

A Survey on Bitcoin Cryptocurrency and its Mining

Suman Ghimire
College of Engineering
University of Nevada, Las Vegas
Email: ghimis2@unlv.nevada.edu

Dr. Henry Selvaraj
Professor
College of Engineering
University of Nevada, Las Vegas
Email: henry.selvaraj@unlv.edu

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. The importance of digital cryptocurrency and the concept of blockchain have been explored by several developers and organizations. It is assumed to be one of the secure and easy payment methods that can be used in the coming days. In this paper, we survey various topics under Bitcoin such as blocks, blockchains, mining process and proof of work(PoW).

Keywords: Bitcoin, Cryptocurrency, Blockchain, Proof of work, mining, SHA-256

I. INTRODUCTION

Bitcoin is a decentralized, distributed, peer to peer virtual cryptocurrency created by an unknown individual under the pseudonym Satoshi Nakamoto in 2009[1]. It can be taken as a form of money that exists only online and termed as virtual currency. Back in 2009, it was only an idea. Bitcoins are transferred from person to person directly via the internet without the involvement of a centralized third party like the banking system. In particular, an owner has full control over Bitcoin, and could spend them anytime and anywhere. Elimination of the third party by this system also eliminates the unnecessary fees required to be paid to the third party. Bitcoin works on the concept of the Blockchain. Blockchain is the chain of blocks containing all the transaction with the hash file of that block and also the hash of the previous block. Since Bitcoin does not have any centralized server for controlling the flow of currency, it is created by the process called mining[1]. Bitcoin network is secured by individuals called 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. From Fig.1, as shown below, we can see how Bitcoin is different from the normal banking system.



Currency	₿	\$
User Facing		
Underlying System	Bitcoin Protocol	Banking System

Fig. 1. Bitcoin system vs current system.

Since the introduction of Bitcoin in 2009, it has attracted a lot of attention from several sectors mainly targeting the academic sector and industry. With a market capitalization of 132 billion and more than 187,000 aggregate number of confirmed transactions per day (July 2018), Bitcoin is the most successful cryptocurrency to date. Bitcoin started its operation on the exchange market on 17 Mar 2010 under the now-defunct BitcoinMarket.com exchange. The first real-world transaction of Bitcoin was done by Laszlo Hanyecz by buying two pizzas for 10,000 BTC (equivalent to \$0.008 during that time)[2]. The growth of Bitcoin capital in terms of money is shown in the graph below[5].



Fig. 2. Bitcoin market capital growth chart.

From the market capital growth chart above, we can see that Bitcoin has undergone rapid growth to become a significant cryptocurrency. Starting from the value of \$0.008 per 1 BTC, it increased its market value to the maximum of almost \$19,500 per 1 BTC on December 2017[5]. Since the market of cryptocurrency is highly fluctuating, the price never maintains the same every time. It keeps on increasing and decreasing depending on the shareholders and the stock market.

Bitcoin has been growing in various business platforms as an alternative to fiat currencies these days. Several countries including USA, Japan and Canada started recognizing Bitcoin as a method of payment[14]. Many restaurants in New York also started using Bitcoin as an alternate source for currency. Every Bitcoin user has an address which acts as an account number in the bank system. Just as we use account number to transfer a certain amount to another account, likewise, we use

The backbone underlying Bitcoin is not a bank that verifies the transaction. Instead, there are miners who are solving complex mathematics puzzle to verify the transaction.

A. Blocks and Blockchain

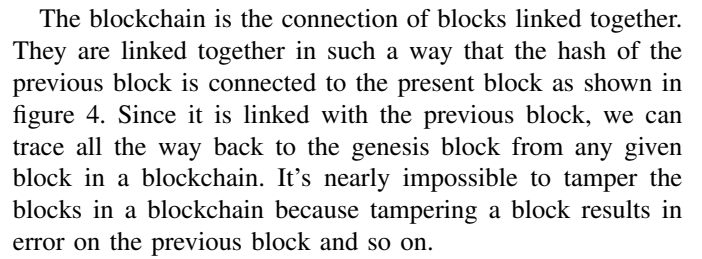


Fig. 5. Chain of blocks in blockchain

B. Mining

Bitcoin network is secured by individuals called miners. Any machine in the Bitcoin network can act as a miner. Users have used several types of hardware over time to mine blocks of Bitcoin. CPU mining, GPU mining, FPGA mining and ASIC mining are popularly used hardware for Bitcoin mining. All the hardware mining has to deal with low profit, excess heat and high electricity cost. Cloud mining is another solution to these problems since it does not have to deal with excess heat or high electricity cost. But it has few other limitations. The miner uses its processing power to solve the puzzle and broadcast on the network. Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger of past transactions or blockchain[6]. A transaction is only considered to be valid when it is signed by the sender. Mining is done by the miners who are watching Bitcoin transaction continuously and trying to verify it. As there are more miners added to the network, the challenge gets actually harder and harder, in such a way that in the average of 10 minutes, a new block of a transaction is added to the blockchain in the network. A block is only considered valid when it has proof of work. The miner who mines the block gets a reward. The new Bitcoins are obtained by miners as a reward and also the transaction fee obtained from all the transactions included in the block. This motivates the miners to continuously compete in the race for finding a valid block. The general process of how Bitcoin blockchain works are illustrated in figure 6.

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

Fig. 4. Structure of a header in a block

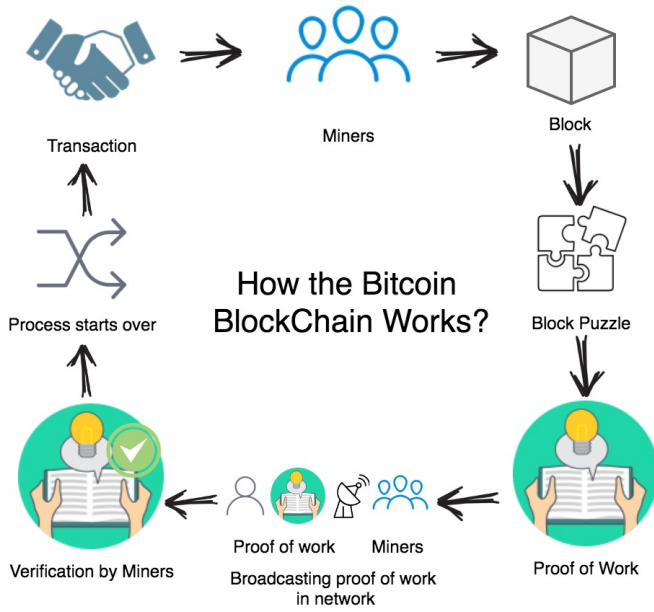


Fig. 6. How the Bitcoin Blockchain Works.

The steps to run the network[1] are as follows:

- New transactions are broadcasted to all nodes.
- Verify if the transactions are valid.
- Each node bundles new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
- 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.

C. Proof of Work (PoW)

The Proof of work consists of a complex cryptographic math puzzle. It scans for a value which is called as *nonce* which when hashed with SHA-256, the resulting hash begins with the number of zeros. A nonce is short for "number only used once.". The average work required is exponential to the number of zeros in the correct hash. This shows that the Proof of Work contains a high level of computational cost on the verification process. The computational process depends upon the computing power of miners. The miners do not mine individual transactions, but they collect a bunch of transactions from a block and they mine that block by calculating the hash of that block with a varying nonce. The miner does this until the resultant hash becomes equal or lower to a given target value. The target is a 256-bit number that all miners share. For Bitcoin hashing, SHA-256 hash function is used[3]. The ultimate solution is to find the hash value lower or equal to the nonce, so unless the cryptographic

hash function finds the required hash value, we need to try different nonces and verify it. 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. Nonce value will start from 0 and increased continuously to create a valid hash. The target value is recalculated every 2016 blocks (approximately two weeks). The mining algorithm[17] used for the mining process is shown below.

Algorithm 1: Mining process

```

1  $nonce \leftarrow 0$ 
2 while  $nonce < 2^{32}$  do
3    $threshold \leftarrow ((2^{16} - 1) \ll 208) / D(t)$ 
4    $digest \leftarrow SHA - 256(SHA - 256(header))$ 
5   if  $digest < threshold$  then
6     return nonce
7   end
8   else
9      $nonce \leftarrow nonce + 1$ 
10  end
11 end

```

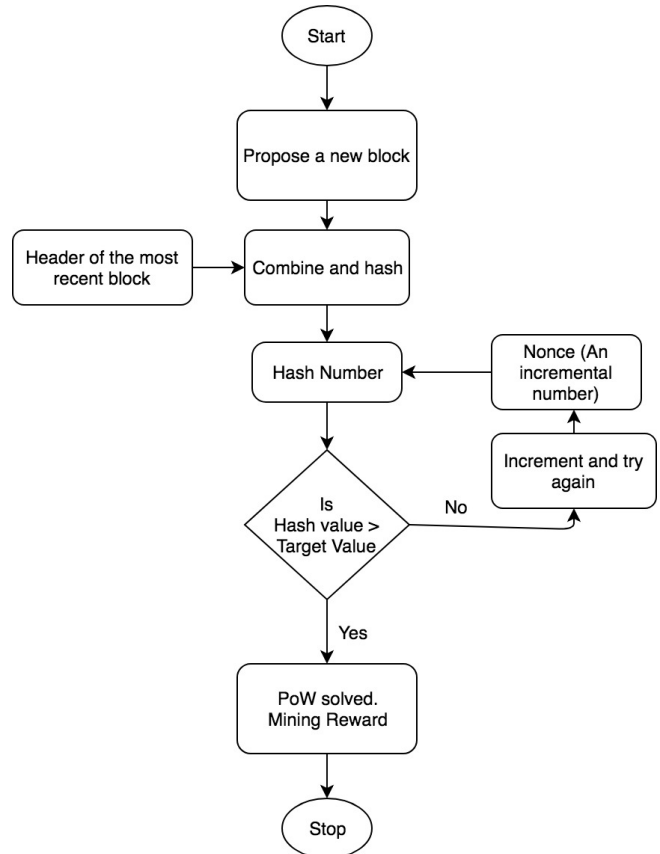


Fig. 7. Proof of Work Flowchart

Once the miner calculates the correct hash value for the given block, the miner immediately broadcast the block to the network with the correct hash value for the given block and

nonce. While doing so, it also adds the block to its private blockchain. The rest of the miner receives the broadcasted block and quickly verify for its authenticity by comparing the hash value given in the received block with the target value. When the majority of the miners considers the block valid, it is added to the blockchain. The miner who solved the first Proof of Work and added the block to the blockchain will be rewarded with Bitcoin. The reward varies with the number of Bitcoins mined. Since there is limited number of Bitcoins, the rewards go decreasing by half after every 210,000 blocks are mined or every after around 4 years. As of August 2018, the successful miners are rewarded by 12.5 Bitcoins. At the beginning of Bitcoin mining, the miners were rewarded with 50 BCTs. 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]. From figure 8 and 9, we can see the decrease in Bitcoin reward after every 210,000 blocks or approximately 4 years.

This is equal to 21 Million Bitcoins. It is really a big number but its likely to be less if we see the demand of Bitcoin and the miners urge to get this cryptocurrency.

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

Fig. 8. Bitcoin Rewards

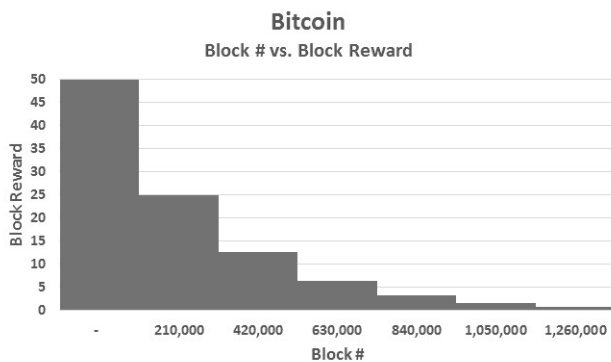


Fig. 9. Bitcoin Rewards

Since this reward decreases geometrically over time, it means that there will never be more than 21,000,000 Bitcoins in existence.

$$210,000(50 + 25 + 12.5 + 6.25 + 3.125 + \dots) \approx 21,000,000$$

III. RELATED WORK

The ultimate goal of a Bitcoin miner is to mine Bitcoin as fast as possible so that the miner can add the mined block on the blockchain and claim the reward. The mining process involves using dedicated hardware (e.g. CPUs, GPUs, ASICs, FPGAs) that use processing power, as well as software applications to manage these rigs. Better the hardware, better hash rate and so the higher chance of mining faster. Hash rate is the measure of miners computation power. Bitcoin mining software is used to communicate between the hardware that we use and the Bitcoin blockchain. Depending on the hardware, different types of Bitcoin mining software are used such as CGMiner, BTCMiner, EasyMiner and so on[15]. The software is available for Windows, Mac, and GNU/Linux. Much of this software is free and open source software that we can download and setup. These mining software have several tasks at hand. Depending on the user, the software has to connect either to a blockchain or the pool. Next, depending upon the mining software that is used, it chooses an algorithm. There are miners who mine using a particular algorithm and those which can dynamically switch between algorithms, such as NiceHash. Besides mining software, trading software and wallet software is also needed. The trading software is used to see the real-time price of Bitcoin. The wallet software is needed to store the Bitcoin safe and secure on our personal online wallet.

We can see the comparison of Bitcoin mining using different hardwares[9] in Fig.10.

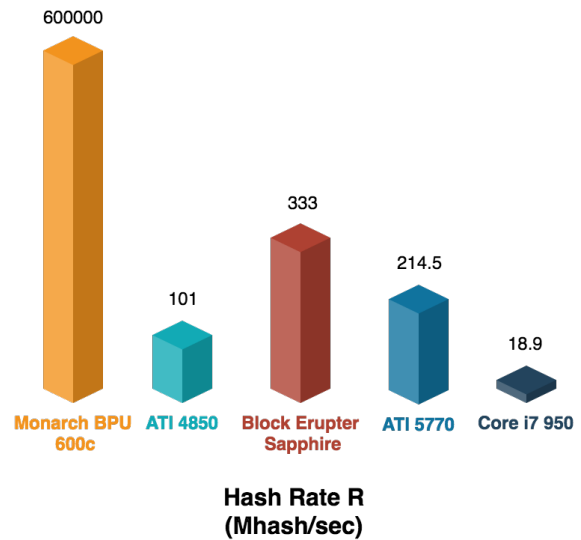


Fig. 10. Hardware mining rate comparison

We need to be efficient in terms of hardware and also cost. The key terms used in these comparisons are power and hash rate. Power is the first derivative of energy with respect to time, measured in energy/time (a watt, for example, is joules per second). Hash rate is the number of calculations (hashes) a machine can perform per unit of time. The relevant measure is Megahashes per second (Mhash/s). Higher the hash rate given

by the hardware, higher the power use and the cost. Fig.11, is the comparison of hardware in terms of power use.

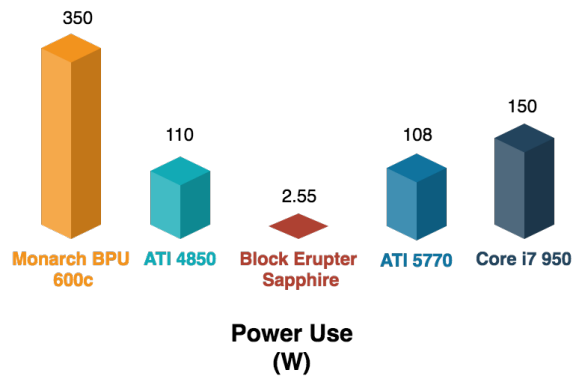


Fig. 11. Hardware power use comparison

We can see the comparison of hardware in terms of hash rate, power use, efficiency and cost[10] in Fig.12. It is not necessary that higher the cost, better the result. We need to see several factors. From the table below we can analyze that ATI 5770 has a good hash rate in terms of power consumption and cost. But Monarch BPU 600 C has got maximum hash rate also with higher power use and higher cost. We need to be careful on whether this investment is worth for generating Bitcoin without being on a loss.

Name	Type	Hash Rate R (Mhash/s)	Power Use P (W)	Energy Efficiency \mathcal{E} (Mhash/J)	Cost (\\$)
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

Fig. 12. Hardware comparison in terms of various factors

The mining difficulty of Bitcoin over the years is shown in the Fig.13 below[16]. We can see that over the years the difficulty of mining is increasing.

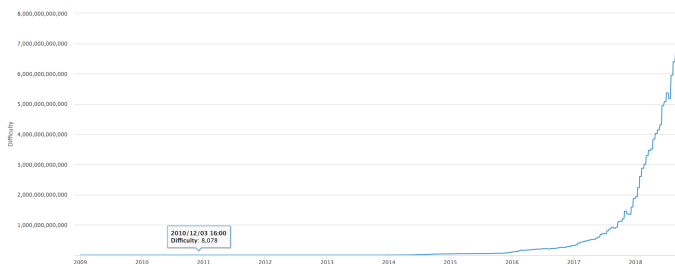


Fig. 13. Mining difficulty of Bitcoin over time

IV. CONCLUSION

Bitcoin has already evinced a popular digital cryptocurrency on the market. It uses the concept of the blockchain, which is

assumed to be the best invention of this century. The number of cryptocurrencies available over the internet as of 19 August 2018 is over 1600 and growing[13]. By market capitalism, Bitcoin is the largest blockchain network followed by other cryptocurrencies such as Ethereum, Ripple and Bitcoin Cash[13]. Since Bitcoin is accepted in several countries, its market is expected to grow at a high rate. Bitcoin mining is a competitive market, and so the resources expended line up with the opportunities to earn revenues. Over the years mining difficulty is increasing and the number of Bitcoins that are left to be mined is decreasing. Using improvised algorithm and better hardware, miners can maximize the chance of mining Bitcoin faster.

REFERENCES

- [1] Satoshi Nakamoto " *Bitcoin: A Peer-to-Peer Electronic Cash System* ". March 2009
- [2] Wikipedia " https://en.wikipedia.org/wiki/History_of_bitcoin ". Accessed, 25 Jul. 2018
- [3] D.E. III and T.Hansen, " *US Secure Hash Algorithms(SHA and SHA-based HMAC and HKDF)* ", Available: " <http://www.ietf.org/rfc/rfc6234.txt> ", 2011
- [4] K. Kaskaloglu " *Near zero bitcoin transaction fees cannot last forever* ". 2014, pp. 91-99
- [5] Coinmarketcap " <https://coinmarketcap.com/currencies/bitcoin/> ". Accessed. July 22, 2018
- [6] Bitcoinmining " <https://www.bitcoinmining.com/> ". Accessed. July 27, 2018
- [7] Iddo Bentov, Charles Lee, and Alex Mizrahi. " *Proof of activity: Extending bitcoins proof of work via proof of stake* ".
- [8] Usman W. Chohan. " *The double-spending problem and cryptocurrencies* ". December 19, 2017
- [9] bitcoin.it. Mining hardware comparison " https://en.bitcoin.it/wiki/Mining_hardware_comparison ". Accessed. July 28, 2018
- [10] Karl J. O'Dwyer and David Malone " *Bitcoin Mining and its Energy Footprint* ". CICT 2014, Limerick, June 26-27
- [11] Mauro Conti, Sandeep Kumar E, Chhagan Lal, Sushmita Ruj " *A Survey on Security and Privacy Issues of Bitcoin* ". Dec 2017
- [12] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, Edward W. Felten " *Sok: Research perspectives and challenges for bitcoin and*

cryptocurrencies. 2015 ". May 2015

- [13] All Cryptocurrencies — Coinlore "<https://www.coinlore.com>" . Accessed August 19, 2018.
- [14] Legality of bitcoin by country or territory "https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory". Accessed August 16, 2018
- [15] Bitcoin Mining Software "<https://www.bitcoinmining.com/bitcoin-mining-software/>". Accessed August 16, 2018
- [16] Blockchain Charts "<https://www.blockchain.com/charts>". Accessed August 19, 2018
- [17] Matthew Vilim, Henry Duwe, Rakesh Kumar "*Approximate Bitcoin Mining*". Proceedings of the 53rd Annual Design Automation Conference Article No. 97, June 05-09, 2016