2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops

Random Mining Group Selection to Prevent 51% Attacks on Bitcoin

Jaewon Bae and Hyuk Lim
School of Electrical Engineering and Computer Science (EECS)
Gwangju Institute of Science and Technology (GIST), Korea
Email: {jaewonbae, hlim}@gist.ac.kr

***Abstract*—Bitcoin is a cryptocurrency based on blockchain technology that enables peer-to-peer transactions without a central authority. Bitcoin is known for resolving double-spending problems. When two or more miners generate a block that includes transaction information at nearly the same time, an accidental fork occurs. In this case, the longest chain of blocks is selected to avoid the double-spending problem. However, if there is an attacker node whose hash power is greater than half of the total hash power, that node can perform a double-spending attack, i.e., a 51% or majority attack. We propose a random mining group selection technique to reduce the probability of successful double-spending attacks. The analysis results demonstrate that if the number of groups is greater than or equal to two, the probability that the attacker will find the next block is less than 50%.**

I. Introduction

Starting with Bitcoin, which was developed by Satoshi Nakamoto in 2009 [1], a number of blockchain-based cryptocurrencies have emerged. Blockchain is a distributed data processing technology for a public distributed ledger. Peer-to-peer (P2P) transaction data are recorded in blocks, and these blocks form a linked list (i.e., chain) of blocks. Each user in the network stores the entire data in a distributed manner without requiring a central authority. In blockchain-based cryptocurrencies, it is nearly impossible to manipulate transactions because the blockchain constitutes a chain of blocks in which each block includes the hash value of the previous block. To maintain a single blockchain in a large P2P network, a distributed consensus mechanism that guarantees system integrity by mutually verifying the results among peer nodes is required. This consensus mechanism should be able to determine who has created new blocks and which chain is valid. Note that different algorithms are used depending on the type of cryptocurrency [2].

Bitcoin uses a proof-of-work (PoW) algorithm, which is the most commonly used consensus algorithm in blockchain-based cryptocurrencies. In summary, compute power is used to derive consensus by finding and verifying hash values that meet specific requirements. PoW is a process to find a nonce value that makes the block hash value less than a target value. Note that a nonce is one of the information specified in the block header. A block is generated if a nonce value that satisfies this requirement is found using brute force. In Bitcoin, the target value represents the difficulty of calculating the nonce value and is adjusted to generate a single block every 10 minutes on average. Peer nodes always accept the longest chain as a correct chain and repeat this procedure such that the blockchain continues to expand. Because a peer node with greater hash power can calculate and find the nonce value faster than peer nodes with less hash power, it has a higher probability of generating a new block.

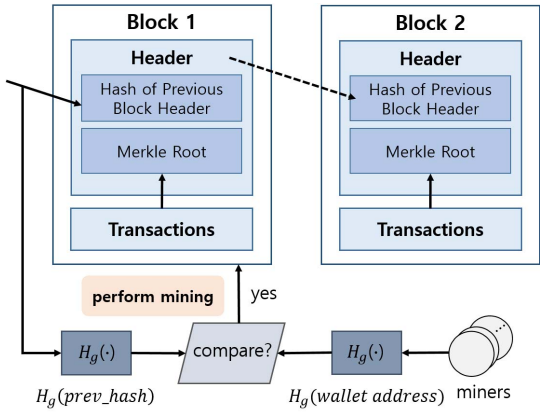

Fig. 1. Schematic of a random mining group selection.

PoW has some critical issues. For example, it requires an enormous amount of computing power [3]. In addition, an attacker with more than half of the total computing power in the entire P2P network can manipulate transactions maliciously. This is referred to as a 51% attack, and such an attack could destroy the Bitcoin system by causing double-spending problem, selfish mining, etc [4]. Several studies have investigated ways to defend against such attacks. Eyal and Sirer [5] proposed a two-phase PoW solution to prevent the formation of a large mining pool with massive hash power. In this solution, the second PoW signs the produced header with the private key of the coinbase address. When the second PoW is sufficiently difficult, pool operators must keep their pool small if they do not want to give up their private keys or sacrifice the pool's mining hashrate. Solat and Potop-Butucaru proposed ZeroBlock [6], a timestamp-free prevention protocol that focuses on defending against selfish mining attacks. Miners must publish a new block within a certain period, referred to as a *mat* interval. If this constraint is not met, the new block is rejected by other honest peer nodes. Ruffing *et al*. [7] proposed non-equivocation contracts to penalize attackers attempting a double-spending attack.

II. Random Mining Group Selection

Each node in the Bitcoin network has a public-private key pair. The public key, which is also called the wallet address, is unique to all nodes. When a transaction is requested, it is

2325-6664/18/$31.00 ©2018 IEEE
DOI 10.1109/DSN-W.2018.00040

propagated to all nodes in the P2P network. Then, the nodes validate each transaction and combine verified transactions into a block. If a peer node successfully creates a new block through the PoW, it propagates the block to the entire network. Then, the transaction is completed if other nodes approve the block and add it to the blockchain.

We propose a random mining group selection technique that reduces computing power and defends against 51% attacks. Here, the basic idea is to divide miners into multiple groups. Note that not all miners are always involved in the mining process, and only miners belonging to a certain group are permitted to mine the next block. Figure 1 illustrates the proposed random mining group selection scheme. Each peer node determines its mining group using hash function $H_g(\cdot)$ and its wallet address. In addition, once a block is created, its hash value is used with $H_g(\cdot)$ to determine which mining group is supposed to find the next block. Only peer nodes belonging to the mining group are authorized to mine the next block and compete with each other. Once a block is propagated over the P2P network, other nodes can inspect whether the block was generated by the proper mining group by comparing the hash value of the previous block in the block header to the block creators address.

Under the proposed mechanism, even though there may exist an attacker with more than one-half of the total hash power, the chances of a successful double-spending attack can be reduced significantly by increasing the number of mining groups because mining groups are chosen randomly, thereby making it difficult for attackers to extend their chain. In addition, the computing power required for block mining is effectively reduced by 1/(number of groups) because (a) peer nodes not belonging to the selected group do not participate in the PoW and (b) the difficulty level can be lowered due to the smaller number of competing miners in each group.

Satoshi Nakamoto, who designed Bitcoin, analyzed the possibility of a double-spending attack on the Bitcoin system using the gamblers ruin problem [8]. Here, let Q_z denote the probability that an attacker would catch up with the normal chain from behind z blocks:

$$Q_z = \begin{cases} 1 & \text{if } p \leq q \\ (\frac{q}{p})^z & \text{otherwise,} \end{cases} \tag{1}$$

where p is the probability that an honest node finds the next block, q is the probability that the attacker finds the next block, and $p + q = 1$. This equation indicates that if the attacker's hash power is less than that of an honest miner, the probability decreases exponentially as z increases. Otherwise, the attack may succeed by 100%.

In (1), q is the ratio of the hash power of the attacker (h) to the total hash power of all N peers in the network (H), i.e., $q = h/H$. Under the assumption that all groups have the same average number of users and the same average hash power, if there are m groups, q under random group selection ($\tilde{q}$) can be expressed as follows:

$$\tilde{q} = \frac{1}{m} \cdot \frac{h}{h + (\frac{N}{m} - 1)(\frac{H-h}{N-1})}. \tag{2}$$

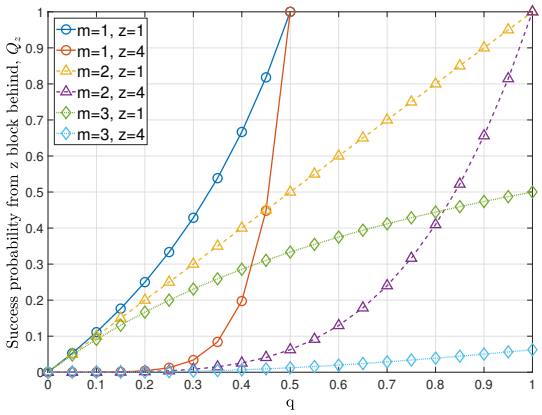

Fig. 2. Probability of the success of attack from behind z blocks.

For large N, $\tilde{q}$ can be expressed as follows:

$$\lim_{N\to\infty} \tilde{q} = \frac{q}{(m-1)q + 1}. \tag{3}$$

The above equation shows that if there are at least two groups (i.e., $m \geq 2$), $\tilde{q}$ cannot be greater than 50%. Using (1) and (3), the proposed method obtains the probability of attack success.

Figure 2 shows the probability of a successful double-spending attack. We plotted the graph for z = 1 and 4 with 1, 2, and 3 groups. The curves with m = 1 correspond to the case of the original Bitcoin. Unlike the original cases, even if q is greater than 0.5, Q_z becomes smaller as m increases.

III. Conclusion

In this paper, we have proposed an approach to reduce the probability of a successful double-spending attack on Bitcoin. The proposed approach divides miners into groups and gives mining opportunity to a randomly selected group. This approach can reduce likelihood of a majority attack and can reduce the computing power costs of block mining.

Acknowledgment

This work was supported by IITP grant funded by the Korea government (MSIT) (No. 2017-0-00421, Cyber Security Defense Cycle Mechanism for New Security Threats), and by GRI grant funded by the GIST in 2018.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," Internat. J. Web Grid Serv., 2016.
[3] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," ISSC 2014/CIICT 2014, Limerick, June 26-27, 2014.
[4] M. Conti, S. Kumar E, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," arXiv preprint arXiv:1706.00916, 2017.
[5] I. Eyal and E. G. Sirer, "How to disincentivize large Bitcoin mining pools," 2014.
[6] S. Solat and M. Potop-Butucaru, "ZeroBlock: Preventing selfish mining in Bitcoin," arXiv preprint arXiv:1605.02435, 2016.
[7] T. Ruffing et al., "Liar, liar, coins on fire!: Penalizing equivocation by loss of Bitcoins," ACM Conf. Comput. Commun. Secur., Oct. 2015.
[8] A. Pinar Ozisik and B. Neil Levine, "An explanation of Nakamoto's analysis of double-spend attacks," arXiv:1701.03977, Jan. 2017.