On the Proof-of-Work Puzzle Hardness in Bitcoin Blockchain

Umer Majeed and Choong Seon Hong

Department of Computer Engineering, Kyung Hee University, Yongin, 446-701 Korea
{umermajeed, cshong }@khu.ac.kr

Abstract

The blockchain is a secure, decentralized, distributed ledger which stores transaction in a chain of blocks. Bitcoin uses the distributed public ledger for storing transactional records. Bitcoin uses proof-of-work to mine blocks which correspond to compute hashes to solve a cryptographic puzzle. Computing power is becoming cheaper exponentially. In this paper, we inspect how bitcoin tackles the growing hashing power available in the network to maintain its consistency.

1. Introduction:

The blockchain is a digital, distributed, decentralized, non-tamperable list of records in which transactions are added in a chronological chain of blocks. The first application of blockchain is bitcoin [1]. Bitcoin is the first digital currency which had tackled the double-spending problem with no central trusted authority in a trustless environment. Bitcoin uses proof-of-work for its consensus algorithm to ensure that each participating node has the same replica of the blockchain. Proof-of-Work is a computational intensive cryptographic puzzle to be solved by miners who append new blocks to blockchain in exchange for bitcoins as an incentive.

Since computing power is growing exponentially at a cheaper cost in accordance with Moore's law. Bitcoin has inherently embedded that its proof-of-work puzzle gets harder with time to counter the effect of computational power growth on its mining algorithm. This paper explores the underlying mechanism responsible for increasing hardness of bitcoin hashing puzzle with time.

The rest of the document is formulated as follows. Section 2 will give system model followed by problem formulation in section 3. Section 4 shows Analytical Results and in section 5, we will conclude our research work.

2. System Model:

Let there be **n** miners in our Blockchain network **S**. The **i**th node has local Blockchain $\mathbf{B_i}$ such that block $\mathbf{b_j}$ contains the hash of block $\mathbf{b_{j-1}}$. Where Blockchain is a chain of blocks such that each block has the block header and transactional data.

The block header stores the cryptographic hash of the previous block, timestamp, nonce and Merkle root of transactional data. While the transactional data is stored in the form of Merkle tree. The transactions are hashed, hashes are paired, again hashed and paired until we get the Merkle root of the Merkle tree.

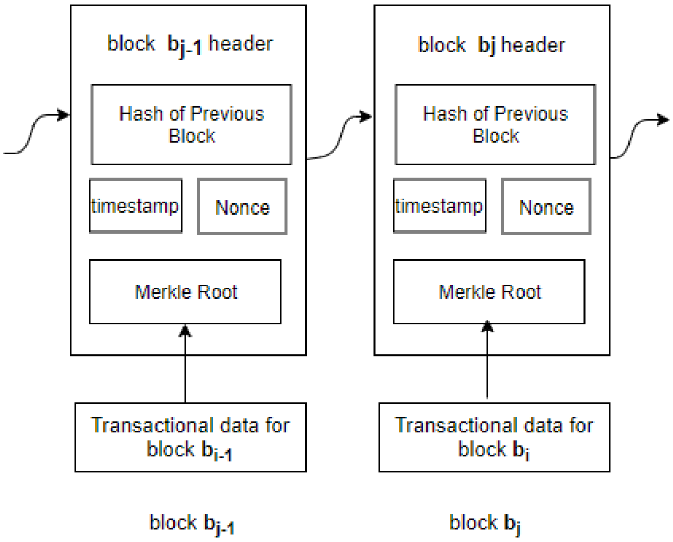

Figure 1: Simplified bitcoin blockchain

3. Problem formulation:

Bitcoin uses SHA-256 as its cryptographic hashing function. In proof-of-work, the miners scan for a value of nonce so that when the block is hashed the hash is less than threshold target number. The threshold target required is set by the difficulty. There is no defined strategy to solve the cryptographic puzzle, the miners simply use brute force mechanism to alter the nonce and get the required hash value which should be lower than current target [2]. Consider **H** as SHA-256 hash function and **D** as block data (except nonce). Successful mining refers to find the value of Nonce **N** such that

$$\mathrm{H(D,N)}\ < current\_target \tag{1}$$

If we have **n** bit hash and we require **k** number of leading bits in it as zero. Then the hash should be

$$\mathrm{H(D,N)} < 2^{n-k} \tag{2}$$

The probability of finding such hash P is given below consequently it will take 2^k attempts to find such a hash.

$$P(\,\mathrm{H(D,N)} < 2^{n-k}\,) = \frac{2^{n-k}}{2^n} = \frac{1}{2^k} \tag{3}$$

The difficulty of this cryptographic puzzle is tunable and depend upon the available hashing power of all the **n** miners in bitcoin network. The computational power (hash rate) needed to reach the target is exponential with respect to the number of leading zero bits required in the target. The difficulty is set so that it is hard enough for miners to mine a block in an average of 10 minutes.

The difficulty is the floating-point measure of how difficult it is to search for a hash below the threshold target. Bitcoin difficulty changes every 2016 blocks and increased or decreased depending upon hashing power available in the network. The formula for difficulty [3] is

$$D = \,difficulty = \frac{difficulty\_1\_target}{current\_target} = \frac{T_{max}}{T} \tag{4}$$

The current target is stored in block header in compact form in a 32-bit field called nBits where difficulty_1_target is the target with difficulty 1. difficulty_1_target is "1d00ffff" in a compact form. The full difficulty_1_target is 0x00000000FFFF000000000000000000000000000000000 0000000000000000000 and can be determined in decimal form from nBits as below:

$$\boldsymbol{T_{max} = 0x00ffff * 2^{8*(0x1d-3)} = (2^{16}-1) * 2^{208} \approx\ 2^{224}}$$

At the time of writing the latest block in bitcoin blockchain is with Block Height 520113, hash 0x0000000000000000000003d1e7e7b8a82a358794c1df268 21df9f7cc5fd4e0c15a and difficulty 3,839,316,899,029.672 while the target in compact form is 1749500d which is stored in nBits field. The decimal target can be obtained as:

$$0x49500\mathrm{d} * 2^{8*(0x17-3)} = 4804621 * 2^{160}$$

The miners have searched for hash lower than this target to mine the block and get their reward. The difficulty **D** of this block can be calculated as follows:

$$\boldsymbol{D = \frac{T_{max}}{T} = \frac{(2^{16}-1)*2^{208}}{4804621*2^{160}}} = 3{,}839{,}316{,}899{,}029.672$$

The probability p of finding 256-bit hash below target [4] T is

$$p = \;\; P(\,\mathrm{H(D,N)} < T) = \frac{T}{2^{256}} = \frac{T_{max}}{D2^{256}} \;\approx \frac{1}{D2^{32}} \tag{5}$$

The estimated time to find a block with hash rate **R** is

$$E[t] = \frac{D2^{32}}{R} \tag{6}$$

Since the intended time to mine a block is 600s. The difficulty is updated after every 2016 blocks as follows where R is hash rate available in the network.

$$D = \frac{R * E[t]}{2^{32}} = \frac{R * 600}{2^{32}} \tag{7}$$

4. Analytical Results:

We get the data from blockchain.info of the difficulty in mining blocks and corresponding hash rate available in the network in bitcoin network. We found that the two metrics are strongly correlated as shown in Fig.2

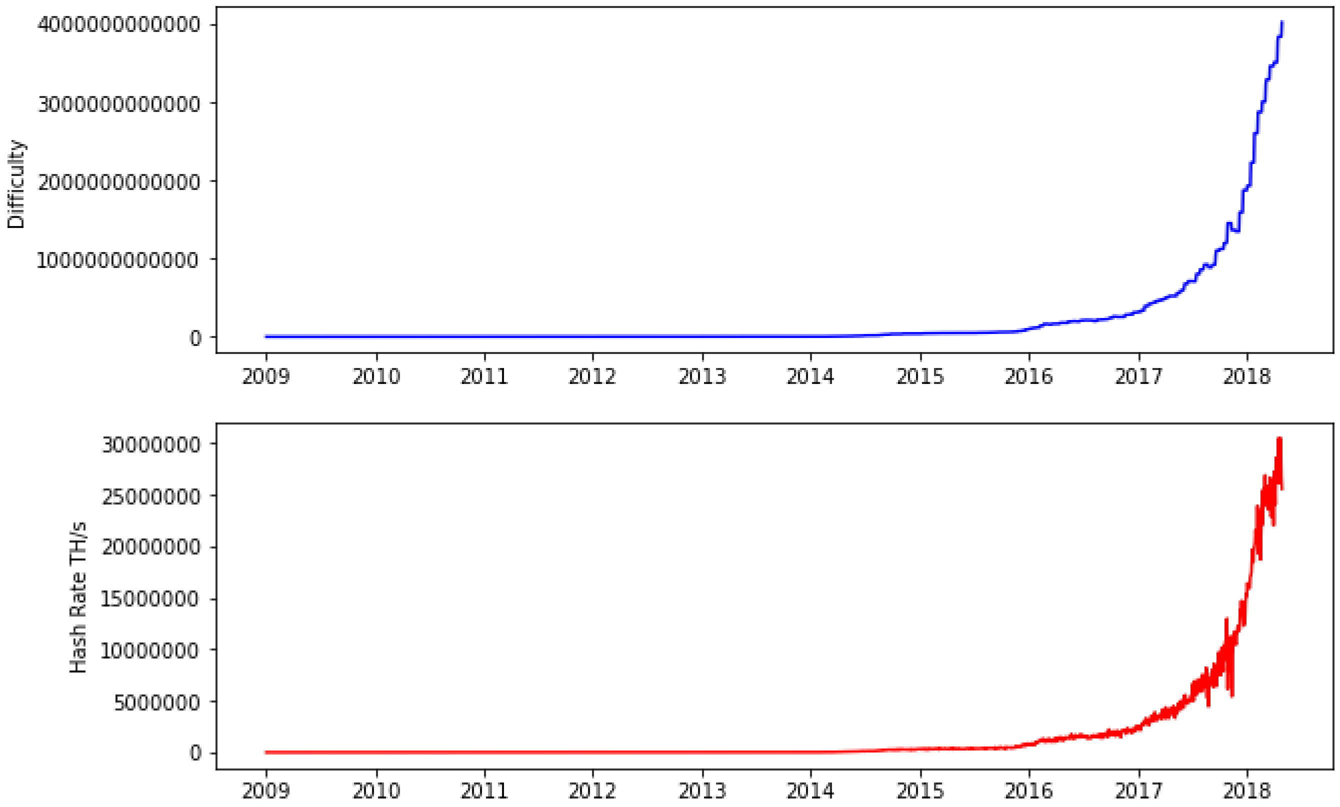

Figure 2: The difficulty and hash rate of bitcoin (Data collected from bitcoin.info/charts)

5. Conclusion and Future Work:

In this paper, we explored the puzzle hardness of proof-of-work of the bitcoin blockchain. We inspected that difficulty to mine a block is increasing based on computational power available on the bitcoin network. The bitcoin processes seven transactions per second on average. With the increasing computational power of miners and the increasing difficulty to mine blocks, the time to mine a block is still at its equilibrium level of ten minutes on average. The increase in transaction speed, scalability as well as consistency and reliability of bitcoin network is critical to its growth and sustainability. There is a need to research and implement algorithms for increasing transaction speed while keeping the consistency of bitcoin blockchain sustained.

Acknowledgment:

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2015-0-00557, Resilient/Fault-Tolerant Autonomic Networking Based on Physicality, Relationship and Service Semantic of IoT Devices) *Dr. CS Hong is the corresponding author.

[REFERENCES]

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[2] Gramoli, Vincent. "From blockchain consensus back to Byzantine consensus." *Future Generation Computer Systems* (2017).

[3] Böhme, Sascha. *Analysis of Bitcoin as a peer-to-peer network for international payments*. Diss. Massachusetts Institute of Technology, 2014.

[4] O'Dwyer, Karl J., and David Malone. "Bitcoin mining and its energy footprint." (2014): 280-285.