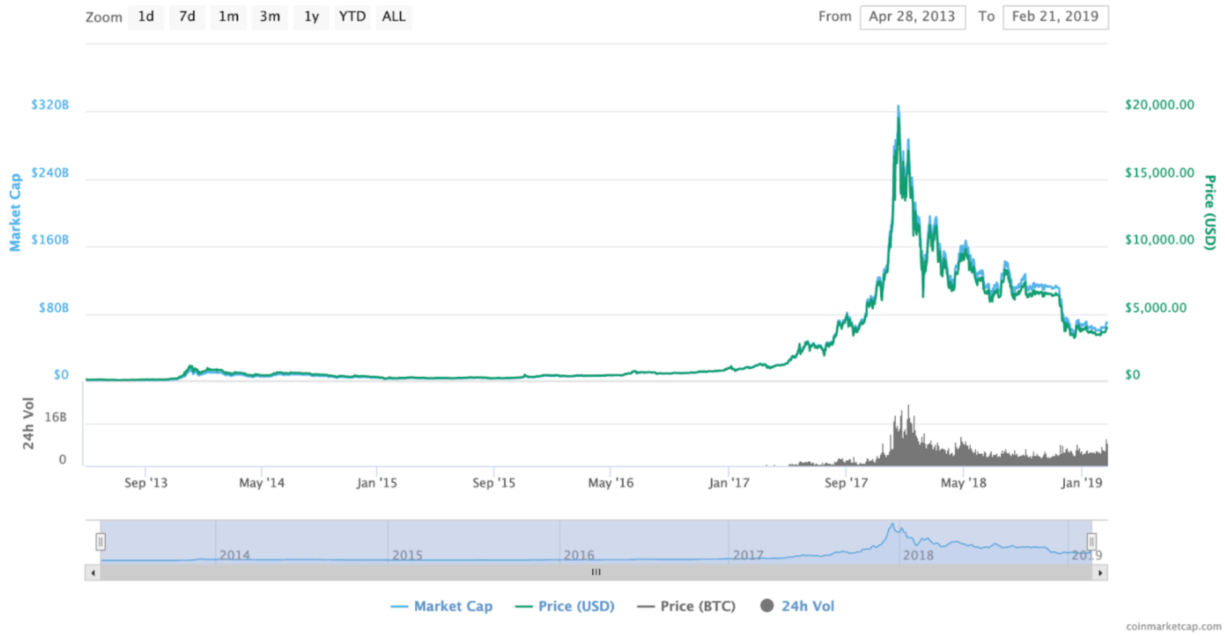


Figure 4: Bitcoin Price History

The market capital growth chart on Figure 4, shows how Bitcoin has undergone rapid success (especially from January 17) to become the most popular cryptocurrency. Initially, the value of Bitcoin was $0.00078 USD per BTC [4]. The price of Bitcoin is highly fluctuating due to its presence in exchange market and supply-demand chain involved over there.

2.5 Transferring Bitcoin

Bitcoin can be transferred from one person to another as easily as sending a message. In order to transfer Bitcoin from one user to another, we need to have Bitcoin address, Bitcoin wallet, and Bitcoin itself. The smallest unit of Bitcoin is called Satoshi. Bitcoin is divisible to the 8th decimal place; hence it can be split into 100,000,000 units.

1 BTC = 100,000,000 Satoshi

2.5.1 Bitcoin Address:

Bitcoin Address is used to transfer Bitcoin from one user to another. Bitcoin address acts as a bank account that we use in the banking system. Provided Bitcoin address, anyone can send and receive Bitcoin from one person to another using internet and laptop/smartphones. A string of 26-35 alphanumeric characters represents the Bitcoin address. There are three different Bitcoin address formats: [7]

Format 1: P2PKH or Legacy address format

In this format, the address starts with the number “1”

Example: 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

Format 2: P2SH address format

In this format, the address starts with the number “3”

Example: 3CfCfnj6bfmCVqfQAqinK7mB1tYJM5Qrnt

Format 3: Bech32 address format

In this format, the address starts with letter “bc1”

Example: bc1qldx8hs6y0m6cxy3ucf9kasvd3vlxky7ypsp233

2.5.2 Bitcoin Wallet:

A Bitcoin wallet is a digital wallet similar to the bank account which is used to store Bitcoin [8]. A software called Bitcoin wallet should be downloaded in order to get a Bitcoin address. The software allows securely sending, receiving, and storing Bitcoin in the Bitcoin network. There are mainly two different types of Bitcoin wallet which are software wallet and hardware wallet.

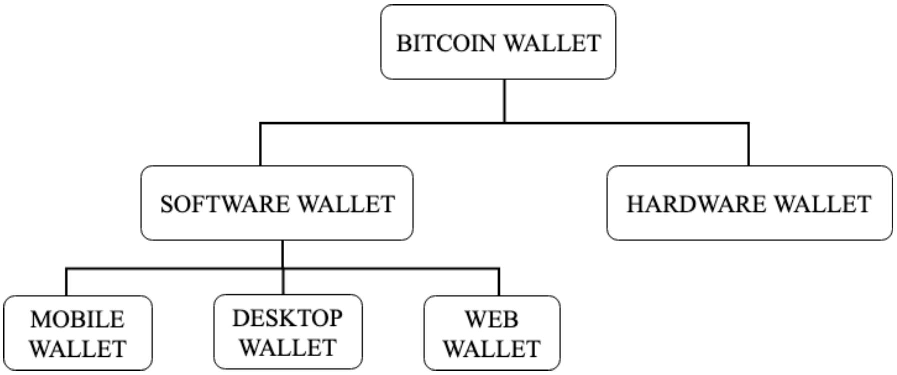


Figure 5: Bitcoin Wallet

Software wallet:

Software wallet is a software program that is installed on our device by using encryption security. Software wallet is further divided into three types: mobile wallet, web wallet and desktop wallet.

The mobile wallets are those wallets that can be downloaded on any smartphones (Android/iOS). Some of the examples of Mobile wallets are Bitcoin Wallet, Circle, Bither, Coin.Space, etc.

The desktop wallet is installed on a desktop computer (Windows/Mac/Linux). It enables the user to create a Bitcoin address for sending and receiving Bitcoins. Some of the examples of the desktop wallet are Bitcoin Core, Armory, etc.

The web wallets are those wallets which can be accessed from any device that has internet and web browser. Some of the examples of web wallet are Coinbase (www.coinbase.com), BitGo (www.Bitgo.com), Blockchain (www.blockchain.com/wallet), BTC (www.wallet.btc.com), etc.

Hardware wallet:

Hardware wallets are similar to external hard drive. Hardware wallets are physical wallets which can be plugged into the computer to store Bitcoin. It is the most secure wallet compared to software wallet since the hardware wallet has very less exposure to the computer and internet making them challenging to hack to breach the data. Some of the examples of hardware wallets are Bitbox, Ledger Nano S, Trezor, etc.

Private and Public Keys:

The Bitcoin Protocol relies on public key cryptography. The Bitcoin owner has two keys, public key, and private key. A rough analogy is username for public key and a password for a private key. Similarly, a hash of a public key is the address of Bitcoin, and there is always a private key associated with that public key. The private keys are used to create the signature and public key to verify it [9]. In the Bitcoin system, if anyone wants to make a transaction then, each owner transfers the Bitcoin to another by digitally signing a hash of previous transaction and the public key of the next owner. It uses ECDSA (Elliptic Curve Digital Signature Algorithm), which relies mainly on mathematics [10].

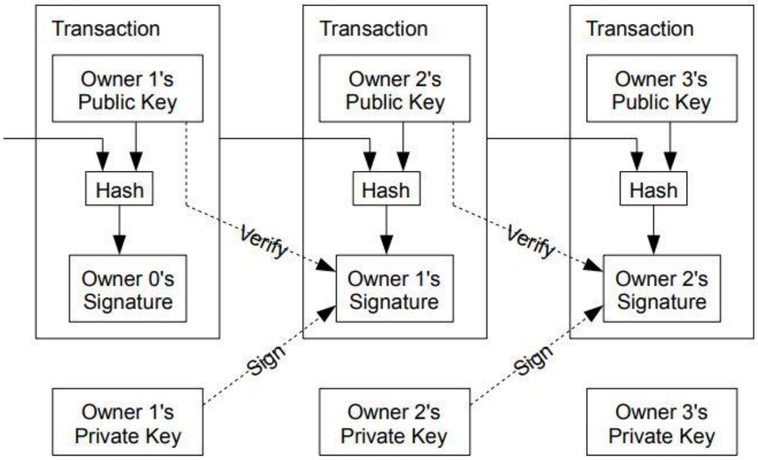


Figure 6: Bitcoin Transaction

Since the Bitcoin is a decentralized peer to peer network, the transaction information is shared among the users on a network. In the case of Bitcoin, the information refers to the transactions that are made during buying or selling Bitcoins.

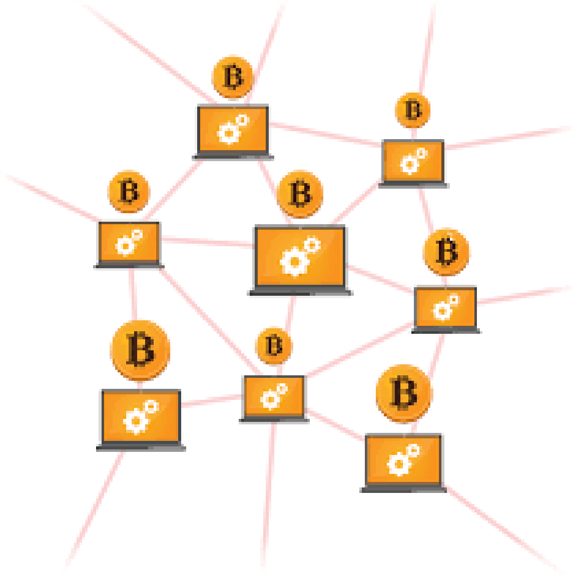


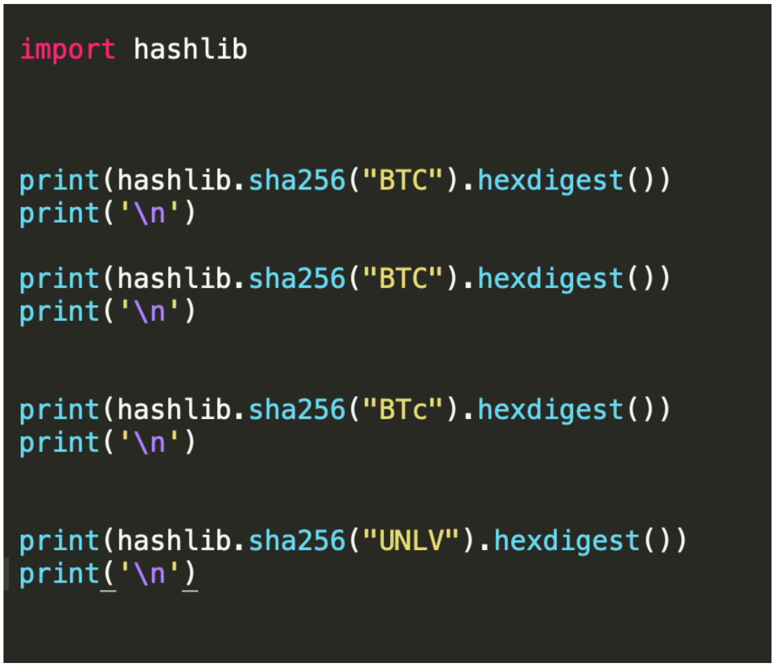
Figure 7: Bitcoin peer-to-peer network

2.6 Hashing

Under the Bitcoin protocol, cryptographic hash functions are used to hash the Bitcoin transactions. Hashing is the process of mapping digital data of any arbitrary size to data of a fixed size [11]. In other words, hash is the digital signature of any data. It is the process of taking some readable information and converting to something that makes no sense at all. There are some requirements that a good hashing algorithm should contain:

- The output of the hashing algorithm is fixed.
- Even the smallest change in the input must provide an entirely different result.
- The same input provides the same output.
- Calculation of input value from the output value (reverse way) should not be possible.
- The calculation of the hash value must be fast.

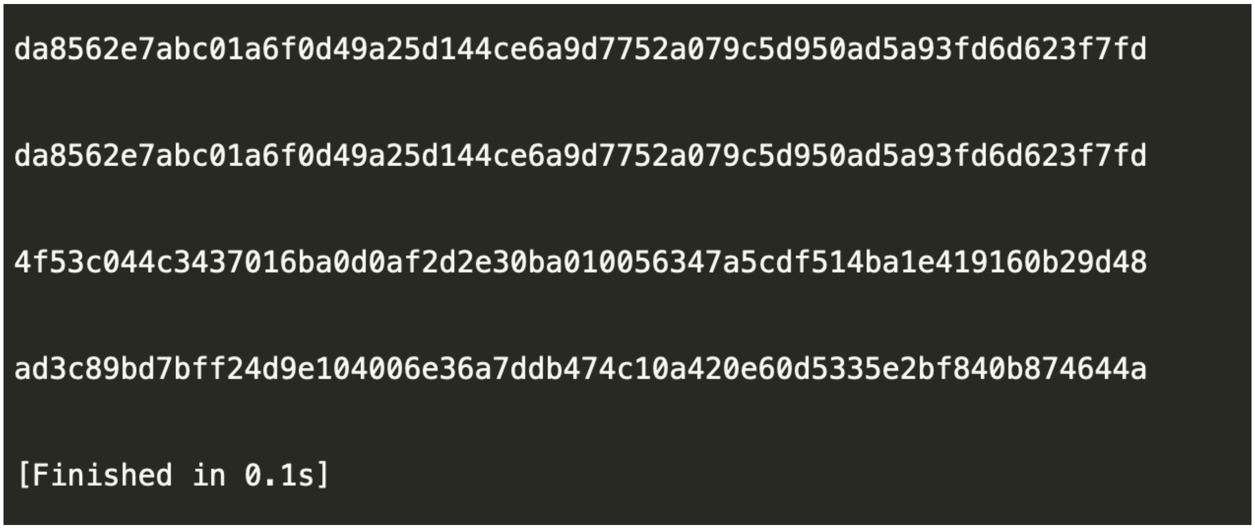
The example of hashing is shown in the Figure 8 using the Python programming language.



```
import hashlib


print(hashlib.sha256("BTC").hexdigest())
print('\n')

print(hashlib.sha256("BTC").hexdigest())
print('\n')


print(hashlib.sha256("BTc").hexdigest())
print('\n')


print(hashlib.sha256("UNLV").hexdigest())
print('\n')
```

Figure 8: Python programming for hashing the input

The output of the values is shown in Figure 9, (lines 1, 2, 3, and 4).



```
da8562e7abc01a6f0d49a25d144ce6a9d7752a079c5d950ad5a93fd6d623f7fd

da8562e7abc01a6f0d49a25d144ce6a9d7752a079c5d950ad5a93fd6d623f7fd

4f53c044c3437016ba0d0af2d2e30ba010056347a5cdf514ba1e419160b29d48

ad3c89bd7bff24d9e104006e36a7ddb474c10a420e60d5335e2bf840b874644a

[Finished in 0.1s]
```

Figure 9: Output of the hashed value

We can see that same results are produced for the same input BTC and the results for different inputs (BTC and UNLV) are different. The slight change (making c of BTC to lowercase as BTc) produced an entirely different result.

SHA-256:

SHA (Secure Hash Algorithm) is a group of cryptographic hash functions published by the NIST (National Institute of Science and Technology) [12]. In the Bitcoin system, SHA-256 Hashing algorithm is used. This algorithm always outputs a 256-bit number which is usually represented in the hexadecimal number system. The output of the SHA-256 function is usually referred to as the hash of its input. The SHA group consists of four subgroups SHA-0, SHA-1, SHA-2, and SHA-3 [13].

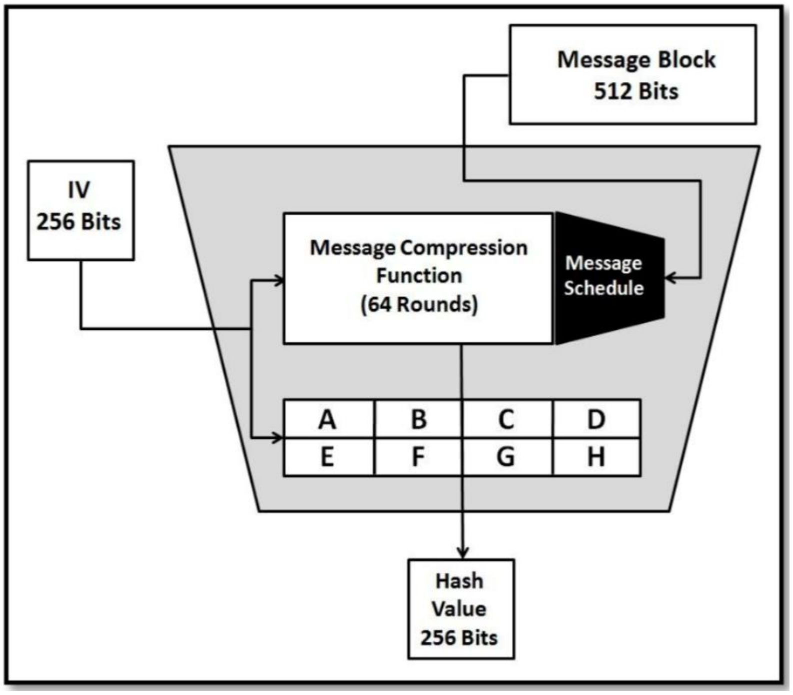


Figure 10: SHA 256 block diagram

Interestingly, Satoshi Nakamoto uses double hashing in Bitcoin protocol to make hashing more robust and also to prevent against attacks such as birthday attack. The Birthday attack is a scenario in attack where an attacker can produce the same hash as another input by using a completely different input (called collision). This breaks the property of hashing called uniqueness. Without it, two completely different Bitcoin blocks may be represented by the same hash, allowing attackers to potentially switch out the blocks.

2.7 Block and blockchain

The blockchain is one of the best inventions of the 21st century. Technically, blockchain is a time-stamped series of immutable record of data that is managed by a cluster of computers not owned by any single entity. Each of these records of data, called as a block is secured and bound to each other using cryptographic functions [14]. Initially, in 1991, a group of researchers described the blockchain. Their main purpose was to timestamp digital documents so that it becomes nearly impossible to backdate or tamper with them [15].

Bitcoin, later used this concept and introduced the digital currency based on blockchain. Today, the potential of blockchain is being used and researched for other sectors as well. There are a lot of users, developers, and enthusiast who truly believe blockchain technology is the future. The blockchain is a distributed ledger that is entirely open to anyone. It is a network of computers (called nodes) which contains the same history of transactions, validated by every new computer that wants to be part of the network. The blockchain is a back-linked chain of blocks which is shown in Figure 11.

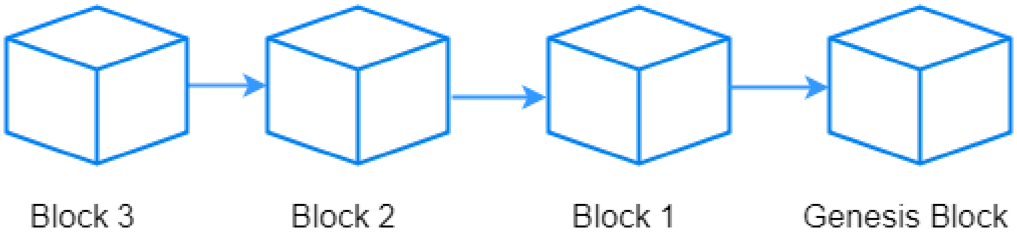


Figure 11: Blocks linked together

Block:

Bitcoin consists of chains of blocks that are linked together. Every block acts as a building material for a blockchain. Genesis block is the first block that was created in Bitcoin. The height of the Genesis block is 0. All the other blocks that are created after the Genesis block is added to the top of it. Every added block on the top of Genesis block increases the height of blockchain by 1. Every block contains certain information within it. The information such as the size of block, the total number of transactions in the block, the transaction itself and the block header is stored in a block. The structure of a block is shown in Table 1.

Item	Description
Block Size	The size of block in bytes
Block Header	Block Header with various fields
Counter	Counts the total transactions
Transactions	Transactions in the block

Table 1: Structure of a block

The block consists of a block header as one of its components. Block header is the summary of the contents of the block itself. It consists of the following six components as shown in Table 2.

Version	Version Number
Previous block hash	Reference to the hash of the parent block in the blockchain
Merkle root	Hash of the root of the Merkle tree of the block transaction
Timestamp	Creation time of the block
Difficulty target	Difficulty target to the Proof of Work algorithm
Nonce	Counter used for Proof of Work algorithm

Table 2: Structure of block header

Here, the root consists of the useful summary of every transaction in the block without having to look at each transaction. The overall structure of a block is shown in Figure 12. The blocks in a blockchain are linked together in such a way that present block has the hash of its previous block. The link of blocks in blockchain is shown in Figure 13. Since every new block is linked with each other in a blockchain, we can trace any block all the way back to the Genesis block [9]. This dependency and binding of the block together with each other makes it robust against potential hackers to tamper with any block in a blockchain. This is because change of information in any block in blockchain results change in the hash of present block causing error on the previous block which causes the error on its previous block and so on. The overall structure of a block is shown in Figure 12.

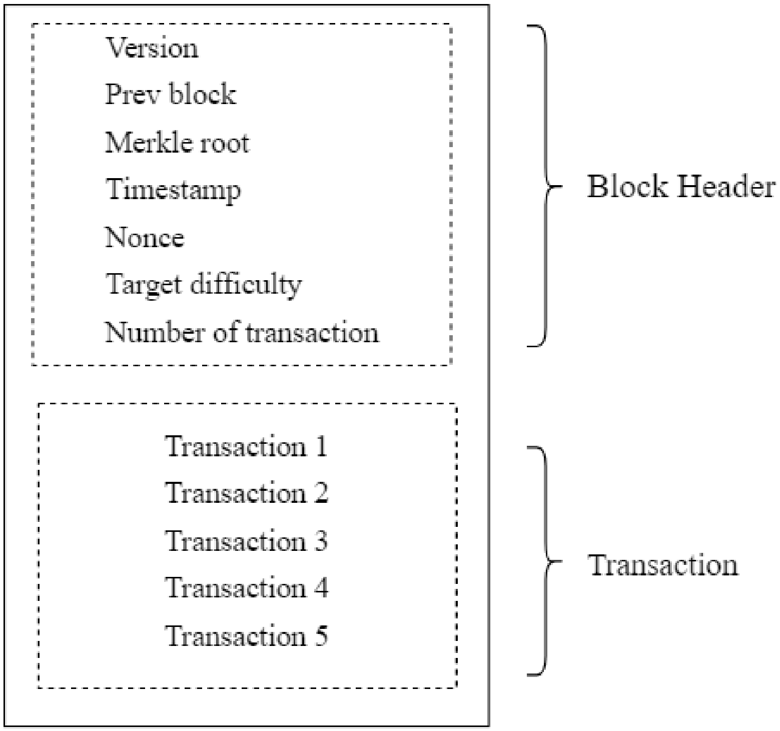


Figure 12: Structure of a block

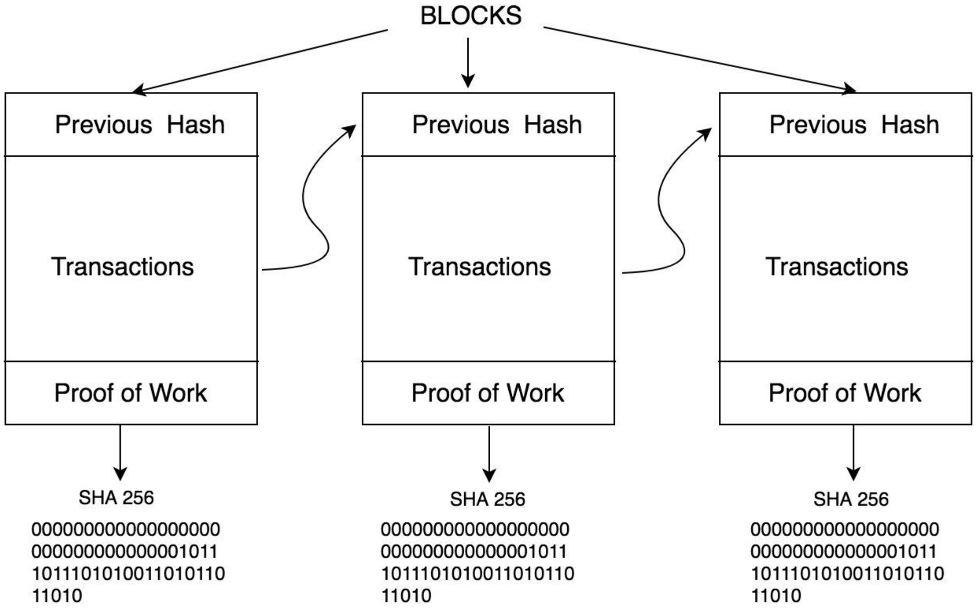


Figure 13: Chain of blocks in the blockchain

2.8 Merkle Tree

Merkle tree is a binary hash tree data structure [16]. The leaf in the tree contains the data. The data contains all the transactions made. The parent node, one level up in the tree, contains a hash of this data and is paired with another parent node. This continues all the way up to the root. In this way, the root node is the hash of all the data in the tree. The root hash is used in public, and it is relatively easy to verify that a particular data block is included in the Merkle tree. This is done by looking only at the block of data in the leaf and the path to the root. One can verify each of the hash of the tree all the way up to the root. If all the hashes are correct, then the block of data is included in the tree. If there are n nodes in the tree, it takes about log(n) time to verify a block of data [16].

Here in Figure 14, H is the hash and T is the transaction. The top hash is referred to as the root, and the intermediate hashes are branches. The hashes on the bottom are referred to as leaves. The Merkle root of any given block is stored in a header as mentioned in table 2.

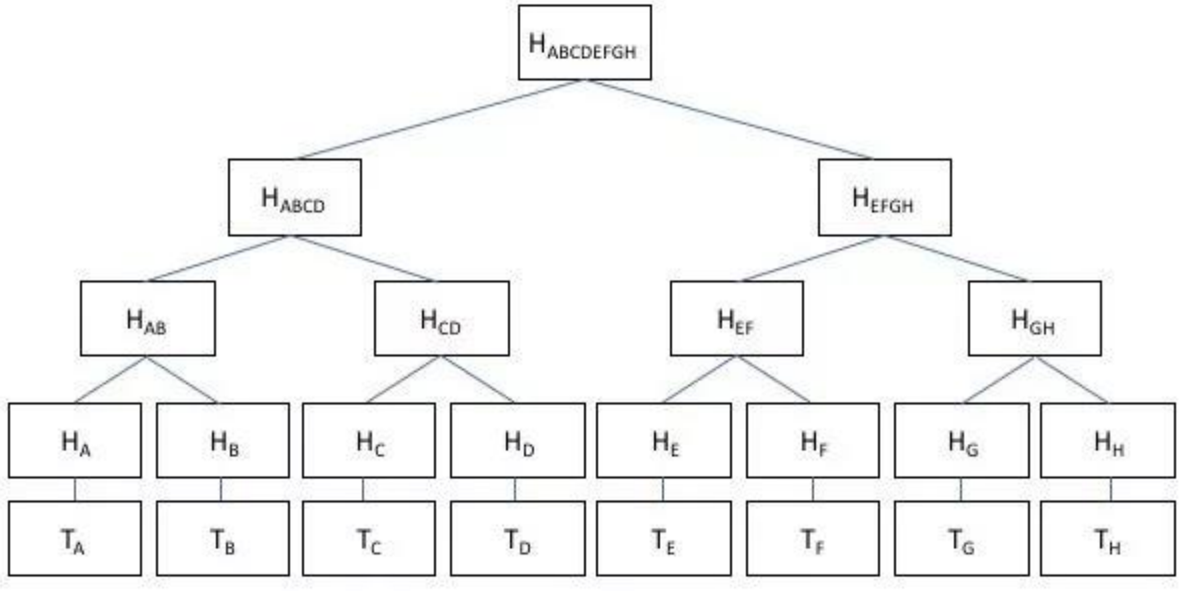


Figure 14: Merkle tree

2.9 Mining hardware

Bitcoin mining is the process of generating Bitcoins by solving the complex mathematical puzzle using hardware. Individuals called miners secure Bitcoin network. Hardware are required to mine Bitcoins, Different types of hardware are used by miners over time to mine blocks of Bitcoin. Originally Bitcoin mining was done by CPU and over the year's hardware changed to GPU, FPGA, and ASIC.

CPU Mining

Central Processing Units (CPUs) were used as mining hardware during the early stage of Bitcoin mining. It is considered as the first generation of Bitcoin mining. CPU mining was as simple as running the code below. The code search nonces in a linear fashion then compute SHA-256 in software and check if the result is a valid block [17]. As mentioned earlier, the SHA-256 is applied twice in the code itself.

```
target  = ( 65535 << 208 ) / difficulty ;
coinbase_nonce = 0;
while ( 1 ) {
        header = blockHeader (transactions,coinbase_nonce);
        for ( header_nonce = 0 ; header_nonce < ( 1 << 32 ) ; header_nonce++ ) {
                if  ( SHA256 ( SHA256 ( blockHeader ( header , header_nonce ) ) ) <  target )
                        Break;      // block is found
        }
 coinbase_nonce++;
}
```

On a high-end desktop PC, the computation is about 20 million hashes per second (MH/s). At that speed, it would take several years on average to find a valid block.

GPU Mining

GPU mining is considered as the second generation of Bitcoin mining. GPU mining started because of low computation power of CPU mining. GPU mining performed better than CPU mining but could not cope up with the increasing difficulty rate over time. There are drawbacks on GPU mining which are overheating and high level of hardware utilization during the mining process.

FPGA mining

FPGA mining is considered as the third generation of Bitcoin mining. After the first implementation of Bitcoin mining came out in Verilog, several miners switched from GPU mining to FPGA mining. The computation power of FPGA mining was much better than GPA mining during that time. Later on, the number of miners increased which increased the difficulty of the network. Due to the increase in difficulty of mining the blocks, FPGA mining could not satisfy the expectations.

Figure 15: Bitcoin mining using several FPGAs

ASIC mining

ASIC mining is the fourth generation of Bitcoin mining. Mining today is dominated by Bitcoin ASICs. These ASIC chips are designed, built, and optimized for the sole purpose of mining Bitcoins. There are some big vendors who produce ASIC mining hardware and sell it to the customers. Some of the examples of ASIC mining hardware that are used today are Antminer S9, Terminator T3, Dragonmint T1, etc.

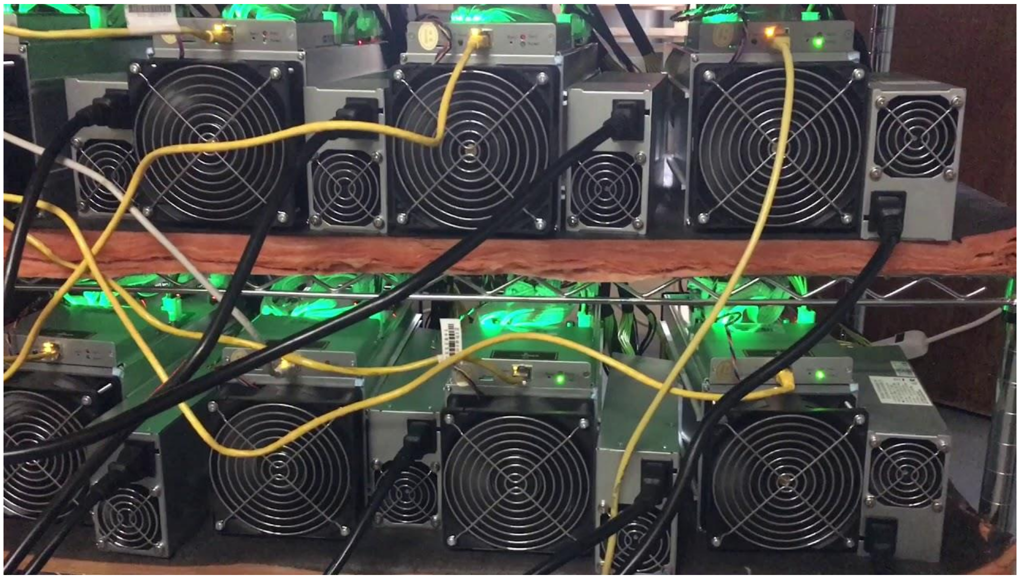


Figure 16: Antminer S9 for Bitcoin mining

During the process of mining, every miner has to with high electricity cost and excess heat produced by the hardware. The alternate to avoid these issues is using cloud mining since the miner does not have to worry about high electricity cost and excess heat [9]. However, it has a few other limitations like risk of fraud, lower profit and lack of control and flexibility which makes it ineffective to other mining techniques.

As mining evolves, more and more companies begin manufacturing dedicated hardware for Bitcoin mining. The most popular Bitcoin miners on the market are [18]:

EBIT E11++, Terminator T3, Antminer S15, DragonMint T1, Antminer S9, AvalonMiner 841, etc.

The specifications of these Bitcoin Miners are shown in Table 3.

SN	**BTC Miner**	**Manufacturer**	**Power consumption**	**Hash rate**	**Efficiency**	**Chip process**	**Noise level**
1	Ebit E11++	Ebang	2000W	44TH/s	0.096 J/GH	10nm	75db
2	Terminator T3	Innosilicon	2100W	43TH/s	0.098J/Gh	10nm	75db
3.	Antminer S15	Bitmain	1600W	28TH/s		7nm	75db
4	DragonMint T1	Halong Mining	1480W	16TH/s	0.0925J/GH	10nm	75db
5	Antminer	Bitmain	1350W	14.5TH/s	0.093J/GH	16nm	76db
6	AvalonMiner 841	Canaan	1290W	13.6TH/s	0.099J/GH	16nm	65db

Table 3: The list of popular Bitcoin mining hardware as of 2019.

The miner uses the processing power of their hardware to solve the complex mathematical puzzle and validate the block. Bitcoin mining is the process of adding transaction records to Bitcoin public ledger [6]. A transaction is only considered to be valid when the sender signs it. The difficulty of mining gets harder as more miners join the network. The Bitcoin protocol is adjusted in such a way that a block is verified and added to the blockchain network in an average of 10 minutes. The block having Proof of Work is considered to be a valid block. Reward is provided to the miner who successfully mines a block. The miners are provided with Bitcoin as a reward (currently, 12.5 Bitcoin per block) for their work done on verifying the block. Besides reward, they also obtain the transaction fee from all the transactions that are included in the block. This reward system encourage the miners to mine the Bitcoin. The general working process of Bitcoin blockchain is demonstrated in Figure 17.

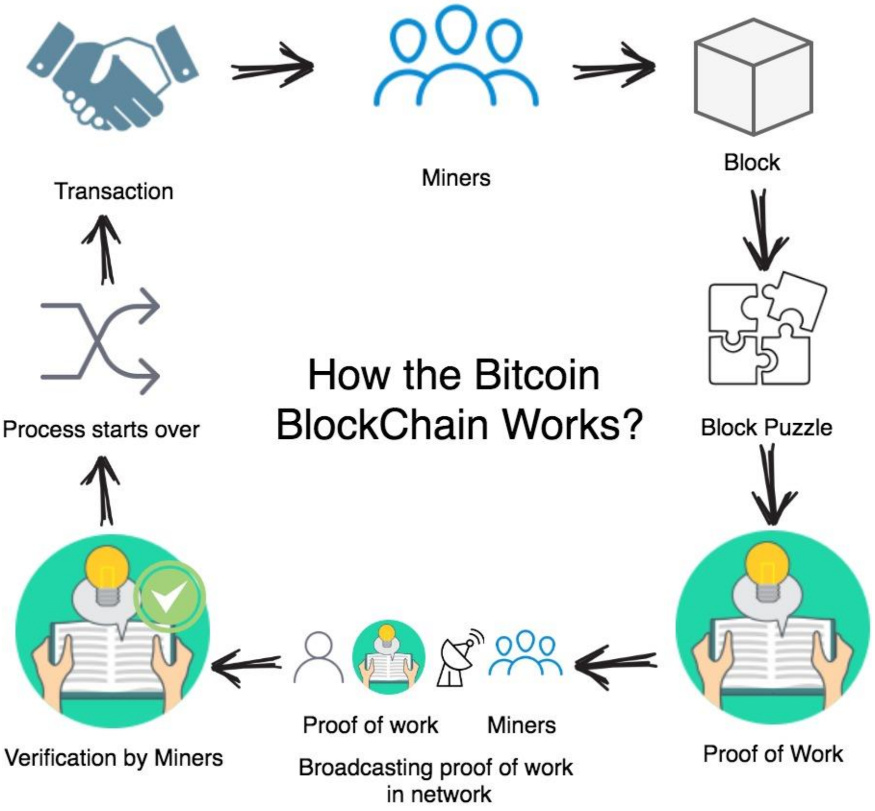


Figure 17: Working mechanism of bitcoin blockchain

The steps to run the network are as follows [2]:

- New transactions are broadcast to all nodes in a network.
- Miners verify if the broadcasted transactions are valid.
- New transactions are bundled into a block by each node.
- Each node works on finding a valid proof-of-work for its block.

- When a node finds a valid proof-of-work for its block, it broadcasts the block to every nodes in a network.
- Nodes accept the block only if all transactions in it are valid and not already spent.
- Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

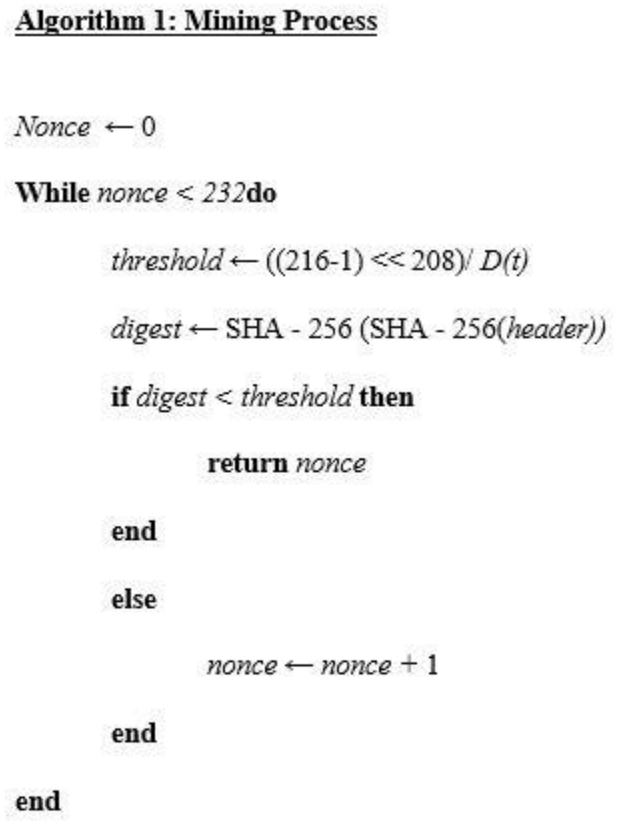
2.10 Proof of Work (PoW)

PoW is a consensus algorithm introduced by Bitcoin and used widely by many other cryptocurrencies. It consists of a complex cryptographic mathematical puzzle. It scans for a value called nonce (number only used once). The nonce is a counter used in the block header, which the miners manipulate to change the hash value of a block to meet the hash criteria. The value of nonce when hashed with SHA-256, the resulting output hash begins with certain number of zeros [10]. The exponential to the number of zeros in the correct hash determines the average work required for a particular block. This signifies that the Proof of Work contains a high level of computation on the verification process. This high level of computation is achieved by the hardware used by miners. The miners mine the block by calculating the hash of that block with a varying nonce. There is no particular formula or pattern to vary the nonce. It is varied in a random order. The miner vary the nonce until the resultant hash value becomes equal or lower to a given target value.

Target:

A target is a 256-bit number that all miners share [19]. The target directly affects the difficulty of the Bitcoin network: the lower the target, the harder is it to discover a block. After every hash, the number is compared with the target value which is 256- bit value, if this is less than or equal to the target value, then the miner who sends the number gets rewarded. Otherwise, the nonce gets increased, and the process is repeated. Here the fast miners have a higher chance of winning, but the process is random, and the slower miners also have chances to win. The target value is re-calculated after every successful 2016 mined blocks It takes around 14 days to mine 2016 blocks which is shown on determining the difficulty section.

The mining algorithm [19] used for the mining process is shown in Algorithm 1.



Algorithm 1: Mining Process

```
$Nonce \leftarrow 0$
While $nonce < 232$ do
    $threshold \leftarrow ((216-1) << 208) / D(t)$
    $digest \leftarrow \text{SHA - 256 (SHA - 256}(header))$
    if $digest < threshold$ then
        return $nonce$
    end
    else
        $nonce \leftarrow nonce + 1$
    end
end
```

The flowchart for the mining process is shown in Figure 18.

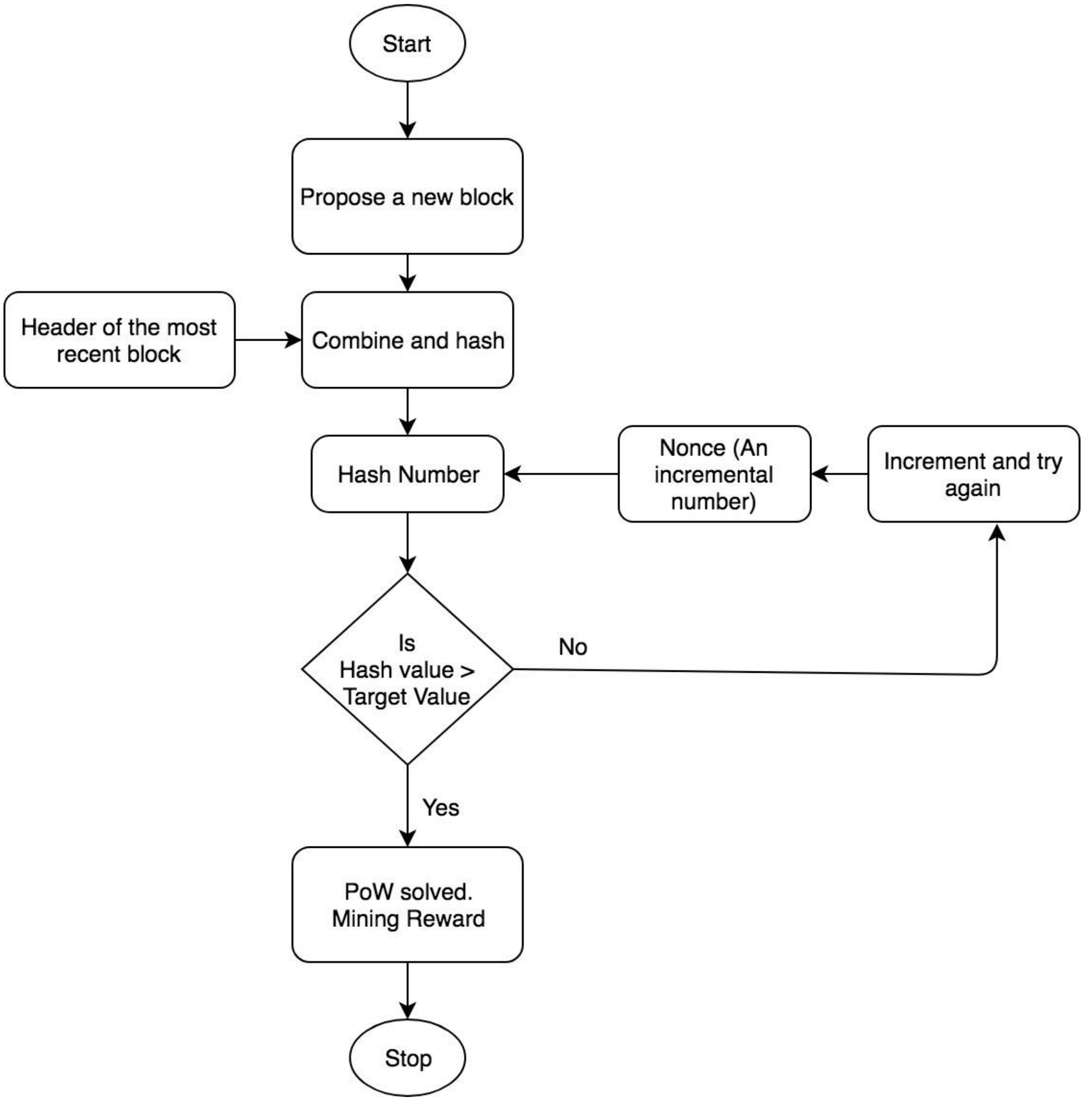

Start
Propose a new block
Header of the most recent block
Combine and hash
Hash Number
Nonce (An incremental number)
Increment and try again
Is Hash value > Target Value
No
Yes
PoW solved. Mining Reward
Stop

Figure 18: Flowchart of a Bitcoin mining process

Process of mining

In order to be a Bitcoin miner, joining the Bitcoin network and connecting to other nodes is mandatory. There are mainly six tasks that are needed to be performed by miners.

1. Miner has to listen for the transactions that are broadcast on the network. They must verify those transactions by checking the correctness of the signatures and also the outputs have been spent before or not. This is done to mitigate double spend problem.

2. Before joining the network, miners must have all the previous blocks that are the part of the blockchain. They listen for the new blocks that are broadcast on the network. Then they must validate each block that is received by validating each transaction in the block. They also have to check whether the clock has valid nonce or not.

3. Once the miners have the latest copy of the blockchain, they can begin building their own blocks. To do this, the miner group transactions that are heard into a new block which extends the most recent block.

4. Now miners have to find a nonce that makes the block valid. This is one of the crucial steps during mining which requires much work.

5. Assume that the block is accepted after finding a nonce. There is no guarantee that the block will be part of the consensus chain even if the block is accepted. If the other miners accept the same block and start mining on top of it, then the block will be a part of the consensus chain [20].

6. If all the miners accepted the block and added to the part of the consensus chain, then the miner who worked on finding the nonce for that particular block will get rewarded. The block reward as of now is 12.5 Bitcoins. In addition to that, if any of the transactions in the block contained transaction fees, the miner collects those transaction fees too.

Mining Reward

The reward for Bitcoin mining is decreasing with the number of Bitcoins mined. The total number of Bitcoin that can be mined is limited to 21 Million. The reward decreases by half after every successful 210,000 blocks mined. The time period of mining 210,000 blocks is around four years. In the present date, the reward is 12.5 Bitcoins. Initially, the reward for mining the Bitcoin was 50 Bitcoin. Apart from the reward that miners get from mining, they also receive an amount called as the transaction fee for every successful addition of transaction in the blockchain [4]. Generally, the transaction fee is 1% of the block reward. From

Figure 19, we can see the decrease in Bitcoin reward after every 210,000 blocks or approximately four years. Since the reward decreases geometrically with increase in time, it can be verified that there will be no more than 21 Million Bitcoin.

210,000 (50 + 25 + 12.5 + 6.25 + 3.125 + ...) ~ approx. 21,000,000 Bitcoins

Time	BTC Reward
Jan 2009 - Nov 2012	50 BTC
Nov 2012 - Jul 2016	25 BTC
Jul 2016 - Feb 2020	12.5 BTC
Feb 2020 - Sep 2023	6.25 BTC

Figure 19: Bitcoin mining rewards

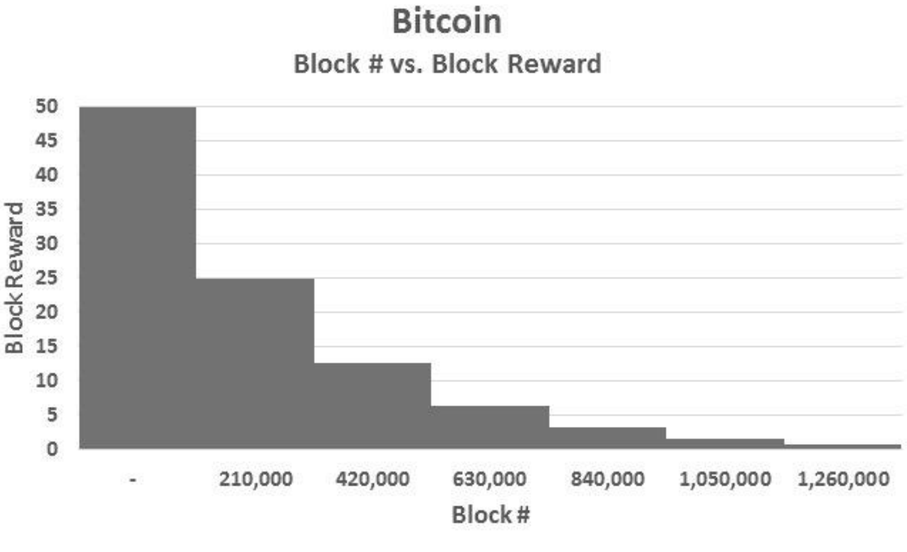


Figure 20: Block vs. block reward

Determining the difficulty:

The difficulty of Bitcoin mining changes every 2016 blocks. The time to mine 2016 blocks of Bitcoin is around two weeks. This signifies that the difficulty of Bitcoin mining is re-calculated about once every two weeks. The formula to calculate the difficulty of Bitcoin mining is shown as:

*new_difficulty = (old_difficulty * 2016 * 10 min) / (total time to mine previous 2016 blocks)*

Here, 2016*10 min is exactly two weeks,

*2016*10 = 20160 min*

= 20160/60 (hours) = 336 hours

= 336/24 (days) = 14 days

= 2 weeks

Therefore, it would take around two weeks to mine 2016 blocks if a block were created exactly every 10 minutes. The difficulty of the mining process is self-adjusting to the accumulated mining power of the network. If more miners join the network, the difficulty gets increased, and it will be harder to solve the problem; if many of them drop off, the difficulty decreases, and it will get easier [18]. The difficulty rate has to be increased or decreased in order to control the new block creation speed.

Mining Methods

There are two different types of mining methods that are used to mine bitcoin. One method is solo mining, and the other is pool mining.

Solo Mining

Solo mining refers to mining of Bitcoin by an individual using their hardware resources and working independently. Since solo mining refers to individual mining, it requires a lot of resources in terms of hardware to compete with other miners and get the mining reward for solving the block. The reward is collected by the miner alone and can get much profit if the miner has good hardware resources. The main drawback for solo mining is that it may take years for solo miners to generate a valid block due to the limited hardware resource. Before the introduction of pool mining in 2011, all the miners were solo miners [21].

Pool mining

Pool mining is a way for miners to pool their resources together to obtain steady payouts. Each pool uses one unique ID to mine Bitcoins [9]. In pool mining, all the miners combine their hardware resources so that they have high power and the mining can be much faster than solo mining. A pool assigns a lower difficulty value to each of its members. It becomes easier for each miner in a pool to solve the hash problem and proof of work.

Each pool miner submits their own work by presenting the hash value under the pool target value (called shares) to the pool for verification. If a share is under network target value, a block is claimed by the pool and pool operator will distribute reward to every pool miners. Most popular payout in pool mining is “Pay-per-share” [21]

Chapter 3

LITERATURE REVIEW

Bitcoin cryptocurrency has been an international sensation. In recent years, there has been a massive interest of people towards Bitcoin cryptocurrency. Several people have started Bitcoin mining as their business and many other companies have started using Bitcoin as a payment method. Since it has been only a few years that Bitcoin was created; there are still lots of research being done on Bitcoin cryptocurrency. As of now, there are a few research papers dealing about different aspects of Bitcoin such as its mining, its security and several attacks on mining pool. Satoshi Nakamoto [2] mentioned every aspect of Bitcoin protocol on his white paper that was released in 2009 AD. The Bitcoin to be the first digital cryptocurrency, but the concept of cryptocurrency and the cryptographic algorithms lying behind it was proposed earlier by David Chaum in his paper in 1983 [22]. The consensus algorithm in Bitcoin is Proof of Work and the idea behind it was originally proposed by Cynthia Dwork and Moni Naor on their paper in 1992 [23]. Decentralization in Bitcoin is achieved by using the concept of blockchain which helps to solve the double spending problem in Bitcoin [24].

Many cryptocurrencies came into existence after Bitcoin was proposed. Most of them follow Proof of work as the consensus algorithm for solving a complex puzzle. However, Proof of Work algorithm is not the only one which is used in cryptocurrencies. Several consensus algorithms like Proof of stake, Proof of activity, Proof of capacity, Proof of Burn were proposed for other cryptocurrencies. Proof of work consensus algorithm has a major drawback that it takes massive energy. Proceeding to that, later came out with another consensus algorithm called as Proof of Stake [25]. This algorithm was introduced to eliminate the high electricity consumption. Cryptocurrencies like Peercoin, Dash, Cardano, KuCoin, etc. use Proof of Stake as the consensus algorithm. However, in 2014, a paper entitled “On Stake and Consensus” written by

Andrew Poelstra [26] verified that the distributed consensus from Proof of Stake is impossible which gave a conclusion that Proof of Work can’t be replaced by Proof of Stake.

Michael Bedford Taylor examined the Bitcoin Hardware movement from first generation miners to the development of customized silicon ASICs [27]. The first publicly available miner was CUDA miner that was released in September 2010. Then shortly after pool mining was started. In this highly competitive environment, individual mining (also known as solo mining) does not stand a chance. The likelihood of finding a valid block and compensating that to hardware and electricity cost is incomparable. Mining Pool gave a chance to solo miners to collaborate their hashing power on the mining pool and share the reward if they were able to mine a block. Andreas M.Antonopoulos on his book “Mastering Bitcoin” [28] gave an example which shows solo mining at this time is waste of money unless they are very rich to afford lots of ASIC hardware. He encourages solo miners with low budget to move towards pool mining for Bitcoin mining.

3.1 Hardware used for mining:

There are several experiments done on different varieties of hardware. These experiments are necessary to understand how different hardware performs during the mining process. Karl J. O’Dwyer and David Malone presented their paper named “Bitcoin Mining and its Energy Footprint” [29] by comparing different hardware with reference to parameters like hash rate, efficiency, power consumption and cost. The comparison is shown in Figure 21 and 22.

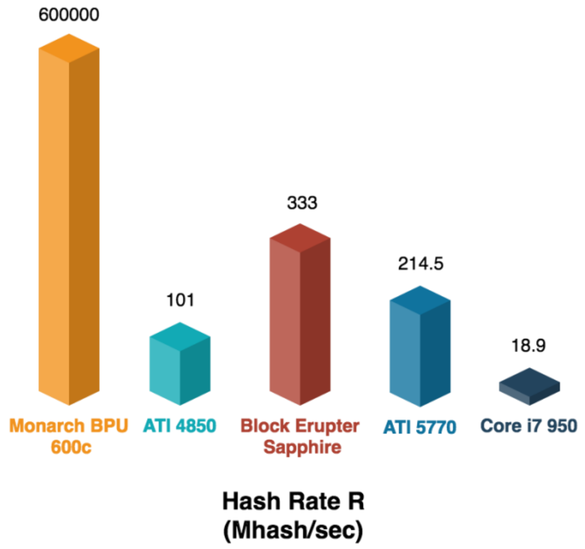


Figure 21: Hardware comparison with reference to hash rate

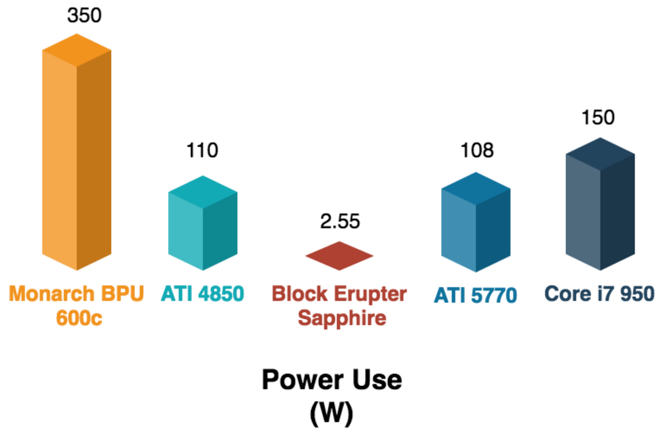
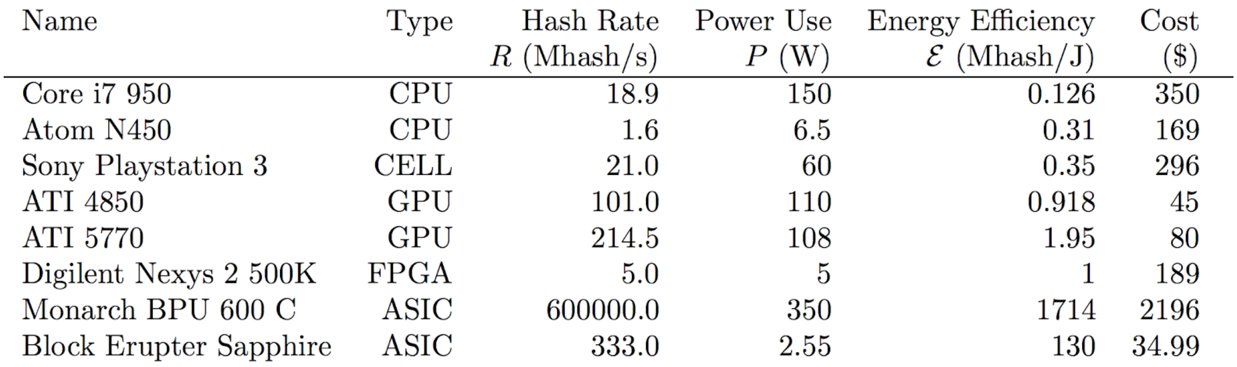


Figure 22: Hardware comparison with reference to power use

According to the comparison done by the authors, we can see the performance of hardware during Bitcoin mining in 2014. They have compared hardware with reference to hash rate, power, cost, and efficiency which is shown in Table 4. From Table 4, we can analyze that the maximum hash rate of 600,000 Mhash/sec is achieved by Monarch BPU 600c but consumes a lot of power and the hardware cost is expensive.

However, ATI 5770 is cheap and delivers 214.5 Mhash/sec by consuming only 108 watt power. This seems to be the efficient hardware among other hardware.



Name	Type	Hash Rate	Power Use	Energy Efficiency	Cost
		R (Mhash/s)	P (W)	$\mathcal{E}$ (Mhash/J)	($)
Core i7 950	CPU	18.9	150	0.126	350
Atom N450	CPU	1.6	6.5	0.31	169
Sony Playstation 3	CELL	21.0	60	0.35	296
ATI 4850	GPU	101.0	110	0.918	45
ATI 5770	GPU	214.5	108	1.95	80
Digilent Nexys 2 500K	FPGA	5.0	5	1	189
Monarch BPU 600 C	ASIC	600000.0	350	1714	2196
Block Erupter Sapphire	ASIC	333.0	2.55	130	34.99

Table 4: Comparison of Bitcoin mining hardware

Several miners and researchers tried mining on different types of CPU, GPU and ASIC hardware to explore the efficient and better way of mining Bitcoin. Over the time mining hardware changes and also the numbers of miners mining the Bitcoin. This increases the competition between the miners to mine a particular block. According to Calvin Ho on his paper [30] there, are several comparisons done based on different hardware. The comparison of price, power and hash rate on different hardware is shown in Figure 23.

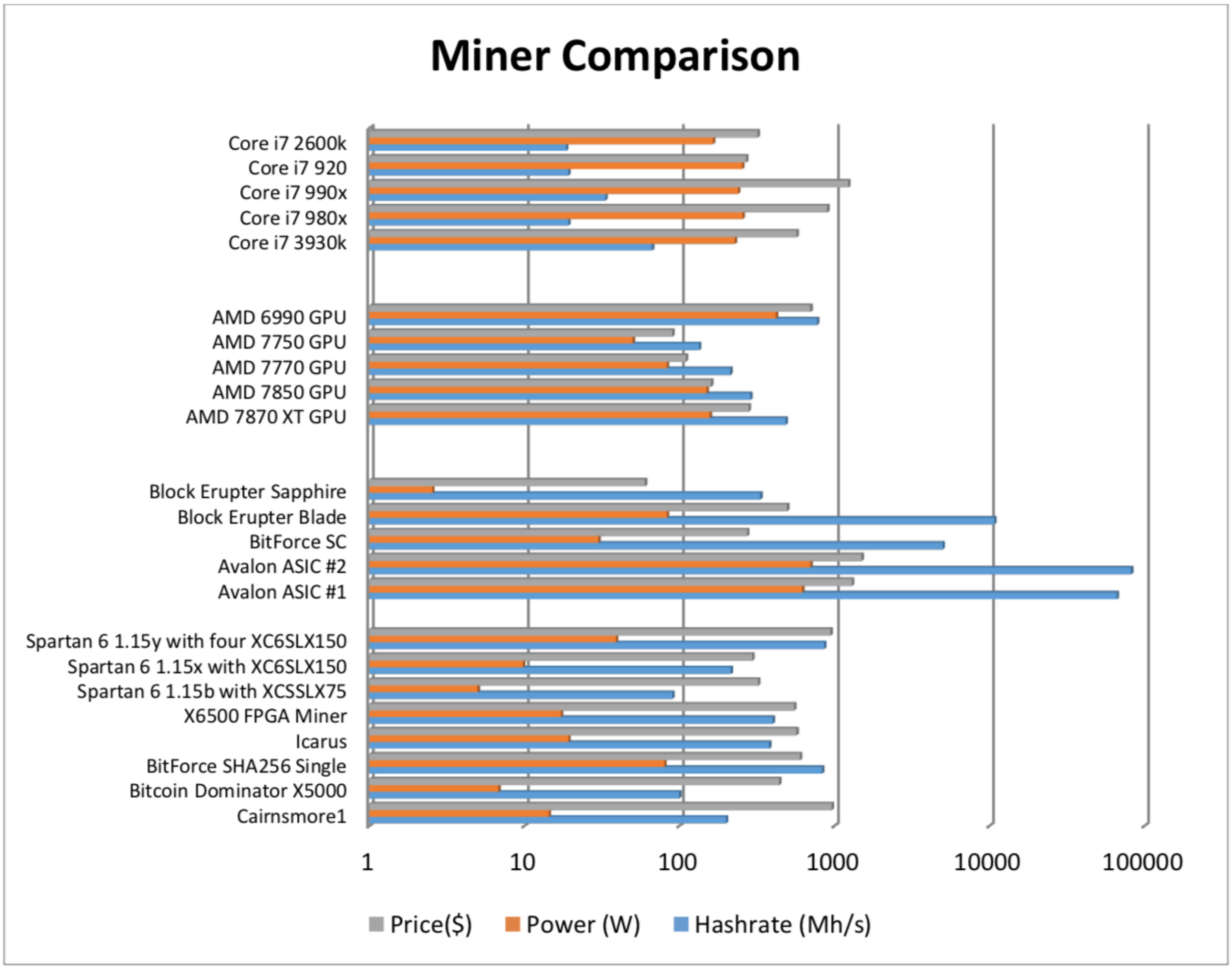


Figure 23: Hardware comparison based on price, power and hash rate

Figure 23 shows the comparison of different types of hardware miner shows that the dedicated ASIC miners such as Avalon ASIC #1, Avalon ASIC #2, Block Erupter Blade has shown the best performance with the lowest price and consuming a lot of less power. ASIC miners are specially designed for mining purpose only whereas CPU and GPU are designed primarily for some other purpose other than mining. The cost for high specs of Core i7 CPU is similar to the price of ASIC miner called Avalon ASIC #2, but the performance of mining is much better than the CPU.

3.2 Security of Bitcoin:

Being the most popular cryptocurrency, Bitcoin has got several security threats since its inception, and several countermeasures have been applied. The most common problem that occurred at the beginning was a double spending attack. Mauro Conti and his team [10] has analyzed the security issue of Bitcoin introducing several attacks and their preventive measures. A paper published in 2014, [31] gave some insights on Sybil resistant attack on Bitcoin. After the inception of pool mining, the security aspect of Bitcoin mining has been a problem. There security analysis of pool mining has been done by [10] [31] on their papers. Some of the major attacks on Bitcoin are mentioned below.

Double Spending attack

In conventional terms, double spending is the result of successfully spending some money more than once. Double spending is a situation where the person sends two different transactions simultaneously within a concise period and is able to spend the same Bitcoin in two different transactions [10]. The primary targets in this problem are sellers. This is because the Bitcoin can never be double spent, but due to the rapid succession, it seems like Bitcoin was not spent previously. Bitcoin Handles the double spending problem by implementing a confirmation mechanism and maintaining universal ledger called the blockchain. Since the transactions are made in rapid succession for the same Bitcoin, when a miner verifies the first transaction and publishes it in the blockchain, the second transaction will be invalid. There may be a case that both transactions are verified and published by a miner at the same time [32]. In order to prevent this issue, the Bitcoin system looks up at least six confirmed transactions so that there may not be a possibility that all six confirmations are verified and published at the same time. The block with the largest valid transaction will be added in the blockchain.

Sybil Attack

It is the attack where the attacker creates multiple virtual identities and fills the network with their control. In this case, many miners are likely to connect to the attacker node. The primary target for this attack is Bitcoin network, miners and users. The possible countermeasure done for this attack is by using a two-party mixing protocol which is presented by G. Bissias and his team in 2014. [31].

DDoS attack

The DDoS attack is termed as Distributed Denial of Service attack. It is a collaborative attack done by attackers to exhaust the network resources. It is done by sending so many data to the network so that it cannot process normal Bitcoin transaction. The primary target in this attack is Bitcoin currency exchanges, eWallets, and mining pools. There are several countermeasures applied to prevent this attack like,

- Restricting the block size to 1 Mb.
- Restricting the maximum number of signatures checks a transaction input may request.
- Fast verification signature-based authentication
- Proof of activity protocol [33]

Chapter 4

ANALYSIS AND PROPOSED SOLUTION

Bitcoin mining is a difficult thing since it requires a lot of hardware and power. We tried to mine Bitcoin on Desktop Pc, laptop and few other FPGA boards. However, we could not mine Bitcoins to come up with a better solution by comparing several factors and implementing a new approach. This is due to the low computation power of the hardware that was used. The hash rate achieved by the hardware that are used for mining Bitcoin is shown in Table 5.

Specifications	Hash rate
Intel® Core™ i7-2600 CPU @3.4GHz (8CPUs) 8 GB RAM(Windows PC)	260.5 KH/S
Intel® Core™ i5-4200 CPU @2.3GHz (4CPUs) 6 GB RAM(Windows Laptop)	187.6 KH/S
Intel® Core™ i5-7200 CPU @2.3GHz (2CPUs) 8 GB RAM (Macbook Pro)	16MH/S
Bitman Antminer U2 (USB Miner)	2.2 GH/S

Table 5: Hardware used for Bitcoin mining

The hash rate given by the hardware on Table 5 was on Kilohashes/second, Megahashes/second, and Gigahashes/second which is very low compared to Exahashes/sec hash rate as of today. Since they are the first generation and second generation Bitcoin mining hardware we could not come close to today’s fourth generation mining hardware performance. Getting new hardware for the purpose of this thesis is extremely expensive and not feasible since there is no guarantee of mining Bitcoin in the given timeframe just by buying expensive hardware.

Due to few limitations as mentioned earlier, we approach Bitcoin mining in a different way by creating an account on several mining pools to collect their real-time data on Bitcoin mining along with different recent Bitcoin mining hardware comparisons in terms of efficiency, power consumption and price. We also analyzed different performance on solo mining and pool mining by collecting real-time data on Bitcoin mining. We also collected an average electricity rate for mining 1 Bitcoin per country to calculate the mining profit for any individual or companies. The analysis of Bitcoin mining in this section deals on various aspects of Bitcoin mining with real-time data and provides a better solution for aspiring Bitcoin miners.

4.1 Bitcoin market Data

The market for Bitcoin is getting bigger day by day. The market capitalization stands approximately at $68.8 Billion with a total volume of around $9 Billion transactions every day. The Bitcoin market is growing with a total capital of around 71 Billion USD. The Bitcoin market capital chart from September 2013 to this date is shown in Figure 24 [6].

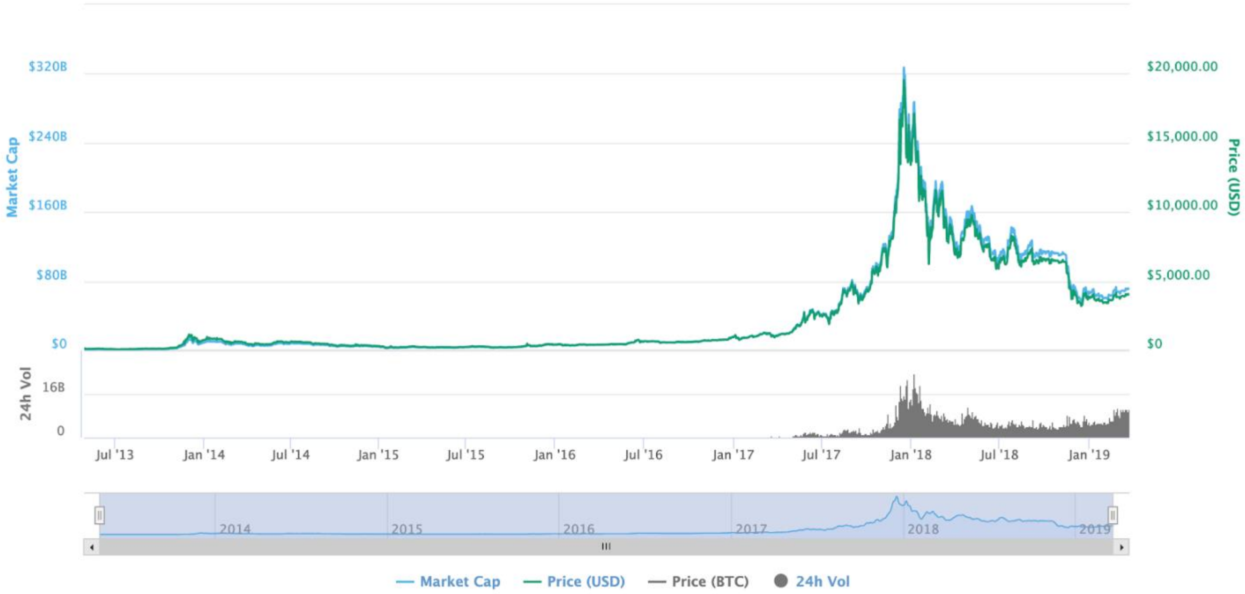


Figure 24: Growth of the Bitcoin Market from 2013 to 2019.

From the graph on Figure 24, we can analyze the price of Bitcoin per USD. Bitcoin's price was around 200 USD during Jan 2017. After that period, its price jumped exponentially high till December 2017 creating a new record of 1 Bitcoin = 19,000 USD. The Bitcoin market capital was around 320 Billion USD. Since then its price dropped back and currently its 4047 USD per 1 BTC with a total market capitalization of 72 Billion USD.

Percentage of total market capital (Dominance)

The graph in Figure 25, shows the total market dominance of Bitcoin compared to other cryptocurrencies. Bitcoin is leading by a massive margin since the beginning. During September 2017 to January 2018, other cryptocurrencies like Ethereum, Litecoin came into light reducing the dominance of Bitcoin. Later Bitcoin came back to its original shape of dominance.

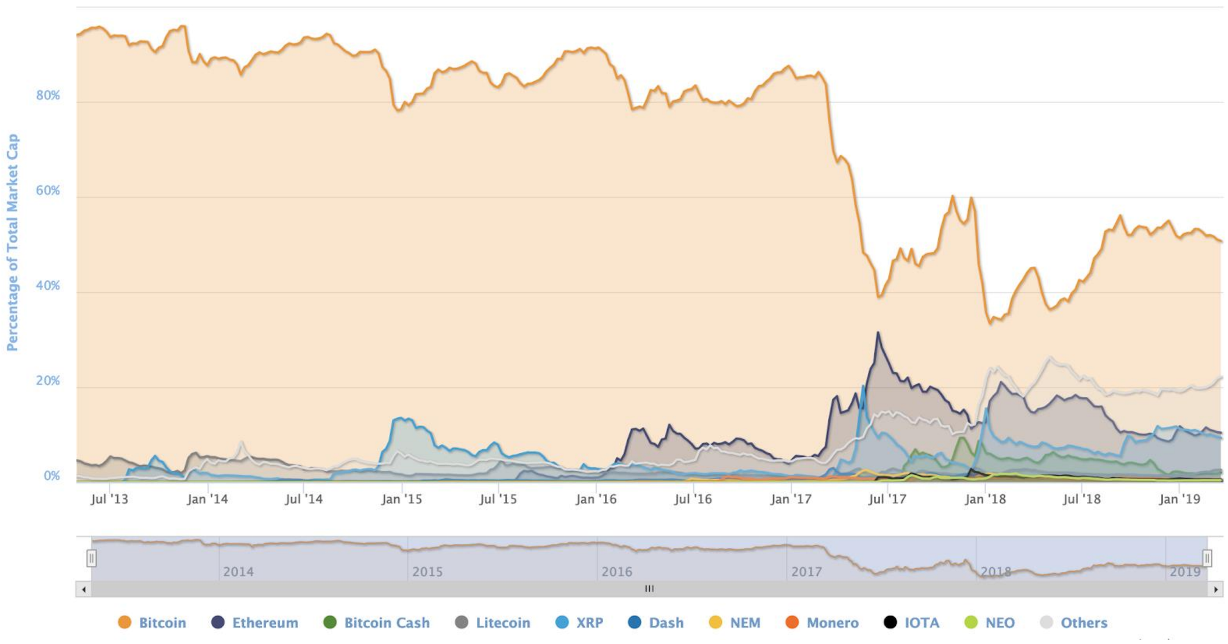


Figure 25: Percentage of total market capital (Dominance)

In order to get Bitcoin there are mainly three different ways:-

- Buy it from the exchange market
- Get it from the Bitcoin ATM
- Mine the Bitcoins

Exchange Market:

We can buy Bitcoin through the exchange market. There are several exchange markets from where we can buy Bitcoin and some other cryptocurrencies. Some of the examples of exchange market are Bitfinex, Gdax, Binance, Bitstamp, Kregen, etc. Based on the present value of Bitcoin we can buy Bitcoin from these exchange market.

Bitcoin ATM:

There are several Bitcoin ATMs all around the world that let us purchase Bitcoin with cash. There is a total of around 4428 BTC ATM all around the world as of March 18, 2019 [34]. The report shows that the rate of BTC ATM installation is 3 ATM per day around the world. Figure 26 shows the total number of Bitcoins ATM found in the world. Similarly, the rate of increase of Bitcoin ATM installations is shown in Figure 27.

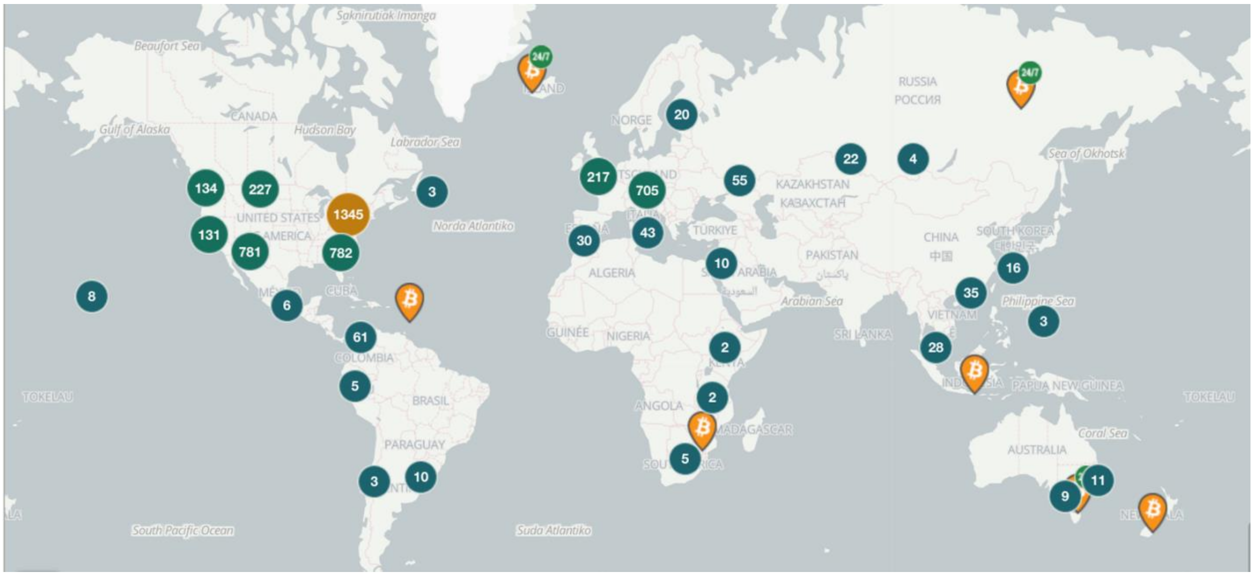


Figure 26: Bitcoin (BTC) ATM machines around the world.

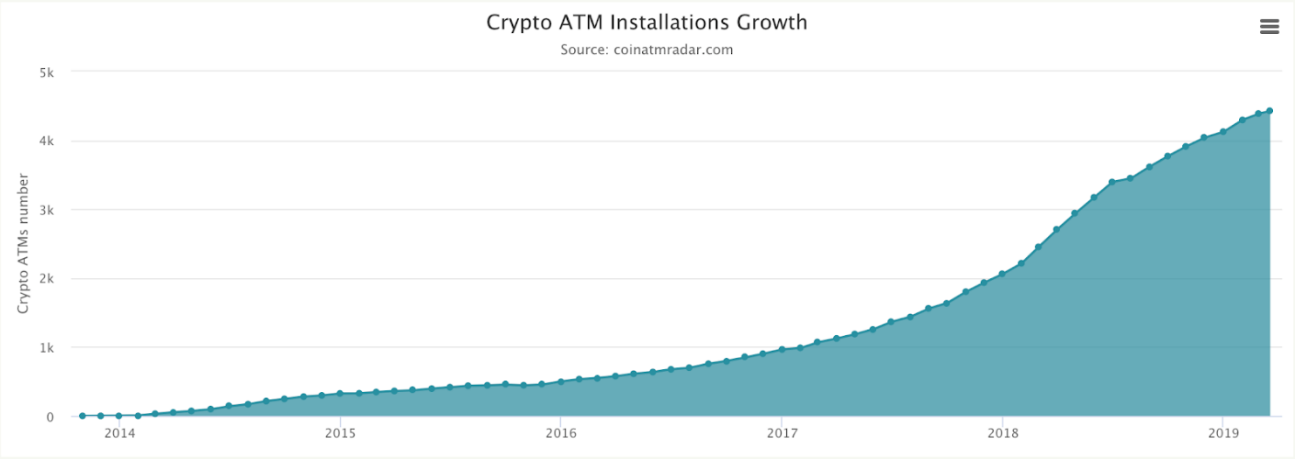


Figure 27: Growth of Crypto ATM installations around the world

In order to get Bitcoin from Bitcoin ATM, we need to insert cash in the machine, and the bitcoins will be sent to our wallet.

Mine the Bitcoins:

Mining is another option to get Bitcoins. In order to mine Bitcoin, we can use two methods as discussed earlier. Since solo mining requires a lot of resources and even does not guarantee successful mining due to its low computation power, pool mining could be the better option for most of the miners.

The statistics of a Bitcoin for a particular day is shown in Table 5. The statistics found in Table 6 are for March 21, 2019 [35]

Price	$4,026
Hash rate	43,141,132 TH/S
Difficulty	6,068,891,541,676
Transactions per day	300,712
Average Value	0.53363 BTC
Average Fee	0.00011815 BTC
Unconfirmed Transactions	364
Mempool (total pending transactions)	139,201 Bytes

Table 6: Bitcoin statistics for a particular day

From Table 5, we can see there are 364 unconfirmed transactions out of around 300,712 successful transactions per day. The blockchain simply ignores these unsuccessful transactions. The hash rate which is also referred to as the computation rate is 43,141,132 TH/S.

The conversion of Hash rate from hash per second to ZettaHash per second is shown as following:

1 ZettaHash = 1000 Exahash

= 1 x 10^{6} *Petahash*

= 1 x 10^{9} *Terahash*

= 1 x 10^{12} *Gigahash*

= 1 x 10^{15} *Megahash*

= 1 x 10^{18} *Kilohash*

= 1 x 10^{21} *hash*

4.2 Mining Pool

Mining pool came into existence after 2011 AD. A mining pool is a place where miners share their resources on a network and mine to claim the reward. Due to the increase in difficulty rate and the decrease in the computation power of mining hardware for the given difficulty, pool mining was operated. As of now, there are thousands of mining pool that are mining Bitcoin. Some of the popular mining pool are Btc.com, F2pool, Slushpool, etc. Since every miner is continuously competing to mine a single block, it becomes challenging for the mining pool which has fewer hardware resources. The chart in Figure 28, shows the network share data of the most popular bitcoin mining pools over the past year [36].

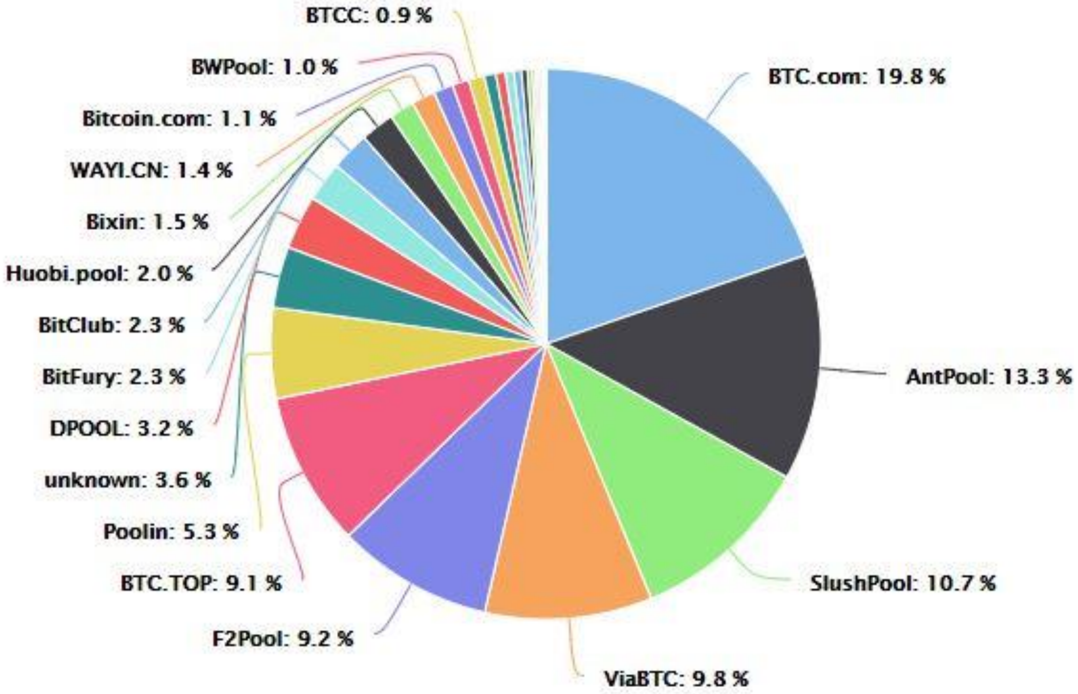


Figure 28: Bitcoin Mining Pools across the globe.

From the chart in Figure 28, we can see that the most popular Bitcoin mining pool is BTC.com over one year period of time followed AntPool, SHulshPool, ViaBTC, and f2Pool. If we dive into the details of every mining pool, we can see how fast each pool mines the Bitcoin and is it profitable for any Bitcoin miner to be on that specific Pool. These data are obtained from [36]. The historical distribution of the mining poll for the past one year is shown in Figure 29.

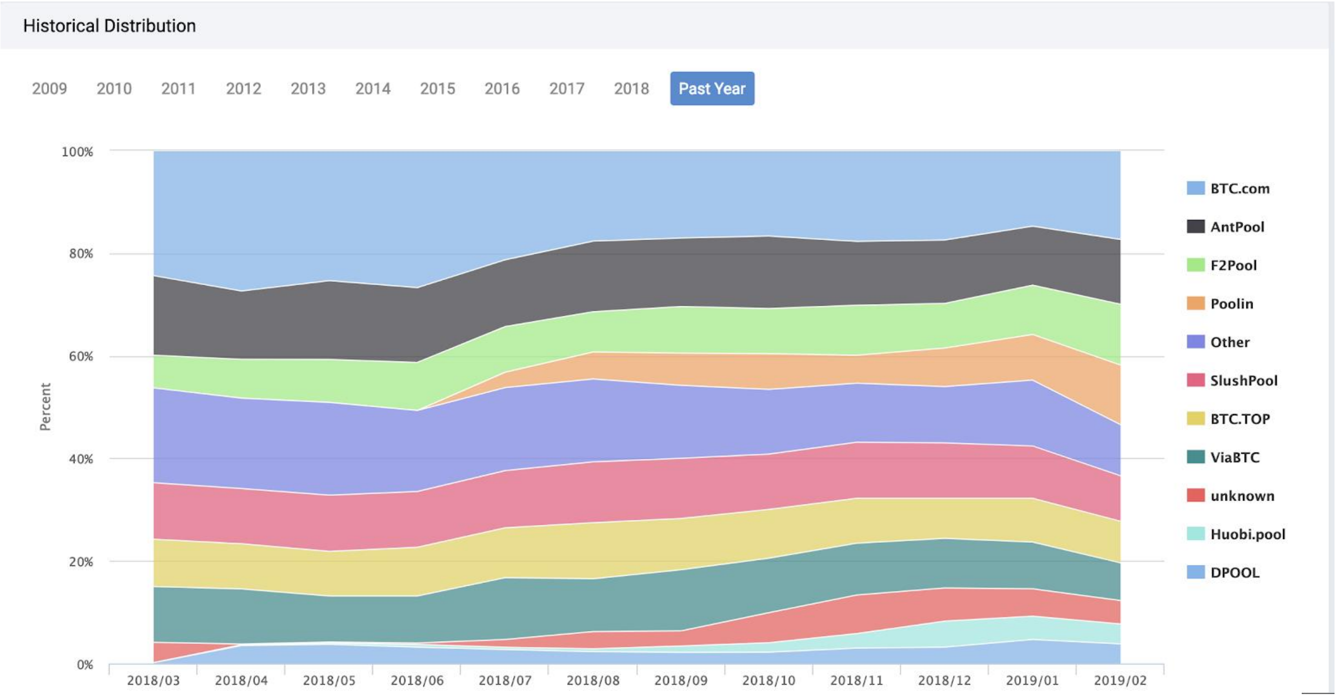


Figure 29: Historical districution of BTC mining pool

Mining Pool	March 19	March 20	March 21
BTC.com	28	29	28
Poolin	16	25	18
BTC.TOP	16	11	6
AntPool	15	17	26
F2Pool	21	12	14
SlushPool	11	19	6
ViaBTC	13	14	8
Bitfury	9	3	6
DPool	7	5	4

Table 7: Daily mined blocks by mining pool

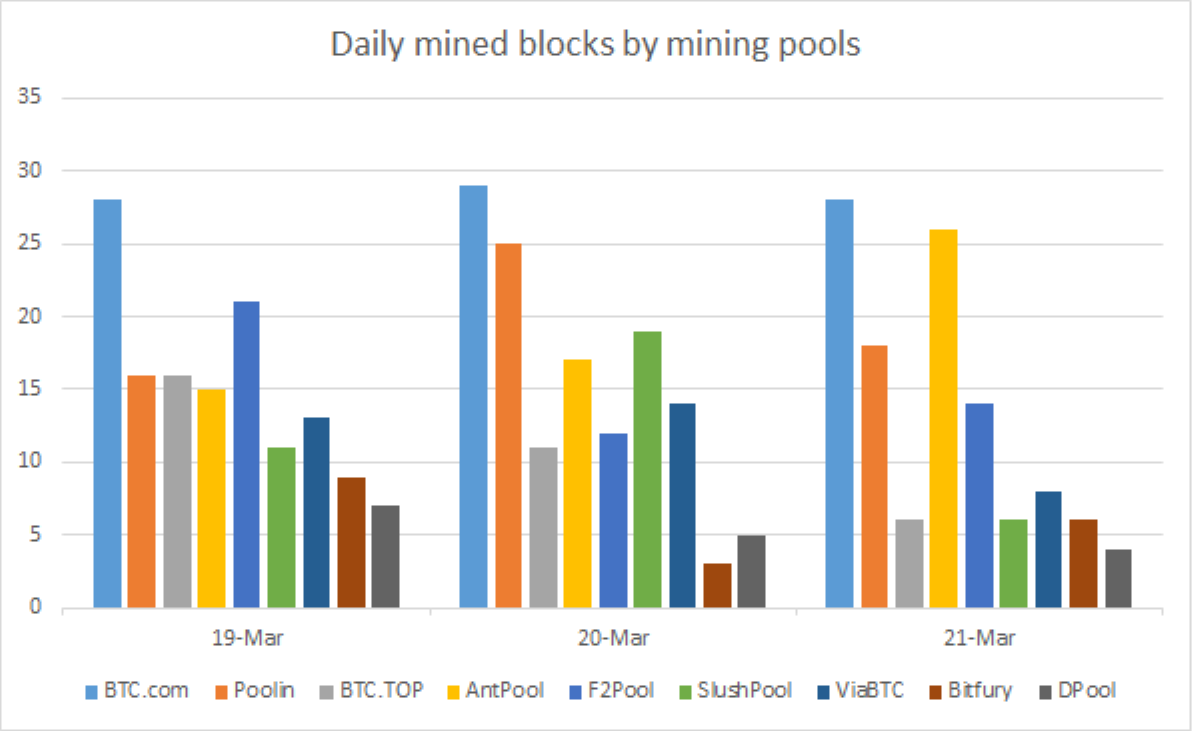
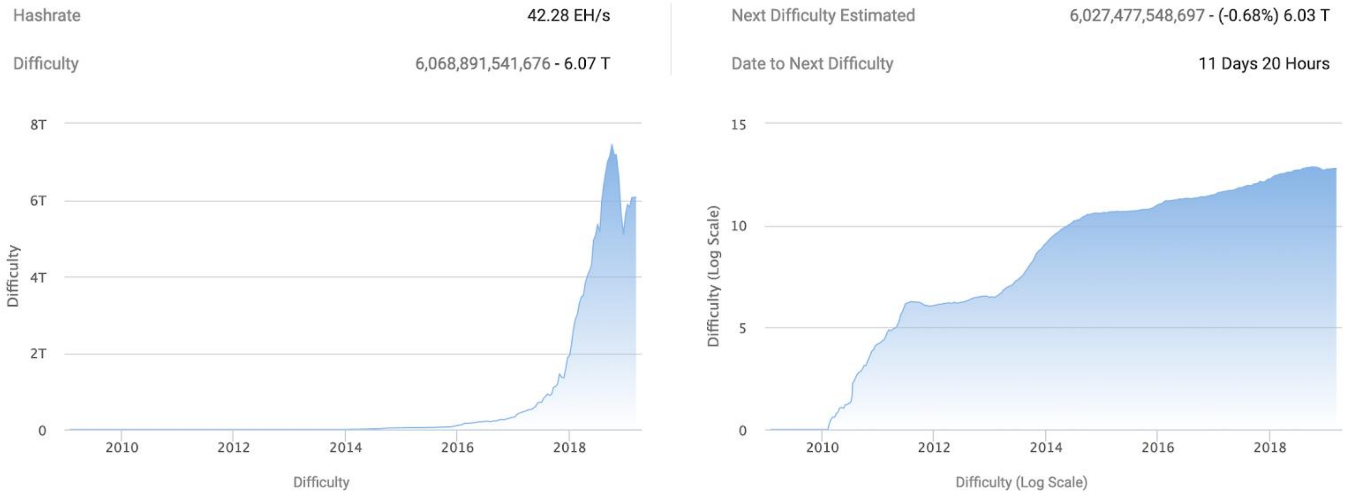


Figure 30: Daily mined blocks by mining pool

From Table 6 and Figure 30, it can be seen that BTC.com mining pool appears to mine the maximum number of blocks of the given day. Other mining pools like Poolin, Slushpool, AntPool are competing in very less difference of blocks mined per day.

As the number of miners mining the bitcoin increases over time, the mining difficulty also increase. The difficulty of Bitcoin mining is shown in Figure 31.



Hashrate 42.28 EH/s

Difficulty 6,068,891,541,676 - 6.07 T

Next Difficulty Estimated 6,027,477,548,697 - (-0.68%) 6.03 T

Date to Next Difficulty 11 Days 20 Hours

Figure 31: Difficulty of mining

From the graph in Figure 31, we can see that the difficulty of mining Bitcoin is getting bigger and bigger day by day. In the current scenario, the mining rate is around 43 EH/sec. The data shows that during 2016, the difficulty was very low, and several CPU and GPU mining hardware could also mine the Bitcoin. However, after 2016, the difficulty rate increased exponentially making very difficult of CPU and GPU hardware to mine the Bitcoin. As of today, ASIC miners are the only hardware that can mine Bitcoin.

Height	Difficulty	Change	Average Block	Average Hashrate
566,496	6,068,891,541,676 - 6.07 T	- 0.05 %	10 min 00 s	43.44 EH/s
564,480	6,071,846,049,920 - 6.07 T	0.0017%	09 min 59 s	43.45 EH/s
562,464	6,061,518,831,027 - 6.06 T	0.0425%	09 min 36 s	43.38 EH/s
560,448	5,814,661,935,891 - 5.81 T	- 1.18 %	10 min 08 s	41.59 EH/s
558,432	5,883,988,430,955 - 5.88 T	0.0472%	09 min 33 s	42.10 EH/s
556,416	5,618,595,848,853 - 5.62 T	0.1003%	09 min 06 s	40.16 EH/s
554,400	5,106,422,924,659 - 5.11 T	- 9.56 %	11 min 03 s	36.55 EH/s
552,384	5,646,403,851,534 - 5.65 T	- 15.13 %	11 min 47 s	40.40 EH/s
550,368	6,653,303,141,405 - 6.65 T	- 7.39 %	10 min 48 s	47.61 EH/s
548,352	7,184,404,942,701 - 7.18 T	0.0002%	10 min 00 s	51.37 EH/s

546,336	7,182,852,313,938 - 7.18 T	- 3.65 %	10 min 23 s	51.41 EH/s

Table 8: Change in difficulty of recent Bitcoin blocks per 2016 blocks

Table 7 shows the difficulty rate after every 2016 blocks. The difficulty keeps on changing after every calculation. The difficulty in the block of height 560,448 decreases by 1.18% than the previous blocks which changes the hash rate from 42.10 EH/S to 41.59 EH/S. Difficulty rate and hash rate are directly proportional to each other. Increase in difficulty rate, increases the computation power, resulting in an increase in the hash rate. Similarly, after another re-calculation of difficulty rate after 2016 blocks, the difficulty increased by 0.0425% which also increases the hash rate to 43.38 EH/S.

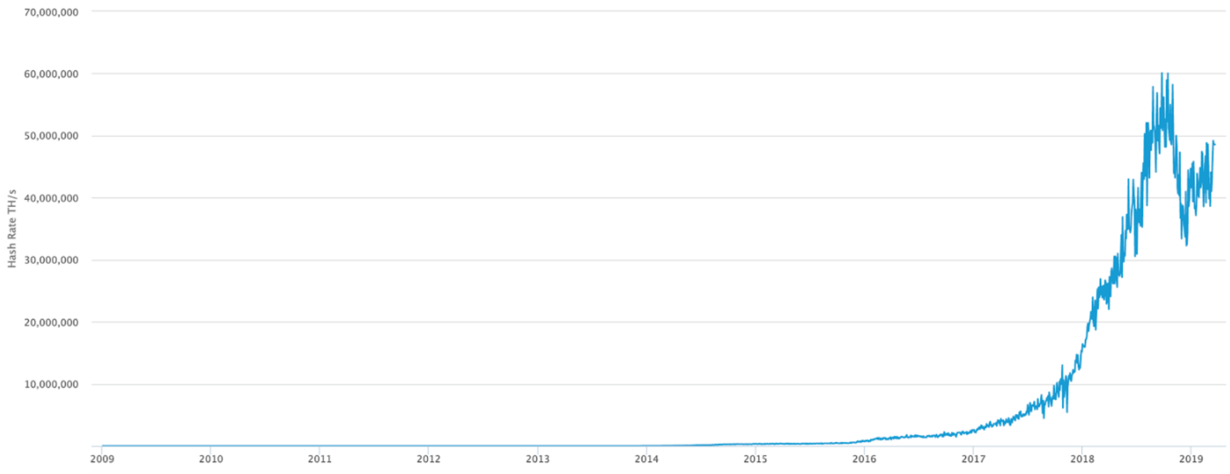


Figure 32: Bitcoin Hash rate

From the graph in Figure 32, we can see the hash rate of Bitcoin mining over time from 2009 AD to 2019 AD. Hash rate is directly proportional to the difficulty of Bitcoin mining. As difficulty increases the hash rate increases and vice-versa. Since the first, second and third generation mining was done by CPU, GPU and FPGA during 2009 to 2015, the hash rate was very low, therefore we can see the difficulty during 2009 AD 2015 AD is very low in Figure 32. After the introduction of ASIC miners, the computation power increased along with the total numbers of miners in the network. We can see how the difficulty of Bitcoin mining increased exponentially after 2017 AD.

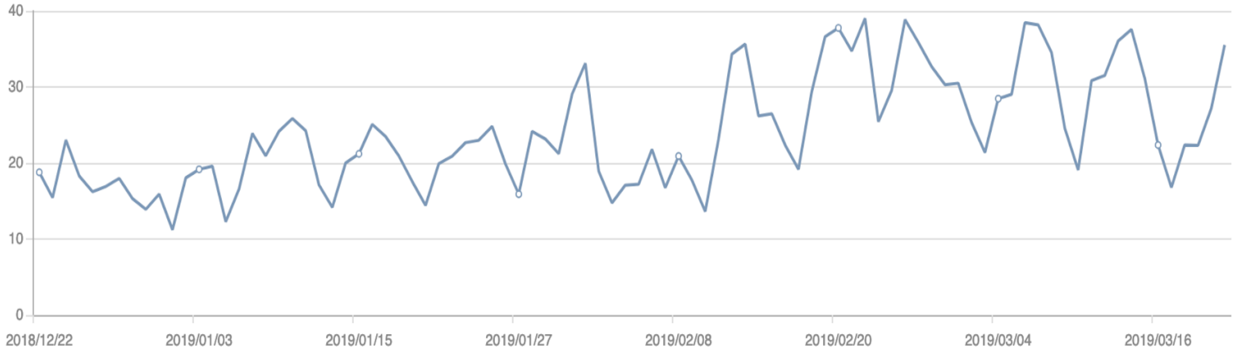


Figure 33: Transaction fee per day

Figure 33 shows the total amount of transaction fee spent for the confirmed Bitcoin blocks per day for the past three months. More blocks mined per day results in more transaction fee and vice versa. Over the period of time transactions fee is increasing, which signifies the increase in the rate of Bitcoin mining over time.

According to [37] the total numbers of Bitcoin in circulation as of now is around 17,606,075 BTC and total left to be mined are around 3,393,950 BTC. This is because there is a limited number of BTC which is around 21 Million BTC. The data shows that on average, 144 blocks per day are mined, and there are 12.5 bitcoins per block.

ie. 144 x 12.5 = 1,800

therefore, a total of 1800 BTC are mined per day.

Bitcoin price (USD):	$4,051.71
Market capitalization (USD):	$71,334,743,995.96
Total Bitcoins in circulation:	17,606,075
Total Bitcoins left to mine:	3,393,925
Percentage of total Bitcoins mined:	83.84%
Total Bitcoins to ever be produced:	21,000,000
Bitcoins generated per day:	1,800
Total blocks:	568,486
Blocks until mining reward is halved:	61,514
Total Bitcoins left to mine until next blockhalf:	768,925
Approximate block generation time:	10.00 minutes
Approximate blocks generated per day:	144
Difficulty:	6,068,891,541,677
Hash rate:	44.41 Exahashes/s

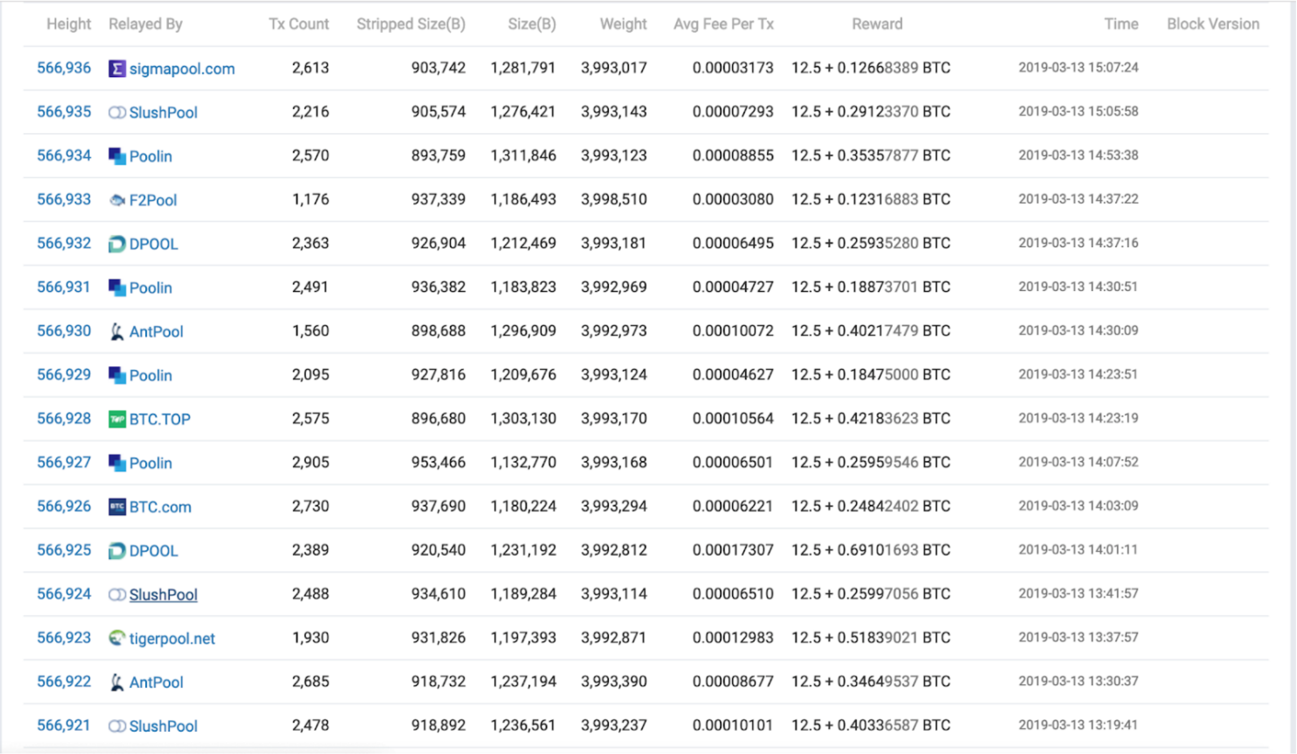
Table 9: Total mined and remaining Bitcoin

China is the undisputed world leader in Bitcoin mining, controlling more than 70% of the Bitcoin network's collective hash rate. India and Georgia are ranked as second and third counties for the network collective hash rate. The table below is the estimated mining hash power breakdown by country:

Country	Collective hash rate
China	71%
India	4%
Georgia	2%
Iceland	2%
Venezuela	2%
United States	1%

Table 10: Bitcoin Network’s mining pool collective hash rate

The Figure 34 shows the total blocks that are mined by respective pools.

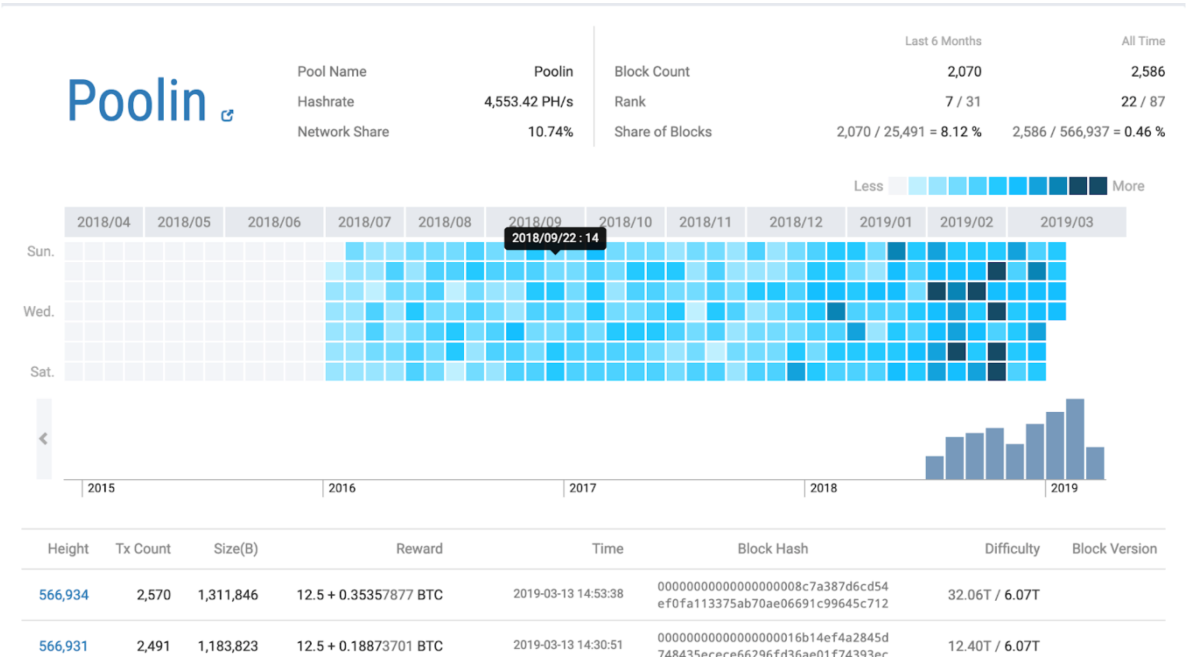


Height	Relayed By	Tx Count	Stripped Size(B)	Size(B)	Weight	Avg Fee Per Tx	Reward	Time	Block Version
566,936	sigmapool.com	2,613	903,742	1,281,791	3,993,017	0.00003173	12.5 + 0.12668389 BTC	2019-03-13 15:07:24	
566,935	SlushPool	2,216	905,574	1,276,421	3,993,143	0.00007293	12.5 + 0.29123370 BTC	2019-03-13 15:05:58	
566,934	Poolin	2,570	893,759	1,311,846	3,993,123	0.00008855	12.5 + 0.35357877 BTC	2019-03-13 14:53:38	
566,933	F2Pool	1,176	937,339	1,186,493	3,998,510	0.00003080	12.5 + 0.12316883 BTC	2019-03-13 14:37:22	
566,932	DPOOL	2,363	926,904	1,212,469	3,993,181	0.00006495	12.5 + 0.25935280 BTC	2019-03-13 14:37:16	
566,931	Poolin	2,491	936,382	1,183,823	3,992,969	0.00004727	12.5 + 0.18873701 BTC	2019-03-13 14:30:51	
566,930	AntPool	1,560	898,688	1,296,909	3,992,973	0.00010072	12.5 + 0.40217479 BTC	2019-03-13 14:30:09	
566,929	Poolin	2,095	927,816	1,209,676	3,993,124	0.00004627	12.5 + 0.18475000 BTC	2019-03-13 14:23:51	
566,928	BTC.TOP	2,575	896,680	1,303,130	3,993,170	0.00010564	12.5 + 0.42183623 BTC	2019-03-13 14:23:19	
566,927	Poolin	2,905	953,466	1,132,770	3,993,168	0.00006501	12.5 + 0.25959546 BTC	2019-03-13 14:07:52	
566,926	BTC.com	2,730	937,690	1,180,224	3,993,294	0.00006221	12.5 + 0.24842402 BTC	2019-03-13 14:03:09	
566,925	DPOOL	2,389	920,540	1,231,192	3,992,812	0.00017307	12.5 + 0.69101693 BTC	2019-03-13 14:01:11	
566,924	SlushPool	2,488	934,610	1,189,284	3,993,114	0.00006510	12.5 + 0.25997056 BTC	2019-03-13 13:41:57	
566,923	tigerpool.net	1,930	931,826	1,197,393	3,992,871	0.00012983	12.5 + 0.51839021 BTC	2019-03-13 13:37:57	
566,922	AntPool	2,685	918,732	1,237,194	3,993,390	0.00008677	12.5 + 0.34649537 BTC	2019-03-13 13:30:37	
566,921	SlushPool	2,478	918,892	1,236,561	3,993,237	0.00010101	12.5 + 0.40336587 BTC	2019-03-13 13:19:41	

Figure 34: Real-time mined Bitcoin blockchain by respective pools

From these data [36], we can analyze that there are several pools under competition to mine Bitcoin as fast as possible so that they can claim the reward. From this small data alone, we can see Poolin mining Pool has the highest number of mined Blocks (4 Blocks) followed by Slushpool (3 Blocks), Antpool (2 Blocks) and so on. If we see more detail on a single mined block, we can see the information like the total number of transactions each block has, amount of rewards the miners received, size and weight of the block and the time it was added on the blockchain. For example, if we analyze the block of height 566,936 we can see it is mined by the mining pool called Sigmapool. The block contains a total of 2,613 verified transactions. The miners who are involved in mining the block received an incentive of 12.5 BTC and the transaction fee of 0.1266 BTC.

As we see the statistics of a single mining pool, we can see that the Poolin mining pool is the newest mining pool out of this three mining pool. It has a hash rate of 4,553.42 PH/s and network share of around 10.74%. Similarly, the statistics for the other pools are shown in Figure 36 and 37.



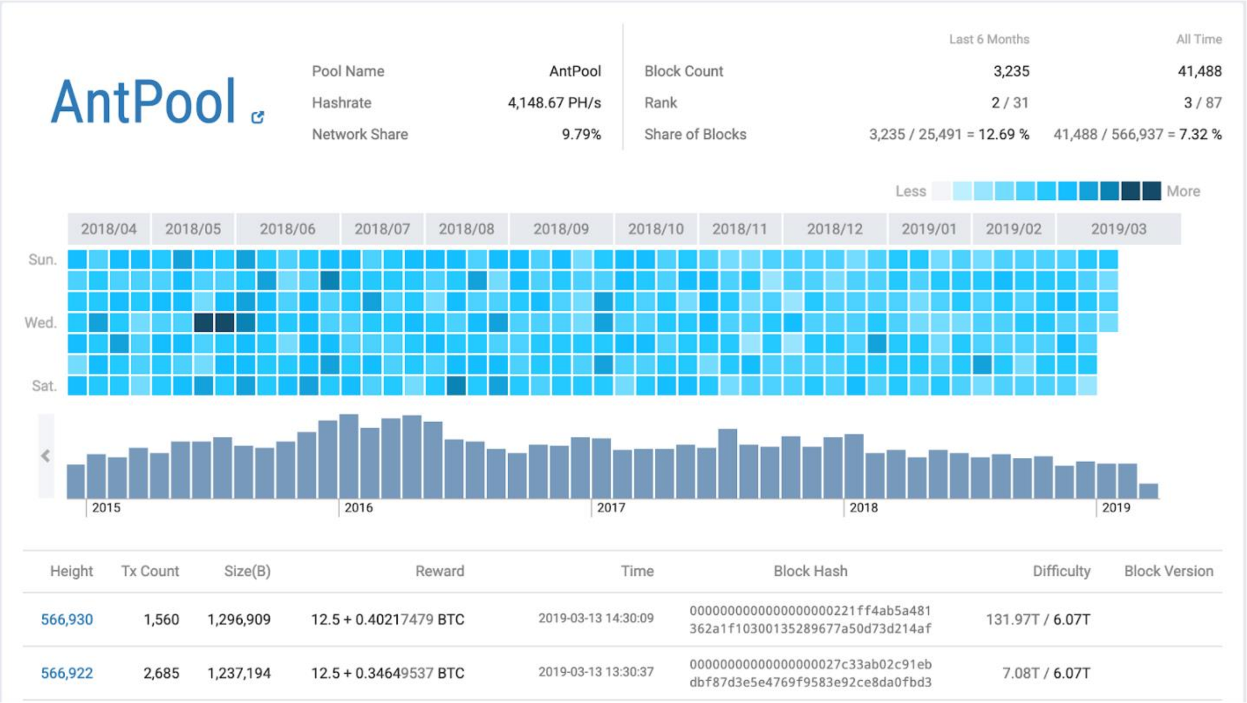
Poolin

Pool Name	Poolin
Hashrate	4,553.42 PH/s
Network Share	10.74%

	Last 6 Months	All Time
Block Count	2,070	2,586
Rank	7 / 31	22 / 87
Share of Blocks	2,070 / 25,491 = 8.12 %	2,586 / 566,937 = 0.46 %

Height	Tx Count	Size(B)	Reward	Time	Block Hash	Difficulty	Block Version
566,934	2,570	1,311,846	12.5 + 0.35357877 BTC	2019-03-13 14:53:38	0000000000000000008c7a387d6cd54 ef0fa113375ab70ae06691c99645c712	32.06T / 6.07T	
566,931	2,491	1,183,823	12.5 + 0.18873701 BTC	2019-03-13 14:30:51	00000000000000000016b14ef4a2845d 748435ecece66296fd36ae01f74393ec	12.40T / 6.07T	

Figure 35: Poolin mining pool

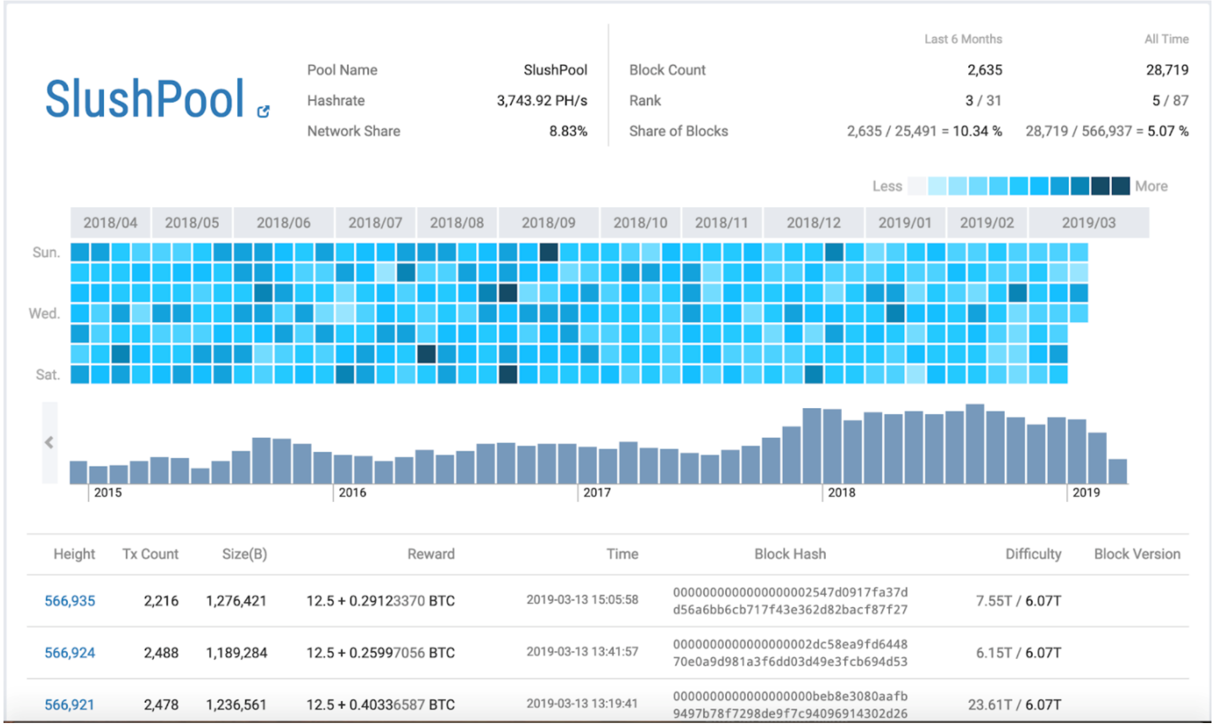


AntPool

				Last 6 Months	All Time
Pool Name	AntPool		Block Count	3,235	41,488
Hashrate	4,148.67 PH/s		Rank	2 / 31	3 / 87
Network Share	9.79%		Share of Blocks	3,235 / 25,491 = 12.69 %	41,488 / 566,937 = 7.32 %

Height	Tx Count	Size(B)	Reward	Time	Block Hash	Difficulty	Block Version
566,930	1,560	1,296,909	12.5 + 0.40217479 BTC	2019-03-13 14:30:09	0000000000000000000221ff4ab5a481 362a1f10300135289677a50d73d214af	131.97T / 6.07T	
566,922	2,685	1,237,194	12.5 + 0.34649537 BTC	2019-03-13 13:30:37	00000000000000000027c33ab02c91eb dbf87d3e5e4769f9583e92ce8da0fbd3	7.08T / 6.07T	

Figure 36: AntPool mining pool



SlushPool

				Last 6 Months	All Time
Pool Name	SlushPool		Block Count	2,635	28,719
Hashrate	3,743.92 PH/s		Rank	3 / 31	5 / 87
Network Share	8.83%		Share of Blocks	2,635 / 25,491 = 10.34 %	28,719 / 566,937 = 5.07 %

Height	Tx Count	Size(B)	Reward	Time	Block Hash	Difficulty	Block Version
566,935	2,216	1,276,421	12.5 + 0.29123370 BTC	2019-03-13 15:05:58	000000000000000000002547d0917fa37d d56a6bb6cb717f43e362d82bacf87f27	7.55T / 6.07T	
566,924	2,488	1,189,284	12.5 + 0.25997056 BTC	2019-03-13 13:41:57	000000000000000000002dc58ea9fd6448 70e0a9d981a3f6dd03d49e3fcb694d53	6.15T / 6.07T	
566,921	2,478	1,236,561	12.5 + 0.40336587 BTC	2019-03-13 13:19:41	0000000000000000000beb8e3080aafb 9497b78f7298de9f7c94096914302d26	23.61T / 6.07T	

Figure 37: SlushPool mining pool

The summary of these mining pools in terms of hash rate, network share, block count and rank are shown in Table 10.

Mining pool	Hash rate	Network share	Block count	Rank for 6 months	Overall rank
Poolin	4,533.42 PH/S	10.74%	2,586	1	22
AntPool	4,148.67 PH/S	9.79%	41,448	2	3
SlushPool	3,743.92 PH/S	8.83%	28,719	3	5
F2Pool	4,932.08 PH/S	10.72%	44,974	4	2
BTC.com	7,821.32 PH/S	17.02%	19,516	6	7
BTC.TOP	2,357.11 PH/S	5.13%	12,296	7	12

Table 11: Bitcoin Mining Pool status

Table 10 shows the mining pool ranks for the last 6 months and overall rank with the total number of blocks mined. As of today, Poolin mining pool is supposed to be the best mining pool although its network share and hashrate are lower than BTC.com mining pool. From this analysis, we can see that the hash rate is not always a necessary factor in mining Bitcoin, there comes a bit of luck also. However, the mining pool with better hardware is always mandatory to mine Bitcoin. The table shows the BTC.TOP with lowest hashrate and the rank for the last 6 months is also low. This shows that higher hashrate increase the chances of mining to a greater extent but not guarantees it.

Hash rate and hardware cost are not only factors that determine the mining profit and effectiveness of mining. The power consumption of each hardware and the electricity rate is also another determining factor of every miner and mining pool. There are different electricity rates in terms of power consumption by device per country. The cost to mine 1 Bitcoin based on the average Electricity rate per country is shown in Table 11 [38].

Country	Average Rate
Albania	3,894
Australia	9,913
Bangladesh	2,379
Belgium	13,482
Brazil	6,741
Canada	3,965
Chile	9,120
China	3,172
Denmark	14,275
Egypt	3,172
France	7,930
Germany	14,275
Greece	9,120
HongKong	7,930
Iceland	4,746
India	3,274
Iran	3,217
Japan	8,723
Kuwait	1,983
Luxembourg	7,693
Malaysia	5,147
Mexico	7,645
Myanmar	1,983
Nepal	3,569
Netherlands	9,449
Niue	17,566
Pakistan	7,137
Portugal	10,825
Russia	4,675
Singapore	5,936
South Korea	16,209
Spain	11,103
Surinam	2,956
Switzerland	7,494
Thailand	4,943
Trinidad and Tobago	1,190
Turkey	4,984
Ukraine	1,852
UAE	3,569
United Kingdom	8,402
United States	4,758
Uzbekistan	1,788
Venezuela	531
Zambia	3,569

Table 12: Cost to mine 1 BTC based on electricity rate per country

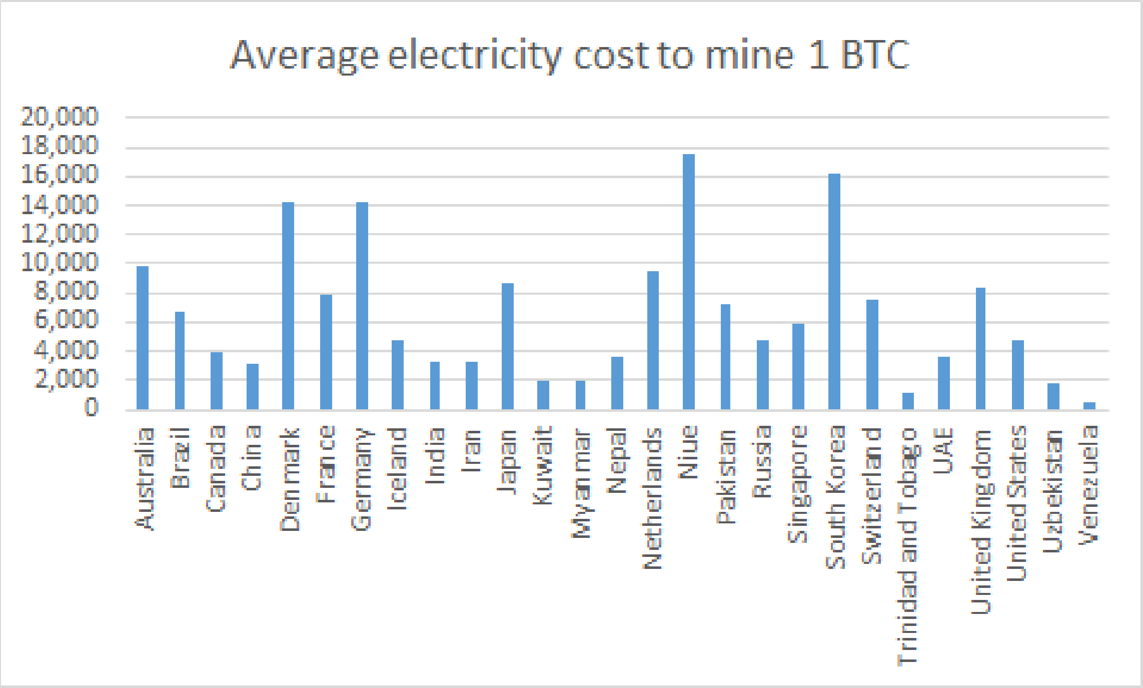


Figure 38: Average electricity cost to mine 1 BTC

From Table 11, we can see that on average, the countries in Asia have less electricity cost to mine 1 BTC compared to other continents. Europe Continent has extremely high electricity cost. It is a wrong decision if any miner or mining pool operates its Bitcoin mining farm on European countries especially those countries with higher electricity cost like Denmark, Germany, Netherlands, and Belgium, etc. Asian countries like China, India, and Nepal have less electricity cost to mine BTC. Venezuela has got the least average electricity cost to mine 1 BTC. This could be the potential place for Bitcoin miners to mine BTC and get much profit. Since the mining rigs produce a lot of heat during mining, miners often choose the cold place to mine bitcoins. The cold places having low average electricity cost would be the optimal place for miners to mine Bitcoin.

A simple economic model to calculate the number of Bitcoins particular hardware can mine a day is calculated as [21]. Here it is assumed that hardware works 24 hours per day.

$$N(t,H) = \frac{H\ X\ 86400}{D(t)x\ 2^{32}}\ R, \qquad \text{Equation 1}$$

where,

D(t) = Difficulty rate in day t,

R = Number of Bitcoins rewarded for each block,

H = Hash rate

The table 12 shows the hardware that are used for Bitcoin mining with their price.

Hardware	Price (USD)	Hash rate (TH/S)
Ebit E11++	2,398	44
Terminator T3	2,266	43
Antminer S15	1,475	28
Dragonmint T1	900	16
Obelisk SC1 Immersion	6,352	2.2
8 Nano Pro	11,600	76
MicroBT Whatsminer M10S	2,516	55
Bitfily Snow Panther A1	2,200	49
Bitfury B8	2,500	49

Table 13: Price of Bitcoin mining hardware

8 Nano Pro ASIC hardware has the maximum hash rate of 76 TH/S among all other available hardware in the market today. The price for this hardware is really expensive. Several big mining pool use this hardware for mining purpose. Other hardware like Bitfur B8, MicroBT Whatsminer M10s, Ebit E11+, and Terminator T3 are commonly used hardware by miners these days.

Cost of Mining: The following algorithm can calculate the cost of mining.

```
if
    mining reward  > mining cost
    then miner goes on profit
else
    miner goes on the loss
where,
    mining reward = block reward and transaction fees
    mining cost = hardware cost and operating costs (electricity, cooling the hardware, etc.)
```

The analysis of Bitcoin mining in this chapter shows different factors included in Bitcoin mining. Some of the important factors that should be taken into consideration are:

- Type of hardware chosen for mining Bitcoin
- Bitcoin reward per block
- Cost of electricity
- The budget for the hardware expenses
- Type of mining: solo or pool mining
- If joining on pool mining, we should look into network share, hash rate of a mining pool, mining reward from mining pool and so on.

Mining Bitcoin is not an easy task since miners mining the Bitcoin are increasing every day resulting in an increase in hash rate and difficulty of the network. The approach of mining a Bitcoin using a High-end Desktop PC, FPGAs and GPU would be the worst idea in current scenario no matter how many of those devices we connect together and mine Bitcoin. However, they were the best mining hardware back in 2010-

2013 AD. Along with the increase in time and miners mining the Bitcoin, the difficulty of the network also increased. In today’s date, ASIC hardware should be used for mining Bitcoin. From the data collected in Table 3, on average, a single ASIC mining hardware provides a hash rate of around 30 TH/S with a high of 44 TH/S. This hash rate is low since the average hash rate as of now is around 43 EH/S. Buying ten or more of these hardware could be one option to mine Bitcoin, but the cost goes really high. From Equation 1 we can calculate the number of Bitcoins particular hardware can mine a day. Taking a single ASIC hardware and applying equation 1, we get that the hardware can mine 0.00018 BTC per day if it runs for 24 hours. At present rate 0.0001844 BTC = 76 USD per day. From the algorithm of the cost of mining, the price of 76 USD per day is not even sufficient to pay for the electricity cost. Consumers with low capital to invest in Bitcoin mining has another platform to mine called as mining pool.

The mining pool has a hash rate of around 6.5 EH/S on average which is ideal for Bitcoin mining since various pools compete with each other on the same mining hash rate. The one with better hardware solves the proof of work for a given block and claim the reward. Sometimes, a better hash rate for any hardware results in excessive power consumption. Being as a starter miner, joining the mining pool is considered to be a good idea. They can join a mining pool with a single hardware and start mining. The mining pool aggregates the computation of all the hardware in a network collectively to mine a single block. Once the pool manages to win the competition by finding a nonce value, the reward gets split among the miners on the particular pool. Since the reward is split, the reward will be very less compared to the solo mining reward. However, the mining pool is risk-free since the initial investment is very low. Joining the mining pool which has mined the highest number of blocks in recent months will be the ideal approach. From Table 11 joining mining pools like Poolin, Antpool, BTC.com, Slushpool, and others on the higher rank for recent months will be good. However, this changes as time increases since every mining pool is competing with each other.

Chapter 5

CONCLUSION AND FUTURE WORK

In this thesis, we studied the analysis of Bitcoin Mining in various aspects. Bitcoin is being used as an alternative to fiat currencies. Various countries like Japan, USA, Australia, China, etc. have started using Bitcoin as the payment method [1]. There are lots of restaurants, shops, and stores that are accepting Bitcoin as an alternative to other currencies. Since Bitcoin is decentralized and works on the concept of the blockchain, all the transactions are transparent and fair. Mining Bitcoin is becoming harder day by day with an increase in difficulty rate and the competition between the miners with the best hardware available in the market. A few years back mining a Bitcoin was much easier compared to nowadays. Mining a Bitcoin requires a lot of computation and good hardware that can deliver good hash rate with low energy consumption.

Miners must be careful about choosing hardware before starting to mine Bitcoin since the cost of hardware is very high and the other added cost during mining is electricity cost and repair cost. Although CPU, GPU, and FPGA mining hardware were used to mine Bitcoins before, however now investing on them as mining hardware is a bad idea since they cannot generate the computing power required to mine Bitcoin today. A single ASIC mining hardware also cannot mine the Bitcoin effectively since there are hundreds of mining pools competing with each other to mine the Bitcoin. A single user cannot compete with a mining pool which has lots of hardware resources. Several mining pools are shutting down in China due to a loss in their business of mining. Choosing the right location is another critical step for miners or mining pool since the cost of electricity to run the hardware is also a determining factor. Mining a Bitcoin consumes a lot of power. Countries like Venezuela, Myanmar. Kuwait, Ukraine, Uzbekistan, India, etc. would be the best solution for miners and mining pool.

Due to the limitation of hardware resources, we could not mine the Bitcoin on our own. The future work for this thesis would be either buying some good hardware by securing funding or collaborating with mining pools to use their hardware for a research purpose.

REFERENCES

[1] Money.CNN, "Money.CNN," [Online]. Available: https://money.cnn.com/infographic/technology/what-is-bitcoin/index.html. [Accessed 21 03 2019].

[2] S. Nakamoto, "Bitcoin: A peer-to-Peer Electronic Cash System," 2009.

[3] Investopedia, "Investopedia.com," [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. [Accessed 21 Feb 2019].

[4] BitcoinWiki. [Online]. Available: https://en.bitcoinwiki.org/wiki/Bitcoin_history. [Accessed 17 2 2019].

[5] Wikipedia, "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/History_of_bitcoin. [Accessed 21 Feb 2019].

[6] [Online]. Available: https://coinmarketcap.com/currencies/bitcoin/. [Accessed 19 2 2019].

[7] Bitcoin.it, "Bitcoin.it," [Online]. Available: https://en.bitcoin.it/wiki/Address. [Accessed 2 03 2019].

[8] S. S. T. M. C. Z. L. a. K.-K. R. C. Tejaswi Volety, "Cracking Bitcoin wallets: I want what you have in the wallets," *Future Generation Computer Systems,* vol. 91, pp. 136-143, 2019.

[9] MasterinBitcoin, "MateringBitcoin," [Online]. Available: https://masteringbitcoin.neocities.org/. [Accessed 11 02 2019].

[10] S. K. E. a. C. L. Mauro Conti, "A Survey on Security and Privacy Issues of Bitcoin," 2017.

[11] MinerHome, "Minerhome," [Online]. Available: http://www.minerhome.com/cryptocurrency-for-dummies-bitcoin-and-beyond/. [Accessed 23 02 2019].

[12] Wikipedia, "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/SHA-2. [Accessed 14 03 2019].

[13] R. P. Naik, "Optimising the SHA256 Hashing Algorithm for Faster and More Efficient Bitcoin Mining," 2013.

[14] blockgeeks, "blockgeeks.com," [Online]. Available: https://blockgeeks.com/guides/blockchain-in-healthcare/. [Accessed 21 02 2019].

[15] Mappfia, "Mappfia.com," [Online]. Available: https://www.mappfia.com/blog/blockchain-work. [Accessed 03 03 2019].

[16] J. B. E. F. A. M. S. G. Arvind Narayanan, "Merkle Tree," in *Bitcoin and Cryptofurrency Technologies*, Princeton University Press, 2016, pp. 34 - 49.

[17] J. B. E. F. Arvind Narayanan, "CPU mining," in *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016, pp. 136-142.

[18] 99Bitcoins, "99bitcoins.com," [Online]. Available: https://99bitcoins.com/bitcoin-mining/. [Accessed 08 03 2019].

[19] H. R. MatthewVilim, "Approximate Bitcoin Mining," in *Proceedings of the 53rd Annual Design Automation Conference*, 2016.

[20] J. B. E. F. Arvind Narayanan, Bitcoin and Cryptocurrency Technologies, Princeton Publications.

[21] L. W. a. Y. Liu, "Exploring Miner Evloution in Bitcoin Network," 2015.

[22] D. L. Chaum, "Untraceable Electronic Mail, Return Address, and Digital Pesudonyms," 1983.

[23] C. D. a. M. Naor, "Pricing via Processing or Combatting Junk Mail," 1992.

[24] U. W. Chohan, "The Double spending Problem and Cryptocurrencies".

[25] S. K. a. S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," 2012.

[26] A. Poelstra, "On Stake and Consensus," 2014.

[27] M. B. Taylor, "Bitcoin and the Age of Bespoken Silicon," in *International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES)*, 2013.

[28] A. M. Antonopoulos, Mastering Bitcoin, O'Reilly.

[29] K. J. O. a. D. Malone, " Bitcoin Mining and its Energy Footprint," in *CIICT 2014*, Limerick, 2014.

[30] C. Ho, "Adaption of All Programmable SoC to Hardware Bitcoin Miners and Mining Servers," 2013.

[31] A. O. B. L. a. M. L. G.Bissias, "Sybil-resistant mixing dor Bitcoin", in proceedings of the 13th workshop on Privcay on the Electronic Society," pp. 149-158, 2014.

[32] E. A. Ghassan O. Karame, "Two Bitcoins at the Price of One? Double-Spending Attacks on," in *In Proc. of Conference on Computer and Communication Security*, 2012.

[33] C. A. a. M. R. I. Bentov, "Proof of Activity Extending Bitcoin's proof of work via proof of stake," pp. 34-37, 2014.

[34] Coinatmradar, "coinatmradar," [Online]. Available: https://coinatmradar.com/charts/growth/. [Accessed 04 03 2019].

[35] Blockchain, "Blockchain.com," [Online]. Available: https://www.blockchain.com.

[36] BTC.COM, "btc.com," [Online]. Available: https://btc.com/. [Accessed 09 03 2019].

[37] Buybitcoinworldwide, "Buybitcoinworldwide," [Online]. Available: https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/. [Accessed 27 02 2019].

[38] Marketwatch, "Marketwatch.com," [Online]. Available: https://www.marketwatch.com/story/heres-how-much-it-costs-to-mine-a-single-bitcoin-in-your-country-2018-03-06. [Accessed 12 03 2019].

[39] I. E. a. E. G. Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," 2013.

[40] p2pool, "p2pool Decentralized mining pool," [Online]. Available: http://p2pool.org/.

CURRICULUM VITAE

Graduate College
University of Nevada, Las Vegas

Suman Ghimire

ghimis2@unlv.nevada.edu / mail.sumangh@gmail.com

Degrees:

Bachelor of Electronics and Communications Engineering 2016

Tribhuvan University, Nepal

Thesis Title:

Analysis of Bitcoin Cryptocurrency and its Mining Techniques

Thesis Examination Committee:

Chairperson, Dr. Henry Selvaraj, Ph.D.

Committee Member, Dr. Shahram Latifi, Ph.D.

Committee Member, Dr. Mei Yang, Ph.D.

Graduate Faculty Representative, Dr. Laxmi Gewali, Ph.D.