EVALUATION OF PROOF OF WORK (POW) BLOCKCHAINS SECURITY NETWORK ON SELFISH MINING

I Gusti Ayu Kusdiah Gemeliarana
Department of Electrical Engineering
University of Indonesia
Depok, Indonesia
i.gusti79@ui.ac.id

Riri Fitri Sari
Department of Electrical Engineering
University of Indonesia
Depok, Indonesia
riri@ui.ac.id

Abstract—Bitcoin is one of the first implementations of cryptocurrency or digital currency. It uses has increased in recent years along with the increasing volume of online transactions that require digital currency A blockchain is a digital ledger that allows parties to transact without use of a central authority as a trusted intermediary. In blockchain, there are a number of consensus protocols proposed including Proof of Stake, Proof of Elapsed Time, but most of the existing blockchain utilizes the computed Proof of Work (PoW) mechanism. Transaction security is secured in Bitcoin by using blocks with a hash-based Proof of Work (PoW) mechanism. PoW is a functional protocol that validates every incoming data to overcome spam attacks and Distributed Denial of Service (DDoS) attacks. Blockchain technology can store historically decentralized transaction data where each connected computer will store exactly the same data. To be able to perform an optimal transaction process, it is necessary to evaluate performance of the POW blockchain and find out what influences the transaction process. In this study, we compare simulation result of different block size and block interval to Block Propagation Time, time setup, and Average upload/download with selfish mining attack using NS3. The experimental results show that the smaller the block interval and block size, the smaller the Block Propagation time. It means that faster transactions are confirmed to peers on the network, and this affects the upload/download speeds.

Keywords—POW, Blockchain, Bitcoin, Selfish mining, NS3

I. INTRODUCTION

Bitcoin is a popular cryptocurrency introduced by Nakamoto [1] in 2008. The use of bitcoin as a digital currency has been widely used by online businesses as a means of payment. bitcoin is a general ledger (global ledger) or balance sheet, called the blockchain. This general ledger records all transactions carried out using bitcoin, from the moment bitcoin is mined all transactions are recorded, so this is what makes bitcoin not easily faked. Bitcoin elements are peer-to-peer, block, blockchain and miners. The peer-to-peer network in bitcoin allows users to transfer a number of bitcoin values, these transactions are stored in files called blocks, these blocks will be connected with each other to form block chains called blockchain, and miners solve complex mathematical formulas to prove ownership of bitcoin. A blockchain consists of many blocks, which in turn verify multiple transactions. Users who create and verify blocks are called miners [12].

Miners received newly created Bitcoins as incentive. To regulate the flow of Bitcoins, blocks are created once in approximately 10 minutes. Every transaction from Bitcoin is stored in an open ledger distributed into the Bitcoin network. Each blockchain will be distributed to each computer connected to the network. Each addition of data will be check whether the data is valid or not, which is usually called mining process or known as Proof of Work (PoW). In the blockchain there are several elements such as hash, block and PoW. PoW in the Bitcoin system is commonly referred to as the mining process. The mining process in Bitcoin is an attempt to perform calculations using hash functions like Hashcash for a new block to be received into the blockchain.

Blockchain is a decentralized technology and is distributed to all peer-to-peer network nodes that are constantly updated. Blockchain is not stored in one central location, blockchain cannot be hacked from just one computer. To change one small data on the blockchain, it takes a large amount of computing power to access each instance (at least 51% witness) of the blockchain participant [4]. So, the bigger a blockchain network, the higher the level of security.

Blockchain Bitcoin has driven many innovations. A number of applications have been designed to utilize blockchain. Bitcoin has been reserved several times to adjust consensus (block generation), and network parameters (block size and information propagation protocols) and to improve blockchain efficiency [1][7]. In line with these efforts, alternative decentralized blockchain-based networks have emerged with ambition to optimize consensus and network parameters as well as to facilitate the deployment of decentralized applications over blockchain.

In this study, we evaluate the performance of various consensus and parameters of the PoW blockchain network by utilizing these consensus and parameters.

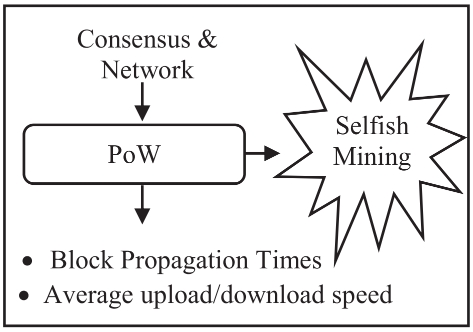

Fig. 1. Component of PoW Blockchain

In Figure 1, we can see the PoW blockchain component which consists of the main element which is the PoW blockchain network. PoW blockchain elements are used with a certain set of consensus and network parameters, such as block propagation times, block sizes, average upload/download speed. The main output of Blockchain is block propagation times (measured or simulated), as inputs in the security model. On the other hand, our security model is based on selfish mining attacks and allows us to consider optimal adversarial strategies and consensus parameters [5][6].

To guarantee the scalability and growth in the system, our work is to provide a way to compare and evaluate the performance of POW blockchains by being given different parameters, including block size and block interval.

The remainder of the paper is organized as follows. In Section 2, we overview the concepts behind PoW Blockchain and simulator NS3. In Section 3, we introduce our experimental scenarios. In Section 4, we present our experimental result and discussion. In Section 5, contains the conclusion of the experiment.

II. Blockchain and Simulator

Blockchain is a database used for decentralized network storage. Blockchain is not only used in financial applications, but also used in many of applications. This section will discuss bitcoin in blockchain and some consensus of Proof of Work [6].

A. Bitcoin Blockchain

Bitcoin is introduced by Satoshi Nakamoto in 2008. Who has a pioneered in cryptocurrency that implements the first blockchain technology. Some of the concepts used are the existence of a database called blockchain which is a "ledger" that can be seen by everyone. Everyone can validate the financial transactions done in the blockchain. This ledger records all transactions that occur, so the flow of transactions can be traced easily.

Blockchain is composed of blocks connected to each other. An n-numbered block is connected with block numbered n-1 and block numbered n + 1. The blocks contain bitcoin transactions that are collected over a period of time. These transactions are validated before they are put into a block [12]. Then a block containing the collection of transactions must be validated also through a process called mining carried out by miners using a computer.

Bitcoin is superior to traditional money, for it is very low transaction costs. An international transaction is usually charged at about 5% of the total transaction value. However, using Bitcoin, the cost can be reduced to very low depending on the size of the transaction. Simply a transaction that only involves 1 sender address and 1 destination address only cost about 1.500 rupiah regardless of the number of bitcoins sent. Charges charged on each bitcoin transaction are paid to Bitcoin miners verifying the transaction. Bitcoin transactions can also be done instantaneously. When transactions in traditional financial systems take several hours to several days to complete transactions, Bitcoin transactions only take 10 minutes [1].

B. Selfish Mining

Selfish mining is mining carried out by a group or miner (miner) that has considerable computing power that does not immediately publish the new block it has created. The new block will be stored long enough for the miner to have longer time to create new blocks. Once the number of blocks created is sufficient, the miner will publish the blocks at once into the Bitcoin network.

Selfish mining can incur losses for other miners who succeeded in creating new blocks, but eventually the new block becomes a stale block or an orphan block, so it does not get new bitcoin [11]. Selfish mining benefits the miners who do it, although of this method is in element of risk.

C. Consensus Proof of Work (PoW)

In blockchain, there are a number of consensus protocols proposed such as PBTS, Proof of Stake, Proof of Elapsed Time, but most of the existing blockchain utilizes the computed Proof of Work (PoW) mechanism. Proof of Work (PoW) contained in Bitcoin is used to protect the ledger blockchain from unwanted changes.

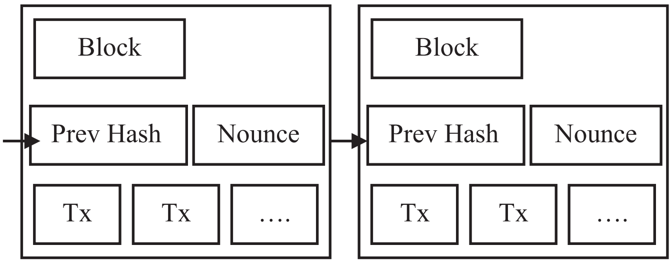

Fig. 2. Proof of Work (PoW)

PoW on Bitcoin works in the following way: All information contained in a candidate block is calculated by its hash value. This hash value generated must meet the criteria of difficulty level determined by the system. If the hash value does not meet the criteria, then the calculation will be repeated by changing the value of nounce (number once). Nonce is a value that does not have any meaning, but is intentionally added to the block in order to generate a hash value according to the conditions. If the hash value has not met the value of the rule, the nonce value will be changed again until the miner finds a hash value that meets the criteria [5].

In addition to using the nonce value, the miners can also take advantage of the coin base value, the first transaction in a block. Miners can add or change the information contained in the coinbase, thereby allowing for a greater variety of hash values. This is done because nonce is only as long as 32bit (4byte) which may not be enough to can be generation of hash values below the target.

The PoW in the Bitcoin system is commonly referred to as the mining process. The mining process in Bitcoin is an attempt to perform calculations using hash functions like Hashcash for a new block to be received into the blockchain. When the result is acceptable, the new block is added to the blockchain. Here the PoW can work to protect the blockchain. With the high level of difficulty, anyone who intends to change the transactions that have been recorded in a block, must do the recalculation of the block and also the next blocks. This is because as has a block is connected to other blocks that form a chain. So when a link is about to change, the next link must also be changed. Therefore, transactions in Bitcoin are very difficult to cancel if they have been included in the blockchain [5][6].

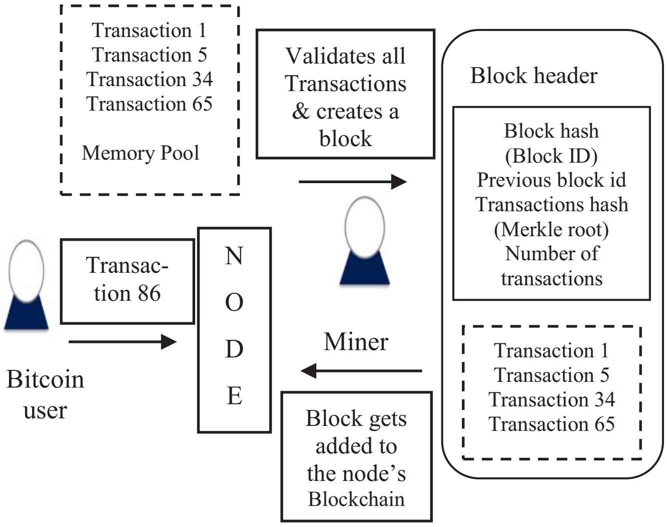

Fig. 3. Block Mining Process

Bitcoin miners are those who provide computing equipment to help make calculations in creating new blocks. Bitcoin miners will get paid in the form of Bitcoin for their efforts. Miners communicate with the Bitcoin node to obtain information about new transactions that must be inserted into the new block.

Bitcoin, for example, uses a hash-based PoW that requires the determination of nonce values, so that when hash with additional block parameters, the hash value must be less than the current target value. When it cannot be found, the miner creates the block and passes it on the network layer to the peers. Other peers in the network can verify PoW by calculating the hash of the block and check if it satisfies the condition to be smaller than the current target value [7].

- Block Interval
  The block interval determines latency when the content is written to blockchain. The smaller the block interval, the faster the transaction is confirmed and the higher the probability of the stale block. The adjustment of block intervals is directly related to changes in the underlying PoW mechanism. Lower difficulty generates more blocks in the network, while more difficult results produce fewer blocks at the same time frame. Therefore, it is important to analyze whether changing difficulties affects the hostility capability of attacking the longest chain, which is the main pillar of security for most PoW-based blockchains.
- Block size
  Maximum block size directly defines the maximum number of transactions performed in a block. This measure controls the throughput achieved by the system. Large blocks produce a slower propagation speed, which in turn increases the stale block rate (and weakens blockchain security).
- Information propagation mechanism
  The block request management system determines how information is communicated to peers in the network. Finally, all peers are expected to receive all blocks, the broadcast protocol is required. The underlying broadcast protocol options clearly impact the robustness and the scalability of the network.
- Stale Blocks
  Stale blocks refer to blocks that are not included in the longest chain, for example, because of concurrency, and conflict. Stale blocks are detrimental to the security and performance of blockchains for triggering chain forks, inconsistent circumstances that slow down major chain growth and result in significant performance and security implications. On the one hand, stale blocks increase the benefits of enemies in the network. On the other hand, stale blocks generate additional bandwidth overhead and are usually not awarded for mining [5].

D. Network Simulator (NS3)

NS-3 is a network simulation that allows network programmers to create simulations of networks to be built and share code from the simulations and implementations of the protocols run. NS-3 is an open source network simulation program, commonly used by researchers, academics, and practitioners. It has been developed for many years and supports almost all communication protocols such as Zigbee, Bluetooth, and others. It also supports various modules that allow parallel simulation, distributed simulation and other. Can be extended easily to support and test various applications. NS-3 is built using C ++ programming language and uses python script [4][11].

III. Scenario and Experiment

In this section, we evaluate the security and performance of various consensus and parameters on the PoW blockchain network using NS3. The purpose of NS-3 is to develop research on the network through simulation so that it makes it easier to do research on the network that will be developed later. The NS-3 developers are committed to making these simulation devices easy to use so they can serve the needs of researchers in floating their networks [4]. In this study, we use the POW consensus method where each computer connected to the blockchain network validates a transaction.

Based on the framework, we designed selfish mining by considering several parameters such as network propagation, time setup and average upload / download speed. Therefore, Arthur Gervais (2016) [5] drafted a framework to capture existing PoW-based applications as well as PoW blockchain variants used with different parameters, and objectively compare the performance and security requirements of blockchain.

TABLE I. Parameter of PoW Blockchain Consensus

Block	Parameters to be measured	
Block Interval	Block Propagation Time (T_{MBP})	Time Setup (s)
Block Size	Average upload/download	

In the experiment, we try to determine the value of the components or parameters to be analyse as in Table II.

TABLE II. SCENARIO OF EXPERIMENT

Parameter	Value
Block Interval	20 minute, 15 minute, 5 minute, 1 minute
Block Size	0.1MB, 0.3MB, 0.6MB, 1MB
Number of Block	10
Number of Node	16

Table II shows the scenario of experiment. We did five experiments with the value of block intervals and block sizes that changed from large to small and determined the number of blocks by 10 and number of nodes by 16.

IV. EXPERIMENT RESULT

In this section, we will conduct a measurement experiment by determining the value of some parameters. The parameters are block size and block interval to measure average Upload/Download, Mean Block Propagation Times, Setup Time.

A. *Block size and Block Interval Parameter*

TABLE III. VALUE OF FIG.4

Line	Value
························	1 Minute
— — — — —	5 Minute
————————	10 Minute

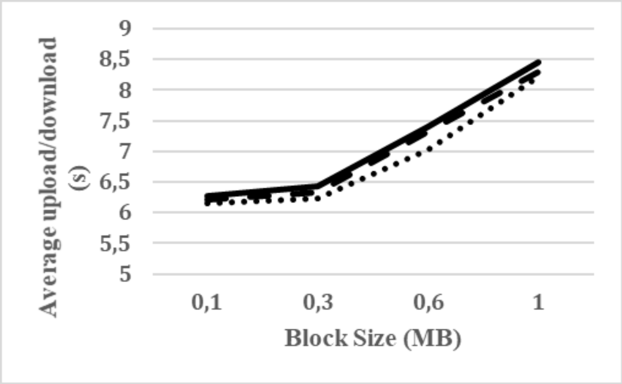

Fig. 4. Block size Vs Average Upload/Download

TABLE IV. VALUE OF FIG.5 –7

Line	Value
························	0.1 MB
— — — — —	0.2 MB
————————	0.5 MB

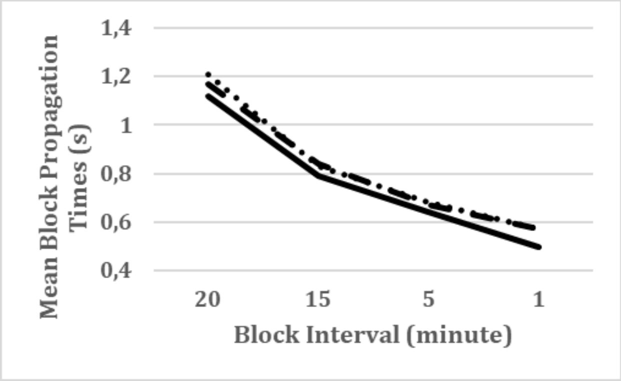

Fig. 5. Block Interval Vs Mean Block Propagation Times

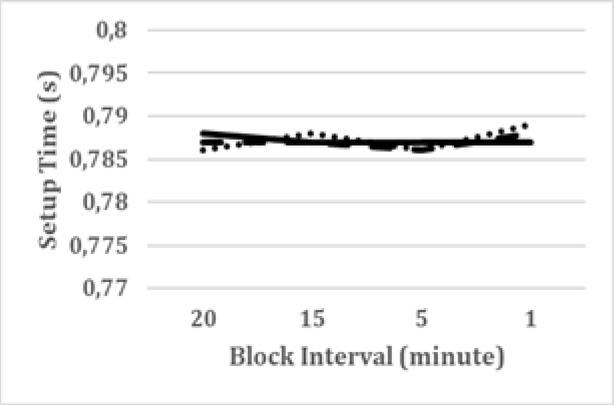

Fig. 6. Block Interval Vs Setup Time

B. *Bitcoin on Selfish Mining Measurement*

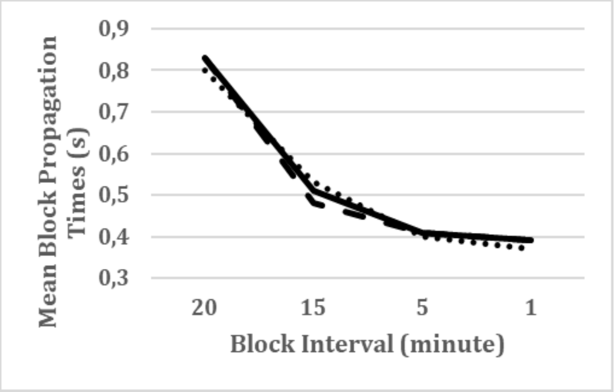

Fig. 7. Block Interval Vs Mean Block Propagation Time (Selfish Mining)

The proof-of-work mechanism is the largest consensus mechanism on blockchain. This mechanism affects including block size and block interval. In Fig. 4, our result show that the larger the block size, the greater the average speed of upload/download. This is because a block size in bitcoin refers to the block code size representing the bitcoin transaction chain. The Bitcoin network collects transactions into blocks that are forwarded to the network approximately every minute. All of these blockchain data must be downloaded and verified in real time. The more data that needs to be downloaded and verified the big block size is needed.

Block interval adjustments are directly related to changes in the underlying PoW mechanism. In Figure 5, our result shows that the smaller the block interval, the faster the mean block propagation time. This is because the role of the block interval is to determine latency when the content is written to the blockchain. The smaller the block interval, the faster the transaction can be confirmed. While in Fig. 6, our result show that the time setup generated is relatively constant. The setup time is the time required to prepare the device, machine, process or system to be ready to work or accept the job.

Selfish mining is carried out by miners who have considerable computational power that does not immediately publish new blocks that they have successfully created. The new block will be stored for a long time so that the miner has more time to create new blocks. In Fig. 5 & Fig. 7, we can compare the results of the block interval measurements before being selfish mining and after being selfish mining. From this result there is a decrease in mean block propagation times between the attack and after the attack. This decrease is due to the selfish mining attack which causes a blockchain performance to decrease.

V. Conclusion

In this experiment, we analyse the performance of various consensus and parameters on the PoW blockchain network. Based on the experiment, we designed selfish mining by considering several parameters such as block propagation, different block size, block interval, and average upload/download speed.

Proof-of-Work (PoW) is the basis for the security of the bitcoin system. It’s also the basis for decision making in the confirmation process on the bitcoin system [5]. From the results of our experiments we have proven the effect of block size and block intervals on POW blockchain performance. Block size served for control the throughput achieved by the system. Large blocks produce a slower propagation speed. While block intervals are responsible for determining latency when content is written to blockchain. The smaller the block interval, the faster the transaction is confirmed [5]. The blockchain POW performance can be reduced and disrupted by attacks from selfish mining. Therefore, it is necessary to hold further evaluation on mining computing power to be able to defend the system from an attack.

Acknowledgement

This paper is funded by Shera USAID Grant University of Indonesia – No. 140/UN2.R3.SC/HKP.05.01/2018.

References

[1] Bitcoin: A Peer to Peer Electronic Cash System, 2008. Available from: https ://bitcoin.org/bitcoin. pdf

[2] Goswami, Sneha, "Scalability Analysis of Blockchains Through Blockchain Simulation" (2017). UNLV Theses, Dissertations, Professional Papers, and Capstones. 2976.

[3] Till Neudecker, dkk. “A Simulation Model for Analysis of Attacks on the Bitcoin Peer-to-Peer Network”, IEEE/IFIP 1st International Workshop on Security for Emerging Distributed Network Technologies (DISSECT), 2015, pp.1327-1332

[4] S.Gan,”An IoT Simulator in NS3 and A Key-Based Authentication Architecture for IoT Devices Using Blockchain ”, thesis, Dept.Computer Science and Engineering. Indian Institute of Technology Kanpur. India, 2017

[5] Gervais, Arthur, “On the Security and Performance of Proof of Work Blockchains”, in CCS’16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016

[6] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, “Tampering with the Delivery of Blocks and Transactions in Bitcoin,” Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. - CCS ’15, pp. 692–705, 2015.

[7] Ittay Eyal and Emin Gun Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography and Data Security, pages 436-454.Springer, 2014

[8] Nubika,Ibrahim.,”Cryptocurrency”, Bitcoin: Recognize a new way of Investing Milennial Generationl, Bantul: Genesis Learning, 2018, pp.84-121.

[9] Bitcoin Simulator, 2016. Available from:
http ://github.com /arthurgervais/Bitcoin -Simulator

[10] F. Dai, N.MengL.Wei and Z.Ye. From Bitcoin to Cyber security: a Comparative Study of Blockchain Application and Security Issues. In 2017 IEEE Fourth International Conference on Systems and Informatics (ICSAI), pages 1–5. IEEE, 2017.

[11] K.Nayak, S.KumarA.Miller and E.Shi. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. In 2016 IEEE European Symposium on Security and Privacy, pages 1–16. IEEE, 2016.

[12] Samiran Bag, and Sushmita Ruj, “Bitcoin Block Withholding Attack: Analysis and Mitigation”, IEEE Transactions On Information Forensics And Security, Vol. 12, No. 8, August 2017, pp.1967-1978.