Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Widya Nita Suliyanti
Assignment title:	Dosen Informatika
Submission title:	Evaluation of Hash Rate-based Double-Spending based on P...
File name:	sed_Double-Spending_based_on_Proof-of-Work_Blockchain_-...
File size:	313.97K
Page count:	6
Word count:	4,412
Character count:	23,372
Submission date:	27-Jun-2023 09:51AM (UTC+0700)
Submission ID:	2123252429

Evaluation of Hash Rate-based Double-Spending based on Proof-of-Work Blockchain

Widya Nita Suliyanti
Departement of Electrical Engineering
Universitas Indonesia
Depok, Indonesia
widya.nita@ui.ac.id

Riri Fitri Sari
Departement of Electrical Engineering
Universitas Indonesia
Depok, Indonesia
riri@ui.ac.id

***Abstract*— A Blockchain is a distributed public ledger that hold immutable data in a secure and encrypted way to ensure that a transaction is safe and cannot be altered. It is implemented based on a consensus algorithm called Proof-of-Work (PoW) which confirms transactions and produces new blocks to the chain. With PoW, miners compete against each other to complete transactions on the network and get rewarded.**

In this paper, we simulate bitcoin, which is a well-known example of a Blockchain, to perform tasks such as network and blockchain simulation, and being the subject of a double spending attacks using a framework established by Arthur Gervais. This framework is utilized to evaluate the double-spending behavior of bitcoin based on an average attacker's hashrate as a proxy measure of the security of processed transactions. This stimulation runs in a discrete-event network simulator called NS-3.

The result of this simulation shows that an increase in attacker's hashrate is parallel with an increase in number of double-spending attacks, an increase in attacker's income and the number of stale blocks posing a threat to transaction's security. Stale blocks increase the advantage of attacker in the double spending attacks in the network.

Keywords—Blockchain, Proof of Work, PoW, hash rate, double spending, NS-3lockchain, Proof of Work, double-spending, security

I. Introduction

Since Bitcoin has been introduced, its underlying technology, blockchain, has been receiving more and more attention. A blockchain is a distributed networking system of replicated state machines that resemble the form of a data chain. This system received its name from how it bundles new transactions into "blocks" and writes those transactions onto the end of a "chain" of existing blocks that describes all prior transactions. As a blockchain grows, new blocks are included in state machines. This addition is then propagated to all participating nodes within the network such that every node in the network has a single global view of all transactions. If there is an attack on a node that tries to change the value of a transaction, this change can be easily detected by other nodes thus it increases the network security.

The design of Blockchain allows it to be decentralized, trustable, traceable and immutable [1]. The process of chaining blocks together provide the level security that has made Bitcoin immune to hacking. The available level of security means that attacks on a node can be easily detected. This would be further elaborated in the literature review. A key feature of Blockchain is the hash rate, which has gained a high level of attention due to its dual purpose. This study aims to investigate how changes in the hash rate affects variables such as the number of double spending attacks, attacker's income and the number of stale blocks, which together form the main behaviors of an attacker. This is accomplished through the use of a simulation based on a framework provided by Arthur Gervais, which runs on NS3. This framework was specifically chosen due to its expertise in accounting for an attacker's hash rate.

II. Blockchain and Bitcoin Transaction

A. Bitcoin

Bitcoin is the first decentralized digital currency (cryptocurrency) which first appeared in 2008 [2] . It is a form of electronic cash that allows electronic transaction without the needs for intermediaries. Bitcoin transactions are recorded in distributed ledger called blockchain using a consensus mechanism named Proof of Work. Bitcoin was launched soon after the financial crisis of 2007-2008 that had dented people's faith in central banking authorities. This could have been another driving force for Nakamoto to start with the decentralized monetary system.

Bitcoin supersedes fiat currency, which is traditional currencies such as US Dollar and Euro, in multiple dimensions because it can be infinitely transferred internationally, transactions have either none or a negligible fee, it currently does not need any personal information, is transparent as every user has a copy of public ledger, and secure as the underlying cryptographic algorithm provides security. As the former is a new currency in the system, two major challenges that Bitcoin is facing are volatility, and degree of acceptance. The latter is perhaps more pressing of the two as the former should reduce as the currency is used by more and more people [3].

Electronic payments are performed by generating transactions that transfer Bitcoin coins (BTCs) among Bitcoin peers. These peers are referenced in each transaction by means of virtual pseudonyms – referred to as Bitcoin addresses. Each address is mapped through a transformation function to a unique public/private key pair. These keys are used to transfer the ownership of BTCs among addresses [4].

Peers transfer coins to each other by issuing a transaction. A transaction is formed by digitally signing a hash of the previous transaction where this coin was last spent along with the public key of the future owner and incorporating this signature in the coin [5]

978-1-7281-0893-3/19/$31.00 ©2019 IEEE

ICTC 2019

Evaluation of Hash Rate-based Double-Spending based on Proof-of-Work Blockchain - 2019

by Widya Nita Suliyanti

Submission date: 27-Jun-2023 09:51AM (UTC+0700)
Submission ID: 2123252429
File name: sed_Double-Spending_based_on_Proof-of-Work_Blockchain_-_2019.pdf (313.97K)
Word count: 4412
Character count: 23372

Evaluation of Hash Rate-based Double-Spending based on Proof-of-Work Blockchain

Widya Nita Suliyanti
Departement of Electrical Engineering
Universitas Indonesia
Depok, Indonesia
widya.nita@ui.ac.id

Riri Fitri Sari
Departement of Electrical Engineering
Universitas Indonesia
Depok, Indonesia
riri@ui.ac.id

***Abstract*— A Blockchain is a distributed public ledger that hold immutable data in a secure and encrypted way to ensure that a transaction is safe and cannot be altered. It is implemented based on a consensus algorithm called Proof-of-Work (PoW) which confirms transactions and produces new blocks to the chain. With PoW, miners compete against each other to complete transactions on the network and get rewarded.**

In this paper, we simulate bitcoin, which is a well-known example of a Blockchain, to perform tasks such as network and blockchain simulation, and being the subject of a double spending attacks using a framework established by Arthur Gervais. This framework is utilized to evaluate the double-spending behavior of bitcoin based on an average attacker's hashrate as a proxy measure of the security of processed transactions. This stimulation runs in a discrete-event network simulator called NS-3.

The result of this simulation shows that an increase in attacker's hashrate is parallel with an increase in number of double-spending attacks, an increase in attacker's income and the number of stale blocks posing a threat to transaction's security. Stale blocks increase the advantage of attacker in the double spending attacks in the network.

Keywords—Blockchain, Proof of Work, PoW, hash rate, double spending, NS-3lockchain, Proof of Work, double-spending, security

I. INTRODUCTION

Since Bitcoin has been introduced, its underlying technology, blockchain, has been receiving more and more attention. A blockchain is a distributed networking system of replicated state machines that resemble the form of a data chain. This system received its name from how it bundles new transactions into "blocks" and writes those transactions onto the end of a "chain" of existing blocks that describes all prior transactions. As a blockchain grows, new blocks are included in state machines. This addition is then propagated to all participating nodes within the network such that every node in the network has a single global view of all transactions. If there is an attack on a node that tries to change the value of a transaction, this change can be easily detected by other nodes thus it increases the network security.

The design of Blockchain allows it to be decentralized, trustable, traceable and immutable [1]. The process of chaining blocks together provide the level security that has made Bitcoin immune to hacking. The available level of security means that attacks on a node can be easily detected. This would be further elaborated in the literature review. A key feature of Blockchain is the hash rate, which has gained a high level of attention due to its dual purpose. This study aims to investigate how changes in the hash rate affects variables such as the number of double spending attacks, attacker's income and the number of stale blocks, which together form the main behaviors of an attacker. This is accomplished through the use of a simulation based on a framework provided by Arthur Gervais, which runs on NS3. This framework was specifically chosen due to its expertise in accounting for an attacker's hash rate.

II. BLOCKCHAIN AND BITCOIN TRANSACTION

A. Bitcoin

Bitcoin is the first decentralized digital currency (cryptocurrency) which first appeared in 2008 [2] . It is a form of electronic cash that allows electronic transaction without the needs for intermediaries. Bitcoin transactions are recorded in distributed ledger called blockchain using a consensus mechanism named Proof of Work. Bitcoin was launched soon after the financial crisis of 2007-2008 that had dented people's faith in central banking authorities. This could have been another driving force for Nakamoto to start with the decentralized monetary system.

Bitcoin supersedes fiat currency, which is traditional currencies such as US Dollar and Euro, in multiple dimensions because it can be infinitely transferred internationally, transactions have either none or a negligible fee, it currently does not need any personal information, is transparent as every user has a copy of public ledger, and secure as the underlying cryptographic algorithm provides security. As the former is a new currency in the system, two major challenges that Bitcoin is facing are volatility, and degree of acceptance. The latter is perhaps more pressing of the two as the former should reduce as the currency is used by more and more people [3].

Electronic payments are performed by generating transactions that transfer Bitcoin coins (BTCs) among Bitcoin peers. These peers are referenced in each transaction by means of virtual pseudonyms – referred to as Bitcoin addresses. Each address is mapped through a transformation function to a unique public/private key pair. These keys are used to transfer the ownership of BTCs among addresses [4].

Peers transfer coins to each other by issuing a transaction. A transaction is formed by digitally signing a hash of the previous transaction where this coin was last spent along with the public key of the future owner and incorporating this signature in the coin [5]

Transactions are included in Bitcoin blocks that are broadcasted in the entire network. To prevent double-spending of the same BTC, Bitcoin relies on the synchronous communication assumption along with a hash-based PoW concept [4].

A key part of Bitcoin is the concept of hashrate. Has hrate forms the backbone of cryptocurrency mining in general [6], particularly because of its far-reaching features. Firstly, hashrate shows the amount of computing power, called hashing power in blockchain, available to the network. This indicates the speed of finding a new block. Then, hashrate is related to the amount of block reward received by miners as an increase in hashrate increases the opportunity of miners to find the next block which allows them to receive a greater amount of block reward. Thus, it is highly valued by miners as it acts as a measure of their performance. The SHA-256 algorithm technique is employed to hash solved Bitcoin blocks.

B. Blockchain

All Bitcoin transactions are collectively stored in a public ledger called as blockchain [3]. Blockchain is a shared database with data that is neither stored in one location nor owned by only one entity. Since control is decentralized, data within the shared database is not easily compromised, stolen or changed.

In comparison with fiat currencies, the evolution and development of a centralized system often used by fiat currencies, have resulted in vulnerabilities and redundancies. This provides an opportunity for the system to then be exploited. Some of the severe consequences include data leaks, transaction manipulation and resource laundering. Whereby in blockchain, the control of transaction is given back to the users where they can transact an asset mutually, effectively eliminated any third-party regulatory body intervention. The transaction is then updated in an irreversible public ledger. This technology provides transparency and eliminates any potential manipulation, bogus transaction, and authority exploitation.

Furthermore, in a centralized system, server failures can lead to the system shutting down. This makes the system vulnerable to DoS attack. Such a system has network and software dependencies, and the efficient functioning of services relies on this factor. On the contrary, the blockchain has a network of miners to update and maintain the ledger. Despite one node failing, other nodes will update transactions on the block. Due to the number of active nodes at each time fragment, the ledger will always be updated. Hence, there are no dependencies for accessing and executing transactions and there is no single point of failure like centralized system [7].

The proposed solution begins with a timestamp server which provides timestamp that proves the data must have existed at the time of transaction. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishes the hash, such as in a newspaper. Each timestamp includes the previous timestamp in its hash, and then proceeds in forming a chain, with each additional timestamp reinforcing the ones before it (Fig. 1) [5] .

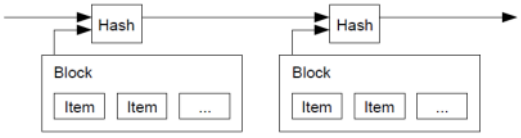

Fig. 1. Block and Hash

Transactions are the atomic data structure of a blockchain. Typically, a transaction is created by a set of users or autonomous objects to indicate the transfer of tokens from the senders to the specified receivers. A transaction specifies a possible empty list of inputs associating the token values with the identities of the sending entities. To protect the authenticity of a transaction record, the functionalities of cryptographic hashing and asymmetric encryption are activated [8].

Bitcoin transactions are grouped into blocks. Each block references a previous block by including a unique hash of previous blocks in its header. An exception occurs for the first block, named the genesis block, which cannot reference an earlier block [9]. The blocks are then organized in chronological order as a “chains of blocks” [8]. Once a block is added to the blockchain, it cannot be modified or removed for two reasons: first, a block modification would lead to wrong verification of the chain of hash values, and second, the block modification would require intensive efforts to change every replicate of the blockchain supposed to be hosted on a large number of independent nodes [10].

In an open-access (i.e. public/permissionless) blockchain network, a node can freely join the network and activate any available network functionalities. Notice the term “node” refers to a logical entity (i.e. identity of a blockchain user) rather than a physical device. For example, multiple “nodes” associated with different network functionalities can be hosted on the same physical machine. In other words, a physical device may appear in multiple identities in the network [8].

Bitcoin uses the PoW technique as an algorithm to confirm the transaction and add new blocks to the chain for block validation. PoW is a blockchain consensus rule for a public network [11]. It is used to protect blockchain ledger from unnecessary changes [12]. With PoW, miners – party who write data to new blocks – go up against each other to finish exchanges on the system and be compensated. A decentralized ledger accumulates every one of the exchanges that are grouped into blocks. Each block is then added on to the Blockchain when a miner solves the hash for that specific block. The goal of Proof of Work is to find a possible solution for a complicated mathematical puzzle. The complexity of the puzzle increases with the growth of the network [13].

Proof-of-Work (POW) system is a distributed timestamp server on a peer-to-peer basis. It is implemented by incrementing a nonce in the block until a value is found. It will give the block’s hash the required zero bits. Once the CPU effort has been expended to satisfy the POW’s requirement, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it (Fig 2).

POW solves the problem of determining representation in majority decision making. When simplified, POW is similar to a one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest invested POW effort [5].

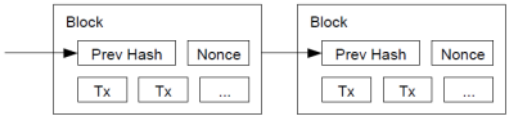

Fig. 2. Proof-of-Work Blockchain

Because there is money involved, miners that performed PoW may try to devise strategies to increase their mining revenue beyond their fair share. Such a technique has been described as selfish mining. This strategy is exploiting the variance in block generation by partially withholding information [14], causing altruistic miners to waste computational resources. For a selfish miner in Bitcoin, withhholding a freshly minted block from the blockchain involves a risk; by the time selfish miner releases the block, the other miners may have advanced in the chain and this block becomes stale, thus not yielding any rewards for the selfish miners.

In Bitcoin circles, the total number of hashes per second made by all players is referred to as the network hash rate [15]. Hash rate is the speed at which a compute is completing an operation in the bitcoin code [2]. Bitcoin measures the level of computing activity on the network in terms of the hash rate [16].

Normally, stale blocks come into existence due to propagation delays [17]. Propagation delay is the combination of transmission time and the local verification of a block or a transaction. The transmission time includes an announcement in the form of an inv message, a request from the receiving party and a delivery. The verification of a block includes the verification of each transaction in the block [18].

Stale blocks are detrimental to the blockchain's security and performance because they trigger chain forks – an inconsistent state which slows down the growth of the main chain. Stale block refers to blocks that are not included in the longest chain. Stale blocks increase the advantage of the adversary in the network (e.g. double-spending) [2]. Stale block can be utilized by attackers to take over the network.

C. *Double-Spending*

At first, a merchant receives a request to provide a product/service. The merchant is convinced that the transaction is true and send the product to attacker who supposedly hold bitcoin to pay for the product. Afterwards, an entire network consisting of a node involved in the transaction is confirmed to accept some other transaction whereby the attacker receives the product/service and will also get the bitcoin as the payment. The end result would be that the merchant is left with neither product nor coins. This phenomenon is called double-spending. In other words, double-spending is a scheme where the same digital token can be spent more than one

The core issue behind double-spending is synchronization. Thus if given two conflicting transactions, only one transaction can be accepted and that same transaction cannot be reversed. Bitcoin solves this problem using the POW consensus using a computational effort consisting of calculation of hashes however if the attacker is in control of substantial computational power, he may succeed in elevating conflicting transactions.

Double spending attack is spending a currency indication more than one of and it is the fundamental reliability issues in digital currencies. In the bitcoin network, the customer attains a double spend if he/she accomplished concurrently to spend the equivalent position of bitcoin in two dissimilar transaction. The attacker assemble a particular blockchain that is extended than the public chain [19].

The main intuition behind Bitcoin is that for peers to double-spend a given BTC, they would have to replace the transaction where the BTC was spent and the corresponding block in which it appeared; otherwise, their misbehavior would be detected immediately [4].

Transaction confirmation in Bitcoin requires tens of minutes, double-spending attacks on fast payments, where the time between the exchange of currency and goods is short (in order of a minute), succeed with considerable probability [4].

The process is in Figure 3.

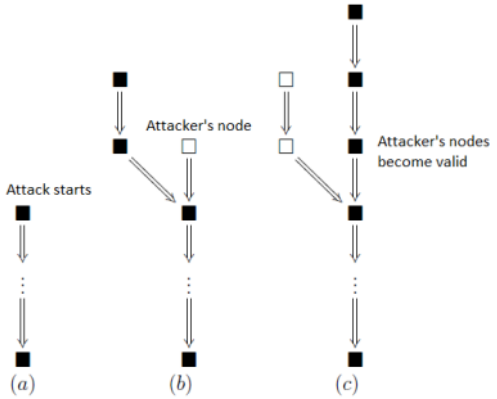

Fig. 3. Outline of double-spending (a) The state of the blockchain when the attack starts. The leaf block does not have any of the relevant transaction yet. (b) The branch on the left is known to the network, and includes the transaction paying the merchant with two confirmations. The merchant now sends the product. Meanwhile, the attacker has found 1 block in an alternative private branch which credits himself instead. (c) If the attacker manages to get his branch to be longer than the one known by the network, he releases it and the payment to himself is now accepted by the network.

A successful double-spending attack consists of the following steps:

1. Broadcast a transaction to the network in which the attacked merchant is paid
2. Secretly mine a branch which builds on the latest block at the time (before the transaction made it into a block), which includes a conflicting transaction which pays the attacker instead of a transaction from honest network
3. Wait until the transactions to the merchant receives enough confirmation and the merchant, confident in his payment, sends the product

4. If necessary, continue to extend the secret branch (which contradicts the transaction) until it is longer than the public branch (which includes the transaction), then broadcast it. Because the new branch is longer than the one currently known by the network, it will be considered valid, and the payment to the merchant will be replaced by the payment to the attacker.

III. METHOD

Using a framework provided by Arthur Gervais [2] with network parameters; average block generation interval of 15 minutes, targeted number of blocks is 300 with 16 number of nodes, we have run our Bitcoin simulator. We modified the last element of the minerHash matrix, which indicates the range of an attacker's hash rate, from 0.3 (30%) to 0.6 (60%).

Attacker's hash rate could provide an indication about the proneness of double-spending attacks in the network. Thus, it relates to blockchain security. High number of double spending attacks might indicate lower blockchain security.

The total hash rate of the honest network and the attacker is constant [9]. Combined they have a hash rate of H, of which pH belongs to the honest network and qH belongs to the attacker, where $p + q = 1$. This means that when a block is found, it has a probability of p to belong to the honest network and a probability of q to be found by the attacker. If the attacker control more than half of the total network hash rate, attacker always succeeds in catching up, from any disadvantage [9] such as double-spending.

Based on Arthur Gervais's Network, we decide to measure attacker behavior and the three components that forms that behavior by varying the hashrate. This approach is valid and reliable because there is a probability, r, of successful double spend, as a function of the attacker hash rate q and for $q > 0.5$, the attack will always succeed [9].

Furthermore, we decided to use three different transaction values as a secondary measure to see how attacker behavior responds to changes in hashrate for different transaction values. In this scenario, we used the transaction values of 10, 20 and 30 because we would like to see the trend of how increasing transaction values with constant hash rate affects the attacker's behaviors.

Nakamoto [5] had previously anticipated that an attacker with more than 50% computational power would be able to find proof-of-work solution faster than the rest of the network. The attacker would therefore be able to eventually replace the transaction history from an arbitrary point in time [18]. Therefore, we are going to have attacker's hash rate extends beyond 50% to see the impact on attacker's behaviors.

Thus in this experiment, we evaluate (a) the number of double-spending attacker, (b)attacker's income and (c) number of stale blocks based on increasing hash rate ranges from 0.3 to a maximum of 0.6 for each transaction value of 10, 20 and 30 block reward.

IV. RESULTS AND ANALYSIS

Based on the first experiment, for attacker's hash rate ranges from 30% to 60%, the number of double spending attacks are shown in Fig. 4. There are three lines that describes different transaction values equal to 10, 20 and 30 block rewards which are double-spent. For attacker's hash rate > 50%, there is significant increase of the number of double-spending attacks up to 42% at maximum. The higher the transaction values, the higher the number of double-spending attack. The number of double-spending attacks is 8, 15 and 17 for transaction value of 10, 20 and 30 correspondingly. The higher the transaction value, the higher the number of double-spending attacks.

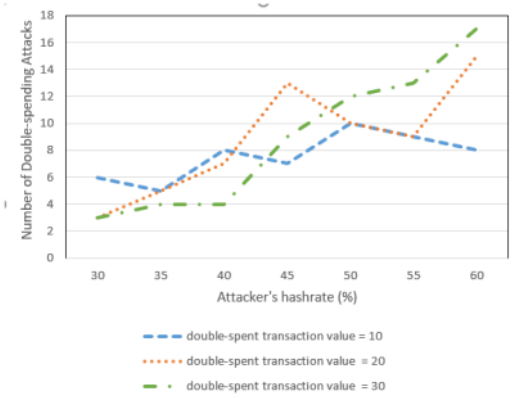

Fig. 4. Attacker's hash rate vs number of double-spending attack

It can be seen from Fig 4, for double-spent transaction value 10 and Attacker's hash rate 0.3, the number of double-spending attacks is 6. While for the same double-spent transaction value with Attacker's hash rate 0.6, the number of double spending attacks is 8. For double-spending transaction value 20, Attacker's hash rate of 0.3 results in 3 double-spending attacks, while Attacker's hash rate 0.6 gives 15 double-spending attacks. It can be concluded that as attacker's hash rate increases, the number of double-spending attacks also increases. Increased attacker's hash rate makes the network prone to double-spending attacks that ultimately lower the blockchain security.

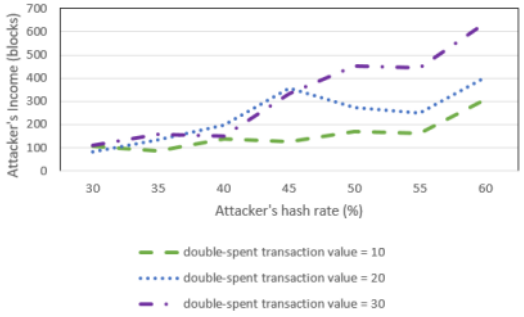

Fig. 5. Attacker's hash rate vs Attacker's Income

For Attacker's hash rate ranges from 30% to 60%, the attacker's incomes are shown in Fig. 5. There are three lines that describe different transaction values equal to 10, 20 and 30 block rewards which are double-spent. For attacker's hash rate > 50%, it shows that on average there are significant increases up to 30% for attacker's income for highest transaction value, e.g. 30. The attacker's income is 310, 406 and 638 for transaction values of 10, 20 and 30

correspondingly. It can be seen from Fig 5. that the higher the Attacker's hash rate, the higher the Attacker's Income. The higher the transaction value, the higher the Attacker's Income.

For Attacker's hash rate ranges from 30% to 60%, the number of stale blocks are shown in Fig 6. There are three lines that describe different transaction values equal 10, 20 and 30 block rewards which are double-spent. The upward trends of number of stale blocks are quite similar throughout the hash rates from 30% to 60%.

Fig 6. shows that with the increase of attacker's hash rate, the number of stale blocks also tend to increase. Number of stale block is obtained from number of overall stale block from all the nodes in the network. Here, it shows that for attacker's hash rate > 50%, the number of stale blocks increases up to 4.5% on average. Number of stale blocks is 129, 128 and 113 for transaction value of 10, 20 and 30 correspondingly. The higher the transaction value, the lower the number of stale blocks.

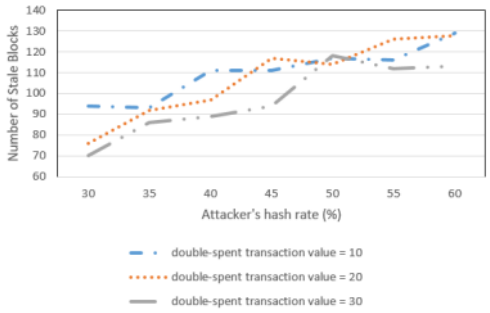

Fig. 6. Attacker's hash rate vs Attacker's Income

V. Summary

In this simulation, we evaluate attacker behaviors such as number of double-spending attacks, attacker's income and number of stale block based on their respective hash rates. Based on the experiment this study has carried out, it shows that three factors of attacker behavior increases with an increasing attacker's hash rate.

The higher the attacker's hash rates, the higher the number of double-spending attacks. The higher the transaction values, the higher the number of double-spending attacks. For attacker's hash rate > 50%, there are significant increase of number of double-spending attack up to 42%.

The higher the attacker's hash rate, the higher the number of attacker's income. The higher the transaction values, the higher the number of attacker's income. For attacker's hash rate > 50%, there are significant increase of attacker's income up to 30%.

The higher the attacker's hash rate, the higher the number of stale blocks. The higher the transaction values, the lower the number of stale blocks. There is an upwards trend for increasing attacker's hash rate.

The importance of this discovery is to show that the defense mechanism of Blockchain technology is vulnerable to the magnitude of attacker hash rate. In hindsight, further study in the area of the level of vulnerability with respect to the level of attacker hash rate is helpful in determining the true level of Blockchain security.

Acknowledgment

We thank Ministry of Research and Higher Education of Republic of Indonesia for financial support for this research under the PTUPT Grant number NKB-1743/UN2.R3.1/HKP.05.00/2019.

References

[1] Y. Yu, R. Liang, and J. Xu, "A Scalable and Extensible Blockchain Architecture," in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, 2018, pp. 161-163.

[2] Arthur Gervais, Ghassan O. Karame, Karl Wust, Vasileios Glykantzis, Hubert Ritzdorf, and S. Capkum, "On the security and performance of proof of work blockchain," in *CCS'16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 2016, pp. 3-16: ACM.

[3] P. K. Kaushal, A. Bagga, and R. Sobti, "Evolution of bitcoin and security risk in bitcoin wallets," in *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, 2017, pp. 172-177.

[4] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, S. J. A. T. o. I. Čapkun, and S. Security, "Misbehavior in bitcoin: A study of double-spending and accountability," vol. 18, no. 1, p. 2, 2015.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[6] S. G. Iyer and A. D. Pawar, "GPU and CPU Accelerated Mining of Cryptocurrencies and their Financial Analysis," in *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on*, 2018, pp. 599-604.

[7] R. Patel, A. Sethia, and S. Patil, "Blockchain – Future of Decentralized Systems," in *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, 2018, pp. 369-374.

[8] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access,* vol. 7, pp. 22328-22370, 2019.

[9] M. Rosenfeld, "Analysis of hashrate-based double spending," vol. arXiv preprint arXiv:1402.2009, 2014.

[10] N. Kaaniche and M. Laurent, "A blockchain-based data usage auditing architecture with enhanced privacy and availability," in *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*, 2017, pp. 1-5: IEEE.

[11] C. Lee, L. Nkenyereye, N. Sung, and J. Song, "Towards a Blockchain-enabled IoT Platform using

oneM2M Standards," in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, 2018, pp. 97-102: IEEE.

[12] I. G. A. K. Gemeliarana and R. F. Sari, "Evaluation of Proof of Work (PoW) Blockchain Security Network on Selfish Mining."

[13] S. S. Hazari and Q. H. Mahmoud, "A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0916-0921.

[14] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM,* vol. 61, no. 7, pp. 95-102, 2018.

[15] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries," in *Proceedings of WEIS*, 2013, vol. 2013, p. 11.

[16] D. Bradbury, "The problem with Bitcoin," *Computer Fraud & Security,* vol. November 2013, no. 11, pp. 5-8, 2013.

[17] F. Ritz and A. Zugenmaier, "The Impact of Uncle Rewards on Selfish Mining in Ethereum," in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2018, pp. 50-57.

[18] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *IEEE P2P 2013 Proceedings*, 2013, pp. 1-10.

[19] S. Shalini and H. Santhi, "A Survey on Various Attacks in Bitcoin and Cryptocurrency," in *2019 International Conference on Communication and Signal Processing (ICCSP)*, 2019, pp. 0220-0224: IEEE.