POSTER: Mining with Proof-of-Probability in Blockchain

Sungmin Kim
School of Computer Science and Engineering
Chung-Ang University
Seoul, Korea
smkim.caucse@gmail.com

Joongheon Kim
School of Computer Science and Engineering
Chung-Ang University
Seoul, Korea
joongheon@cau.ac.kr

ABSTRACT

As interest in cryptocurrency has increased, problems have arisen with Proof-of-Work (PoW) and Proof-of-Stake (PoS) methods, the most representative methods of acquiring cryptocurrency in a blockchain. The PoW method is uneconomical and the PoS method can be easily monopolized by a few people. To cope with this issue, this paper introduces a Proof-of-Probability (PoP) method. The PoP is a method where each node sorts the encrypted actual hash as well as a number of fake hash, and then the first node to decrypt actual hash creates block. In addition, a wait time is used when decrypting one hash and then decrypting the next hash for restricting the excessive computing power competition. In addition, the centralization by validaters with many stakes can be avoided in the proposed PoP method.

CCS CONCEPTS

• **Networks** → Network reliability;

KEYWORDS

Blockchain, Cryptocurrency, Transaction, Sorting, Hash, Nonce

ACM Reference Format:
Sungmin Kim and Joongheon Kim. 2018. POSTER: Mining with Proof-of-Probability in Blockchain. In *ASIA CCS '18: 2018 ACM Asia Conference on Computer and Communications Security, June 4–8, 2018, Incheon, Republic of Korea.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3196494.3201592

1 INTRODUCTION

The success of Bitcoin, one of the most well-known blockchain applications, has attracted much attention to cryptocurrency. People have adopted various methods to acquire cryptocurrencies including Bitcoin. In addition, the major attraction point was an incentive/compensation-earning method which is implemented in each cryptocurrency. There are two representative methods in incentive/compensation-earning, i.e., Proof-of-Work (PoW) and Proof-of-Stake (PoS), as follows:

- PoW (Proof-of-Work): A way of getting compensation by working, e.g., solving complicate problems.
- PoS (Proof-of-Stake): A way of getting compensation by the stakes of the original cryptocurrency.

ASIA CCS '18, June 4–8, 2018, Incheon, Republic of Korea

ACM ISBN 978-1-4503-5576-6/18/06.
https://doi.org/10.1145/3196494.3201592

However, there exist drawbacks to the two major proof methods. The PoW method is uneconomical due to excessive power consumption occurred during complicate problem solving using distributed computing systems (e.g., GPU). In addition, the PoS method is easy to monopolize by people with large stakes and has a drawback that new network participants may be reluctant to participate in the blockchain network. Several Altcoin (the term collectively used for the sequel to the Bitcoin) have begun to appear that have complemented or applied new concepts. However, these Altcoins are not completely deviate from the PoW and PoS methods. Therefore, it is difficult to solve the problems of excessive power consumption or monopoly those are occurring in currently existing methods.

This paper proposes a way to solve the issues/drawbacks in PoW and PoS methods, which is called Proof-of-Probability (PoP). In the proposed PoP method, each node has its own hash sorting algorithm. When attempting to create transaction information in blocks, the encrypted actual hash and a number of fake hash are distributed over blockchain network. Then, each node finds the actual hash through its own sorting algorithm. The node that first mined the actual hash receives the cryptocurrency compensation.

The remainder of this paper is organized as follows: Section 2 provides related work and literature surveys. Section 3 explains the details of the proposed Proof-of-Probability (PoP) method. Section 4 concludes this paper and presents future research directions.

2 RELATED WORK

This section introduces two major proof algorithms in blockchain cryptocurrecy mechanisms, i.e., PoW (Section 2.1) and PoS (Section 2.2).

2.1 PoW (Proof-of-Work)

The concept of PoW was initially introduced in 1993 by Cynthia Dwork and Moni Naor. In 1999, it was named Proof-of-Work by Markus Jakobsson and Ari Juels. In 2008, Nakamoto SatoshI adopted the PoW method in Bitcoin systems, and this makes the PoW method popular [1].

All transactions made of cryptocurrencies are stored in blocks within the blockchain. A method for verifying the validity of these blocks is called Proof-of-Work. The structure of the block in the blockchain consists of Version, Pre Block Hash, Merkle Root, Creation Time, Bits (diffculty), and Nonce.

In other words, PoW is to find a nonce value and prove the validity of the transaction. The node that found the nonce value receives the cryptocurrency in return for proving the validity of the transaction. The algorithm for finding nonce values is as follows. All cryptocurrencies that can be mined use PoW method. Miner has to insert input values one by one in order to do mining. An average

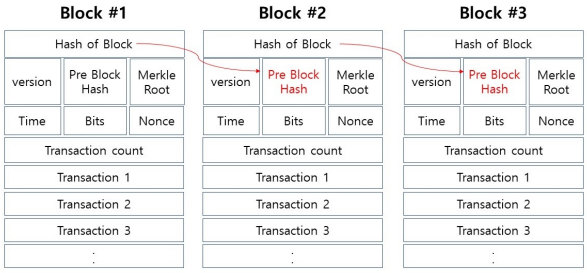

Figure 1: Structure of PoW method.

of trillions of input attempts are required to find a nonce value, and it is almost impossible for the person to do so. For this reason, a group called Mining Pools allocates their computing power, and when the mining succeeds, the cryptocurrency is distributed by the amount of allocated computing power. Currently, the computing power of the Top4 Mining Pools is over 50 percent of the total. If these Mining Pools have a combined computing power of more than 50 percent, then the security of the cryptocurrency is in danger of deteriorating rapidly.

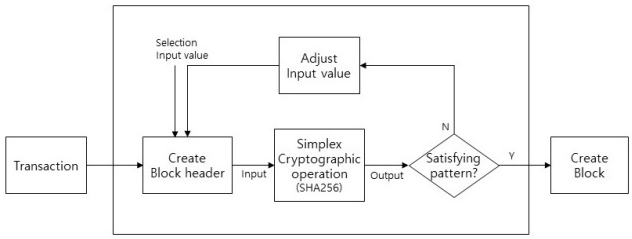

Figure 2: Block creation algorithm.

The nother drawback of the PoW method is cost efficiency. Since the PoW method has to maintain hash consistently, it is necessary to purchase high-performance ASIC and GPU. Moreover, as mentioned above, mining of cryptocurrency requires more than a few trillion input attempts, which consumes a large amount of electricity. The electricity consumption of Bitcoin and Ethereum, which are representative cryptocurrencies adopting PoW method, is higher than that of Syria, which is the 72nd largest electricity consumption country in the world.

Based on this drawback, PoS (Proof-of-Stake), which will be introduced in Section 2.2, appeared in order to solve the high cost of mining, and the security problem caused by hash's monopoly.

2.2 PoS (Proof-of-Stake)

The PoS method was initially used in Peercoin in 2012. PoS method does not have mining that uses computing power unlike the PoW method. In the PoS method, the block validity is verified through own stake. It is similar to the idea of paying a dividend on a stock. The process of validating a blockchain and creating a new block is called forging. The forgers take only transaction fees. When you connect a wallet with a certain amount of cryptocurrency to a blockchain network, you can be rewarded with a cryptocurrency. The way and amount to obtain each cryptocurrency is slightly different, however the more and more cryptocurrency you have, more cryptocurrency can be obtained continuously. For example, a person who has 100 Peercoins would be entitled to validation 100 times more than a person who has only one Peercoin.

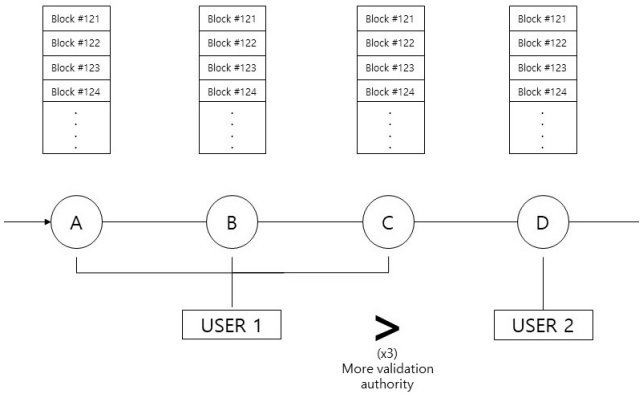

Figure 3: Qualification to validate based on stake.

In case of PoS method, one PC with internet connection can participate in the blockchain. Moreover, additional GPU devices are not necessary. The PoS method is more cost effective than the PoW method because it does not use too much computing power than PoW. However, it is not easy to inflow large amounts of money into the cryptocurrency blockchain because of the fact that the price increase is not large. The fact that a person with a large stake can easily monopolize, the lack of gain in cryptocurrency makes it unfair for new participants. This is one of major disadvantages in the PoS method.

3 SYSTEM MODEL AND ALGORITHM

The basic design concept of the proposed method in this paper is introduced in Section 3.1; and the details of the algorithm is described in Section 3.2.

3.1 Design

The PoW method consumes a large amount of electricity due to over-heated mining as well as the cost of purchasing a mining equipment. To handle this issue, the PoS method solved the economical disadvantage of the PoW method, however participants are hard to come into the system, and they can easily be monopolized by a large shareholder. Only the top four percents own 97 percents of the actual Bitcoin issues. The method used to solve these problems is called the PoP (Proof-of-Probability) in this paper. The overall structure of this PoP method is shown in Fig. 4.

1) Each node (A, B, C, D) has its own hash sorting algorithm.

2) When a transaction occurs, it sends an encrypted hash and a lot of fake hash through the blockchain network.

3) Each node prioritizes hashes to mine with its own hash sorting algorithm.

4) The node put the input value into the sorted hash to find the nonce value satisfying the computation. In the case of fake hash,

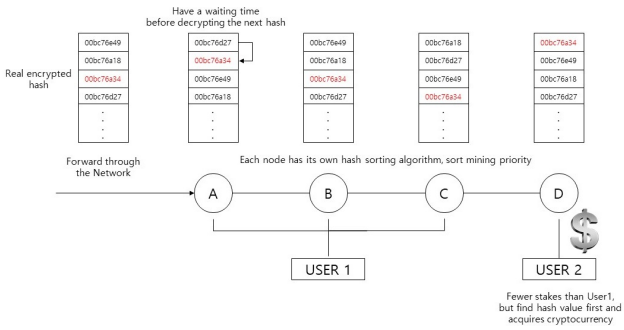

Figure 4: Overall structure of PoP method.

you must have a waiting time to find the nonce value corresponding to the next hash.

5) The node that finds the nonce that corresponds to the real hash receives compensation for the cryptocurrency.

3.2 Main Algorithm

The PoP method proceeds as shown in Fig. 5.

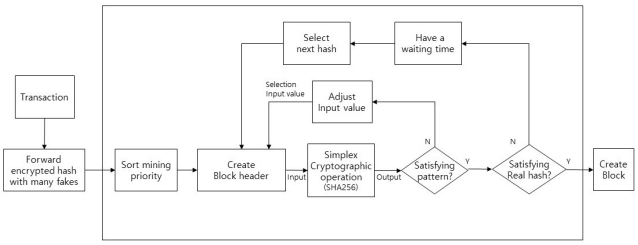

Figure 5: Main Algorithm of PoP method.

1) When a transaction occurs, it sends an encrypted hash and a lot of fake hash.

2) Each node uses its own hash sorting algorithm to sort by mining priority.

3) Create a block header and input any nonce value to perform SHA decryption operation.

4) If the required pattern is not satisfied, adjust the nonce value to repeat step 3.

5) If the required pattern is satisfied, verify that the nonce corresponding to the hash is the nonce of the real hash value.

6) If it is not a real hash value, select the next sorted hash value with wait time, then try step 3.

7) If it proves to be a real hash value, it creates a block for the transaction.

When organized, the following pseudo code is presented in Alg. 1.

It takes about 10 minutes to calculate one hash by adopting PoW method in Bitcoin. For PoP method, you have to compute many hashes, so network can adjust the bits value using bits adjusting algorithm. It is adjusted to take about 1 minute based on the node having hash power of 5,000,000 TH/s (1 TH/s = 10^{12} hash operations per second). When the calculated nonce value from each hash is

Algorithm 1 Pseudo code of PoP method

```
if Occur the transaction then
    transmission(hash[])
    newhash[] = sort(hash[])
else
    Wait until create transaction
end if
if GetHash then
    Create transaction block
else
    GetHash
end if
//Definition of each function
procedure SORT(hash[])
    sort hash[] by independent algorithm
end procedure
procedure GETHASH
    while Satisfied with hash[nz] do
        SHA256(nonce)
        gethash = nonce
    end while
end procedure
```

binarized. If the bit of a nonce of 2^n is 1, the hash is determined to be the true and that node creates a block. If the bit of a nonce of 2^n is 1, the hash is determined to be the true and that node creates a block. n changes randomly every time a transaction occurs, and the value of n is known only to the validator. Also, the calculated nonce is verified for nonce calculated in the real hash. After validating, set a time limit of one minute until the next is validated so that the node can not be verified consecutively.

4 CONCLUSIONS AND FUTURE WORK

In this paper, we propose a Proof-of-Probability (PoP) method to overcome the disadvantages of the existing PoW and PoS methods. The time limit was set whenever one hash was verified, thus the blockchain participants no longer need to have high computing power. In addition, more participants have a stake, the higher the probability of acquiring cryptocurrency, however this is not as absolute as the PoS method when the hash sorting algorithm is different for each node. Using this method will reduce the craze of the overheated computing power and make the participation of new blockchain nodes popular. The exact number of time limits, bits adjusting algorithms in PoP method will be adjusted through future experiments and evaluation of indicators. In addition, we will investigate data-intensive performance evaluations for comparing with existing methods in various aspects.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (2017R1A4A1015675). J. Kim is a corresponding author.

REFERENCES

[1] NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. *Technical Report, Available: http://bitcoin.org/ bitcoin.pdf* (2008).