J Inf Process Syst, Vol.16, No.3, pp.699~717, June 2020
https://doi.org/10.3745/JIPS.03.0140

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

The Dilemma of Parameterizing Propagation Time in Blockchain P2P Network

Sandi Rahmadika*, Siwan Noh*, Kyeongmo Lee*, Bruno Joachim Kweka*, and Kyung-Hyune Rhee**

Abstract

Propagation time on permissionless blockchain plays a significant role in terms of stability and performance in the decentralized systems. A large number of activities are disseminated to the whole nodes in the decentralized peer-to-peer network, thus causing propagation delay. The stability of the system is our concern in the first place. The propagation delay opens up opportunities for attackers to apply their protocol. Either by accelerating or decelerating the propagation time directly without proper calculation, it brings numerous negative impacts to the entire blockchain system. In this paper, we thoroughly review and elaborate on several parameters related to the propagation time in such a system. We describe our findings in terms of data communication, transaction propagation, and the possibility of an interference attack that caused an extra propagation time. Furthermore, we present the influence of block size, consensus, and blockchain scalability, including the relation of parameters. In the last session, we remark several points associated with the propagation time and use cases to avoid dilemmas in the light of the experiments and literary works.

Keywords

Blockchain, Block Size, Decentralized System, Peer-to-Peer Network, Transaction Propagation

1. Introduction

The popularity of blockchain technology through the emergence of Bitcoin and Ethereum has introduced the decentralized cryptocurrency era to the public rapidly. The nature of blockchain changes digital assets via an online transaction system faster and easier. The core principle of blockchain can be further utilized than what has been applied in the current Bitcoin and Ethereum [1]. The majority of the financial structure such as the online trading system is still in the centralized form. It counts on a middleman (conventional bank) to manage every transaction that occurs. Meanwhile, a blockchain technology automatically eliminates the single failure issues caused by the middleman since the third parties are not involved in the decentralized system. Transaction costs also can be reduced since the system does no longer rely on human intervention. Furthermore, blockchain simplifies the complicated administrative processes through a smart contract among the contract stakeholders.

By design, blockchain is inherently resistant to data modification known as a tamper-proof property. Data stored in the blockchain database cannot be changed or manipulated by the attacker as far as they

Manuscript received December 31, 2018; first revision July 10, 2019; accepted July 31, 2019.

Corresponding Author: Kyung-Hyune Rhee (khrhee@pknu.ac.kr)

* Interdisciplinary Program of Information Security, Graduate School, Pukyong National University, Busan, Korea (sandika, nosiwan, dlrud 2531, drbruno@pukyong.ac.kr)

** Dept. of IT Convergence and Application Engineering, Pukyong National University, Busan, Korea (khrhee@pknu.ac.kr)

do not have 50% of the total mining power in the same blockchain network. Due to these merits, blockchain technology is widely applied in various fields of science such as digital identity, distributed cloud storage, decentralized energy trading [2], supply chain [3], digital healthcare [4], digital forensics [5], satellite communication [6], and to name a few.

Every transaction that occurs within the blockchain network results in propagation delay. The large propagation time in such a system can be one of the obstacles that lead to the inability of the blockchain to achieve high scalability [7]. Numerous researches have been proposed to tackle the scalability issue in the blockchain system by parameterizing the protocol version, adjusting the frequency, mining diversity, block sizing, and sharding techniques. Eyal and Sirer [8] introduce Bitcoin-NG (Next Generation) as a new blockchain protocol. This mechanism aims to overcome the issues of scalability in the blockchain system. This protocol uses Byzantine fault tolerance (BFT) which is robust to extreme churn conditions on the same trust model as many existing blockchain platforms. The proposed model shows that it is possible to improve the scalability of blockchain. However, the security aspects are necessary to be explored further.

Another protocol called Proof-of-Luck is presented by Milutinovic et al. [9] as a new consensus protocol which provides low-latency validation and equitably distributed mining. The low-latency transaction validation of consensus protocol in the P2P network straightly affects the propagation time. However, the changes bring new security challenges. Pappalardo et al. [10] conduct the research to observe transactions broadcasted within the Bitcoin network. Many factors that cause this to happen including block propagation time. Similar objective researches with the different mechanism are described by [11-13]. The aforementioned researches provide essential information about block propagation time in the blockchain network.

In this research, we describe the paramount information related to the block propagation time within the blockchain peer-to-peer (P2P) architecture along with some other influential parameters in accordance with our observations and works of literature. The performance of an attack caused by block propagation time is also discussed to determine the extent of the impact generated by propagation time. The relationship between the parameters is elaborated since it is crucial in maintaining the security of the decentralized blockchain system. In addition, we present a use case design by applying off-chain solutions to avoid the dilemmas in parameterizing block propagation time. Intuitively, this use case is applied to the electronic medical records stored in a cloud server. We provide collaboration between blockchain with access control architecture. Our solution does not incur any transaction processing burdens or fees.

Section 2 explores the structure of blockchain with a peer-to-peer network topology as well as the information of transaction propagation and blockchain parameter measurement. The influence of block size within the blockchain P2P network is given in Section 3. Whilst, Section 4 presents our observations and the dilemma of parameterizing propagation time and the attack. The use case to avoid the dilemma that apply off-chain solution is described in Section 5, and the future work direction is presented in Section 6. Finally, the conclusions are drawn in Section 7.

2. Blockchain P2P Network

In this section, we explore the transaction propagation in the current blockchain system, likewise its parameters and measurement. We use the structure of the Bitcoin blockchain as our main reference

because most platforms are inspired by following Bitcoin architecture. The purpose of this section is to have knowledge about blockchain parameters in general that affect the transactions on P2P networks. At the end of this section, we outline the essential points that we use as the principal material to be discussed in this paper.

2.1 Transaction Propagation

Blockchain P2P network is network topology and architecture that makes the workload at each node always equal. The nodes are also called as peers. It refers to the address that performs several functions in the network [14]. This concept allows the nodes to exchange and forward the information received to other nodes in the same network. In the case of Bitcoin, whenever a node draws a number of Bitcoin IP addresses, then the node will be able to manage up to 8 outgoing connections with a certain time span. In general, there are two sorts of transactions that are propagated across nodes namely, block and transaction. If the node receives a new notification for the incoming message, the node checks the validity of the block in the first place (see Fig. 1) as follows:

- Block verification, before the block received by Node A is distributed to Node B, Node A must verify on such a block in advance. If the block (consists of many transactions) is confirmed as a valid block, then Node A sends the inventory message to Node B. Conversely, if the block is invalid, then the process cannot be processed.
- Sending inventory message, this message contains information about the block which is owned by the sender. The size of the message inventory is relatively small at around 61 bytes. Through this message, the recipient can easily check the information in order to ensure that the recipient has never received this block beforehand. The structure of the inventory message in general can be seen in Table 1.
- Sending getdata message, when Node B ensures that the inventory message sent by Node A has never been received earlier, Node B sends getdata message to Node A afterward. This message can be interpreted as a data request.
- Sending the block, after accepting the getdata information from Node B, then Node A directly assigns the full block to Node B. This process occurs continuously for every transaction that happens on the blockchain network.

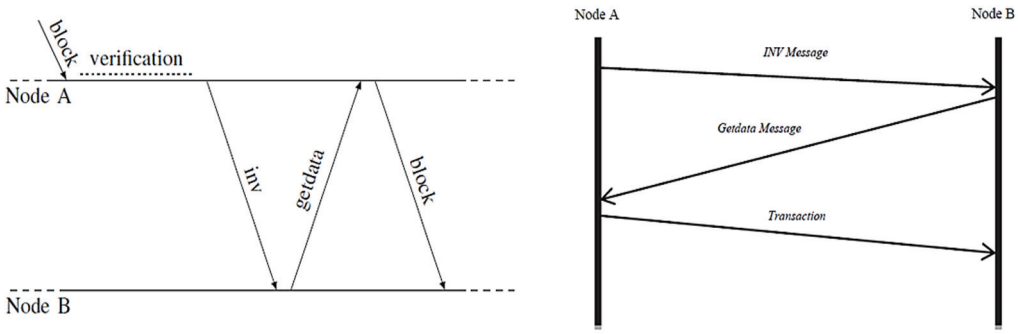

Fig. 1. The message exchanged and distribution protocol (Node A and Node B).

Table 1. Inventory vector message

Size	Definition	Data type	Note
4	type	unit32_t	Determines the object that related to the inventory
32	hash	char(32)	Digest value of the object

2.2 Blockchain Parameter Measurement

There have been extensively recognized studies by measuring the effectiveness of a block propagation in the P2P blockchain network. Commonly, the objective is to figure out the extent of the success of a connection that occurs. Thus, the relation between the numbers of nodes against the block propagation time has become an interesting topic. A statistical data of Bitcoin's P2P network was obtained in 2014 conducted by Hearn [15]. The objective is to gather the connection information from the Bitcoin network. The documentation is publicly available. Surprisingly, the data provided by Feld et al. [16] revealed the cumulated connection attempts and successful connections in the Bitcoin network. The total connection attempt is carried out with 688,281 unique addresses in a span of 16 hours as shown in Fig. 2. The results obtained show that the connection in Bitcoin's peer-to-peer network is not very effective due to only 10,549 addresses of the total addresses are successfully connected and known by other peers (proportion success/attempts is 1.53%). Stated differently, there are several failed connections caused by many factors such as propagation delay, network topology, and block size.

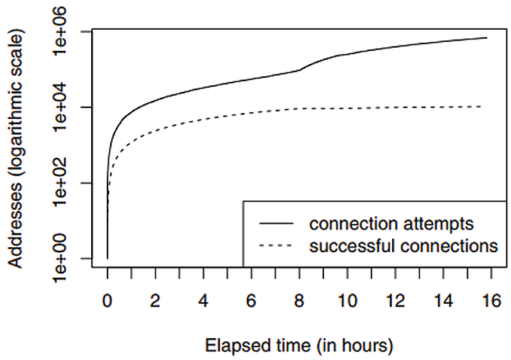

Fig. 2. Cumulated connection attempts and successful connections.

Another similar research was carried out with the goal to achieve a better performance of the block propagation time in the Bitcoin architecture [17]. The authors present a novel model that can cut down transaction time. The results show an improvement by shortening the route of the transaction. However, there is still room for improving the optimal number of clusters by upgrading the network topology of the existing system. In another paper [18], the authors proposed an improvement of propagation time by grouping Bitcoin nodes according to the geographical location (location-based clustering). As a result, the location-based clustering model outperformed the predecessor protocol proposed in [17].

In 2016, an experiment was conducted to determine the relation of the number of parties in the system against the proportion of announcing transaction [19]. The number of nodes for the experiment is set to 14 nodes. Every nodes received the incoming message which is propagated in a blockchain P2P network. The order of nodes is always the same for simulation. In short, node 1 is the first node that receives the

message and continues with node 2 and then forwards to the next node. The transactions are calculated over 1,000 runs. The order of the first four nodes (nodes 1, 2, 3, and 4) received almost all messages sent with proportions around 90 to 100. The last sequence node (node 14) is the lowest node that receives the message. The node 14 only receives 23% of the total messages sent.

The authors [8] proposed a new blockchain protocol to improve scalability as well as to provide better latency and bandwidth. There are two types of blocks in the protocol which is a key block for the election as shown in Fig. 3. In [20], the authors proposed a new Byzantine consensus protocol technique. It uses a scalable collective signing whenever the parties carry out the activities in seconds.

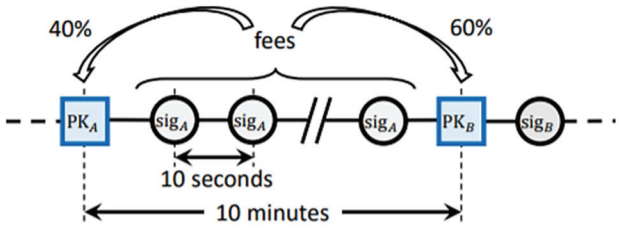

Fig. 3. The structure of the Bitcoin-NG.

Decker and Wattenhofer [21] in 2013 also managed experiments for propagation delay on the blockchain network. Propagation delay can be understood as a combination of the time needed to transmit the transaction and the time used to verify the transaction. The propagation time data in the paper is derived by collecting the information from blockchain height 180,000 to 190,000 and measured it for 60 seconds. Information for each transaction consists of the hash value of the block, the publishing IP nodes, and timestamp. The median time for a peer receiving a transaction is 6.5 seconds, and the mean time is around 12.6 seconds. The propagation time of messages is quite effective until the time reaches 40 seconds, where there are around 5% of peers do not receive the transaction sent.

Based on the experimental data obtained from various literature reviews, the results indicate that there is a strong relationship between the numbers of nodes along with the propagation time against the transaction data in the blockchain P2P network. Therefore, the research about parameters of blockchain has become a research trend for cryptocurrency researchers. The propagation time on the blockchain network is essential since it is directly related to the level of effectiveness in transactions. By considering this factor, we take the block propagation time to be analyzed further in this study. The relationship with other parameters on the blockchain P2P network is also discussed. In the following section, we analyze the impact of propagation delay against the security aspect in the blockchain transactions.

3. Block Size and Its Influences

The block size term in the Bitcoin blockchain can be interpreted as the upper limit of a block within the network to be filled with a number of transactions. A block consists of a bundle of transactions [22]. Every block needs to get verification by the miners before it can be fully accepted to be integrated with the whole block in the network. The characteristic of the block size is different for each blockchain platform. In practice, the maximum block size in Bitcoin stands at 1 MB [23]. The miners have the ability

to select the number of transactions to be processed further. In the case of Bitcoin, whenever the miners commit a transaction that exceeds the upper boundaries, the block will be rejected by the other miners [24]. The objective of determining the size of a block is to tackle the possibility of denial-of-service attacks where the networks are vulnerable. With the maximum limit size of a block is set in such a way, it can reduce motivation for attackers who intend to flood the block with extra meaningless transactions. It can cause various problems such as bottleneck issues.

The propagation time is unable to be separated from the block size. There is a close relationship between the propagation time and the size of the block in a transaction. As mentioned earlier, the more the capacity of a block, the more transactions can be done and stored within the block. Nevertheless, by simply increasing capacity in a block without proper analysis can affect the propagation time that sacrifices security in the blockchain system [25] (we present detail in Section 4). Its correlations are presented in Fig. 4 [26]. The capacity of the block in the transaction is adjusted up to 350 kB to determine the time needed for a node to receive block information. The red line covers 25% of total block size, while the green line covers 60%, and finally, 75% is covered in blue. The simulation results support the theory which stages the more capacity in a block, the longer propagation time needed.

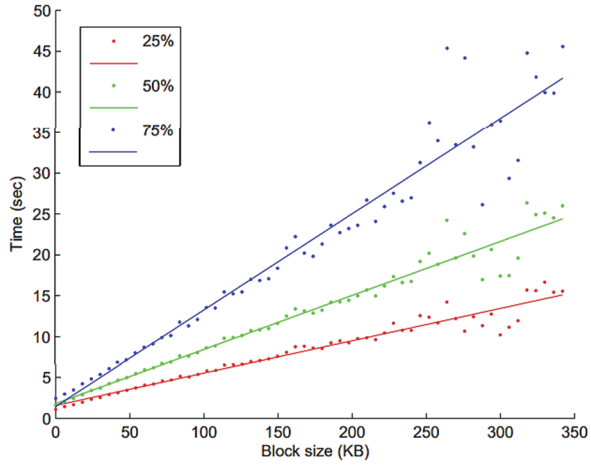

Fig. 4. The relation between the block size and the time.

A deeper analysis of the Bitcoin network by Decker and Wattenhofer [21,27] enlightens some vague points. It provides a lot of essential information about the parameters in the Bitcoin blockchain network. Therefore, it has become the main reference in various studies in the field of blockchain system. The research using a multi-hop broadcast to propagate the transactions and blocks to the entire nodes in the same network. This study confirms that there is a correlation between propagation delay and the size of a block. The authors commented that the primary factor of having a forking in the blockchain is a propagation delay in which also influence attacks to occur such as double spending attack and withholding attack. Finally, the authors proposed a solution by parameterizing the protocol. In practice, the verification time is set up faster than the default protocol. There is also a modification in message exchange on the network. The message received which contains an “inventory message” are then forwarded directly to the connected nodes, along with adopting a star sub-graph structure to the system, it has been proven to increase connectivity speed, blocks verification, and transaction propagation.

The measurements are made on the Bitcoin network by setting up a block size limit up to 140kB. There is a new parameter called “delay cost” to describe the delay time for each kilobyte caused by the dissemination of transactions and blocks between the nodes. The results indicate that for block sizes larger than 20 kB, the cost is stable. Whilst, for the small sizes, are deemed overhead due to the roundtrip delay. The roundtrip delay is influential for small blocks (less than 1 kB) that shows 96% for all transactions. Moreover, the fact shows for blocks larger than 20 kB, each kilobyte costs an additional 80 ms delay until the node detects a transaction.

The capacity in each block straightly influences the length of confirmation. When the nodes select a new transaction to be processed, he is able to check the validity of the information before accepting it as a valid transaction. The length of time to confirm a block depends on the capacity of the block itself. Specifically speaking, the time to validate a block linear to the block capacity. Thus, those parameters are essential in the decentralized blockchain system.

4. Our Findings and Dilemma

We present several selection points in accordance with the predecessor of literature reviews. At the beginning of this section, we describe the results of a withholding attack measurement. This attack is one part among factors as a result of propagation delay in the blockchain network. Simulation of the P2P network is also presented by generating a small decentralized system in order to determine the status of data communication. Based on the parameters used and our findings, we analyze the relationship between them in increasing the level of reliability in the blockchain P2P network. In a quick summarize, there is a trade-off for each decision taken.

4.1 Communication Data of P2P Network

The virtual network is designed based on P2P network computing. The network is built on the top of another network. Nodes in the network can also play more than one role such as miners, clients, and the prosumer. This information is in line with our previous research [28] which is also our ongoing research. Each stored data uses a cryptographic public key standard that is encrypted using a public key and the decryption using a private key which is generated in advance. The key pairs are referred to the consecutive numbers as an integer from a given particular range.

The verification time in our previous experiment is beyond our focus at that time. Likewise, the length of time needed for a transaction to be accepted by all nodes is not our main concern. Specifically speaking, if there is any notification for a new incoming message such as transaction message in the blockchain network, the recipient simply receives the message without verification. The goal is only to measure the status of data communication between nodes in the P2P network. The setting for propagation message between nodes in the P2P network can be seen in Fig. 5.

$$S = \begin{cases} tf, & the\ node\ is\ connected \\ tf + \delta, & the\ node\ is\ not\ connected \end{cases} \quad (1)$$

$$\mathrm{E[s]} = (1 - Qc)tf + Qc(tf + \delta) = \mathrm{tf} + Qc.\delta \quad (2)$$

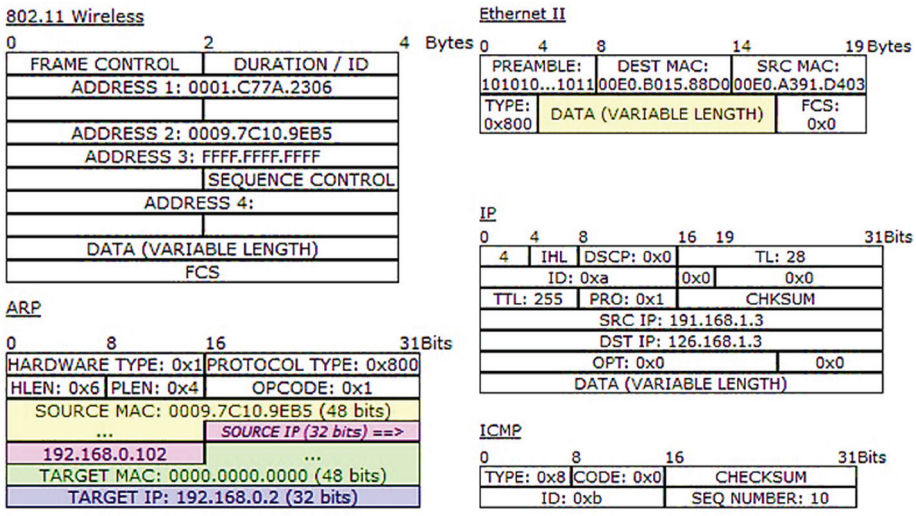

Fig. 5. The parameter settings in the peer-to-peer network.

Table 2. Inventory vector message

Source	Destination	Type	Last Status
PC_A05	LP_T21	ICMP	Successful
PC_B33	PC_A17	ICMP	Successful
PC_A06	PC_A07	ICMP	Successful
PC_A11	LP_T01	ICMP	Successful
LP_T32	PC_A06	ICMP	Successful
PC_A15	PC_A05	ICMP	Failed
PC_A03	LP_R05	ICMP	Failed
PC_A06	LP_R04	ICMP	Successful
PC_A07	PC_A09	ICMP	Failed
PC_A09	LP_A08	ICMP	Successful
LP_A06	PC_A13	ICMP	Successful
…	…	…	…

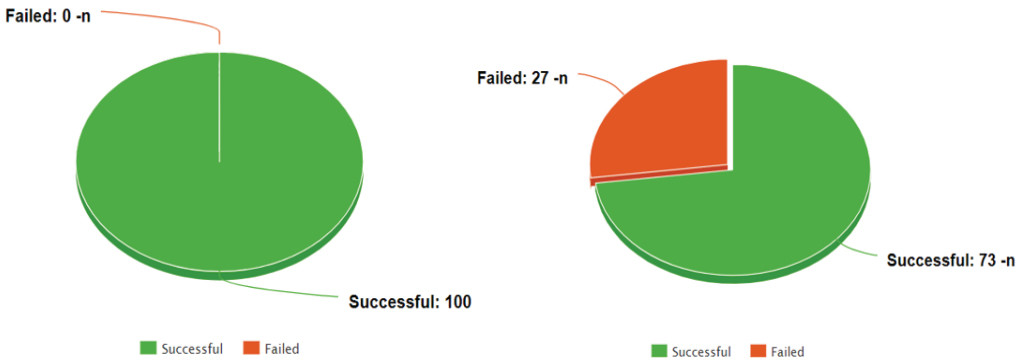

Fig. 6. The setting of propagation message in the P2P network. Regularly every *n* seconds (left) and rapid propagation (right).

A protocol called "Chord-based distributed system" is implemented to manage the value of the node such as "edit data keys", "insert objects", and so forth. Define t_f as a time to do the service in the P2P network. A request coming from other nodes in the same network which is randomly selected. The service time s_t can be defined in formula (1). When a new command notification appears, the node allows making a connection directly based on address linkage with the probability Qc. The average value of service time is defined in (2). The network settings use an open cache solution that aim to achieve a better performance and ensure each node in the network following the Chord protocol.

The new messages are committed by broadcasting 100 transactions to the blockchain network. The source and the destination address for every transaction are chosen randomly. The number of nodes listed to be 25, all of which use the same protocol and capabilities with different addresses. Each node only serves to receive information about messages sent without the need to verify the message received. The results of data communication obtained from the distribution of transactions in the P2P network are shown in Table 2 and Fig. 6. The data from Table 2 is selected randomly at a particular time with a total of 100 rows of data. In general, the deployment of unverified transactions requires an average of 1:14 ms for every 100 bytes of Internet control message protocol echos (ICMP). Transaction data is distributed to all random nodes in two different ways as follows:

- **Regularly every n seconds.** A total of 100 new transactions are sent regularly for every 10 seconds. The node which roles as a sender and a recipient are chosen randomly. There are no special requirements and setup to be the sender and the recipient. The results of the data show that the propagation of transactions is successfully sent to all nodes within the network (see Fig. 6) with the success rate reaching 100%. In this sense, there is no lost data transaction nor unknown transaction to the nodes.
- **Rapid sending transaction.** The propagation message using this method is slightly different from the regular distribution of every n second. The amount of 100 transactions data are sent very quickly (n < 10 seconds) to the node within the P2P network. Senders and recipients are chosen randomly based on the available list. This illustrates the number of new transaction notifications received by certain nodes which can result in loss of transaction data caused by many factors.

4.2 Orphaned Blocks, the Attack, and the Dilemma

An orphaned block is an unwanted event for every miner on the blockchain. The main cause of orphaned block is propagation time on P2P networks. Miners do not get rewards for each orphaned block and stale even though the transactions are successfully mined. Orphaned blocks are described as a block that loses the parent block. Whereas stale blocks are defined as a valid block but are not the main chain in the blockchain network as shown in Fig. 7. That is because the Bitcoin blockchain using the "tie-breaking protocol", where if there are two transactions that are the same for a certain time interval, the miner only accepts the block with the longest transaction chain. In other words, the miner rejects the block which results in loss of reward from mining activities. Thus, orphaned and stale blocks are avoided by the miners. It gets worse since the miners who are mining on orphaned blocks only wasting the resources without any profits at all.

$$\frac{(1-\gamma)}{(3-2\gamma)} \leq \alpha \ \frac{1}{2} \tag{3}$$

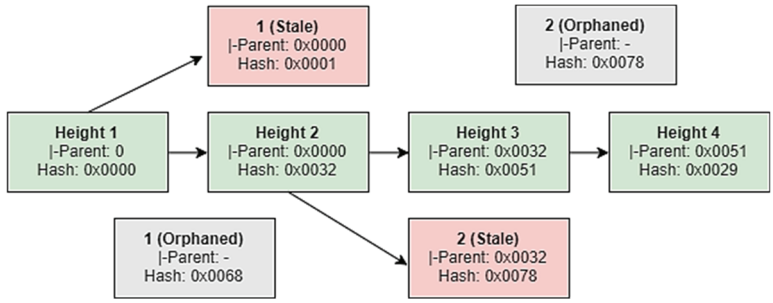

Fig. 7. The setting of propagation message in the P2P network.

We conduct measurements to find out information about orphaned blocks by adopting the attack algorithm called withholding attack strategy. It was outlined in 2014. In this research, we only present the essential part of withholding attacks. However, we suggest the readers refer to literatures [29-31]. The motivation of withholding attack is to compete with honest miners in solving the proof-of-work puzzle until the attacker nodes outperform the honest nodes. For certain circumstances, the attacker nodes do not have any reward since the blocks are kept secret in their network. The transaction cannot be mined cause it is not available for the public. As a result, the rewards vanish if the attackers do not publish the blocks. As the nature of blockchain, the miners get the reward as long as the block found is broadcasted to the public and get confirmed by other miners within the network [32].

In the P2P network, there are the honest node dan the attacker node. The honest node follows the standard blockchain protocol, whilst the attacker node adapts the withholding strategy which is depicted in Fig. 8. We set the mining power of the attackers constant at 30% of the total mining power available on the network. By design, blockchain is assuming secure as long as honest network possesses more than a half of total mining in the network (secure $\gamma > 50\%$). The assumption is refuted by selfish mining attack which enables to gain the revenue even though they only have less than 50% of computing power ($0 \leq \alpha \leq 0.5$) [33]. Therefore, various methods are proposed to prevent this attack such as re-parameterized the value of the threshold for each parameter as can be seen in (3).

```
if (delta_prev == 0)
and (self.secretLength == 2):
  self.announce_block (self.chain_head)
    self.secretLength = 0 self.mine_block ()if delta_prev
  <=0:
  self.chain_head = hash (t_block) self.secretLength = 0 elif delta_prev == 1:
   self.announce_block (self.chain_head) elif delta_prev == 2:
     self.announce_block (self.chain_head) self.secretLength = 0
  else
  :
    iter_hash = self.chain_head temp = 0
```

Fig. 8. Withholding attack strategy.

The simulation is carried out in order to know the performance of dishonest miners (in withholding attack) that follow their strategy in finding a new block. The goal is to explore the new block until the dishonest network becoming the longest chain in the public network. For that reason, dishonest miners can increase their reward after broadcasting it to the public network. In our setting, we manage the selfish miners to be able to compete with honest miners within 14 days to solve the mining puzzle and explore a new block. The computing power of the selfish mining network is 0.4 out of 1.0. The process is running randomly from 0.0 up to 0.4 for 14 days simulation as shown in Figs. 9 and 10.

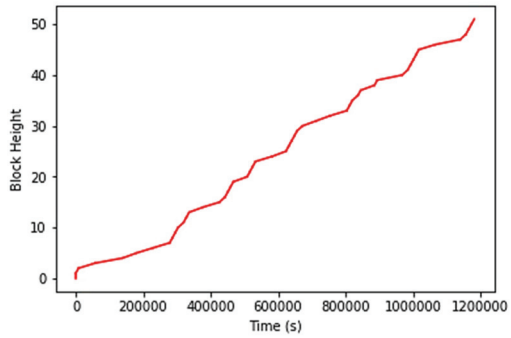

Fig. 9. Block height against time in the blockchain P2P network.

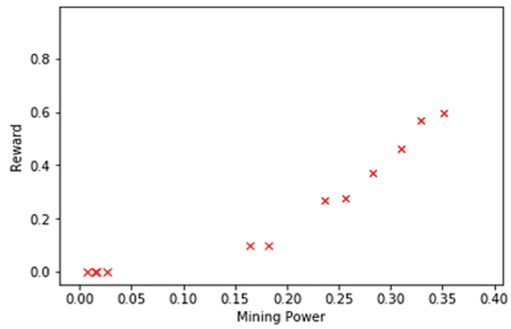

Fig. 10. The performance of withholding attack strategy.

There exist 12 nodes of dishonest miners with computing power varied from 0.0 up to 0.4 (Table 3). We set the upper bound of mining power to be 0.4 (40% of the total network available). Based on the simulation result, with computing power 0.322, it is enough to get unfair revenue compared to the honest protocol. In general, 51 new blocks are successfully added, yet there exist 4 orphaned blocks. The average of block generation time is 7.72 minutes.

So far, we have discussed the fundamental marks associated with blockchain parameters that affect the performance in its application. The remarks are based on our implementation and several works of literature. Nevertheless, numerous papers have been published to address the propagation issues in the P2P network architecture. Some techniques suggest replacing network topology and changing the verification time to a minimum. The message exchange protocol (upgraded version) can be a solution that needs to be considered. Substantially, adjusting propagation time directly into the system can affect the other parameters [34,35].

In the article [36] the authors explained how the propagation delay perpetuates attacks on the Bitcoin network. For instance, the IP address hijacking less than 900 IP address then an adversary can partition the network or control the delay of block propagation. It has led to miners to waste their computation power, revenue loss and influencing the double-spending attacks. However, an encryption mechanism was proposed to prevent the attacker from a secret look into the open connection.

There are many deliberations in increasing the effectiveness and performance of the current blockchain system. By considering at this point, we select the block propagation time and block size parameters to be discussed thoroughly. As an concise summary, Fig. 11 depicts the overall points of parameter consideration. The merits and drawbacks of parameterizing the block propagation and and block size are described as follows:

Table 3. Performance of withholding attack

No.	Dishonest miner	Mining power	Revenue (ratio)	SM Succeed? (Y/N)
1	Miner 1	0.009	0.000	N
2	Miner 2	0.018	0.000	N
3	Miner 3	0.019	0.000	N
4	Miner 4	0.027	0.000	N
5	Miner 5	0.161	0.112	N
6	Miner 6	0.181	0.112	N
7	Miner 7	0.238	0.212	N
8	Miner 8	0.259	0.215	N
9	Miner 9	0.287	0.388	N
10	Miner 10	0.322	0.425	Y
11	Miner 11	0.333	0.457	Y
12	Miner 12	0.361	0.597	Y

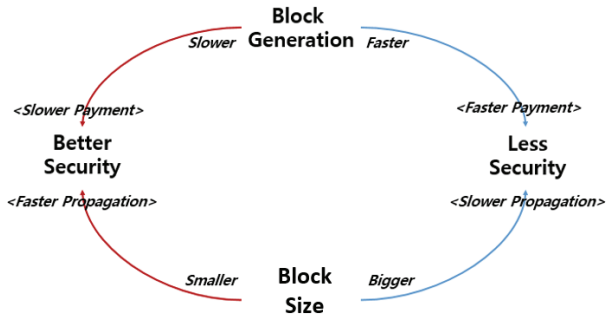

Fig. 11. The setting of propagation message in the blockchain P2P network.

Block generation and propagation

- Speeding up the block generation and propagation: The propagation time can be defined as the length of the transaction distribution added by time to verify each transaction before the miners accepting it. In theory, if the block generation time can be set as quickly as possible, it will benefit the miners in conducting validation so that each party will complete the transaction quickly [37]. However, the issues occur when the block generation time is accelerated without considering other parameters. For instance, the orphaned blocks will appear that open the door to various other types of attacks. In this matter, the miners receive a lot of unconfirmed transactions that lead the possibility to accept the same transaction more than once. As we mentioned earlier, the *tie-breaking* protocol in Bitcoin blockchain regulates each miner/recipient to accept only one valid block. Even though the miners receive the blocks from honest miners, still he is only able to accept one of many. The protocol requires choosing the longest chain. The worst part goes to the rejected blocks that later become the orphaned blocks. A large number of orphaned blocks motivate rational miners to follow the protocol of dishonest miners.
- Cutback the block generation time: By decelerated the block generation time for all transactions occur, the number of transactions that can be verified at the same time will be reduced. Fortunately, it provides some merits such as providing a better blockchain security system. By decreasing the number of orphaned blocks in the network, it will get rid of the selfish mining attacks directly.

Parameterizing the block size

- Increasing the block size: The larger capacity in a block, the more activities can be contained in it.

However, the bigger capacity in a block leads to the slower propagation and verification time [38]. Decelerated propagation time in the P2P blockchain network also causes to a double-spending attack that allows malicious parties using the same coin for more than once. Since the distribution transaction or block is very slow, the whole node cannot receive all transactions while the other nodes one step ahead in the verifying process for those transactions. Due to these differences, it is possible for malicious parties to double-spend their funds because some nodes are not familiar with the confirmed transaction.

- Downsizing the capacity of block: Since only a few transactions can be accommodated by a block, this will accelerate the block generation and propagation delay. Without proper calculation, it brings many drawbacks. The chosen of this strategy can result in the appearance of an orphaned block in the P2P network. This is not desirable because the orphaned block is the forerunner of withholding attacks that endanger the blockchain system. However, the good thing is that the system will provide fast transactions on the blockchain network.

5. Use Cases to Avoid Dilemma

The development of Internet of Things (IoT) devices helps people to generate a large amount of data in their daily lives. A health monitoring service is one of the use cases in big data applications. In a healthcare monitoring system, patients generate personal health information from wearable devices and smart home appliances, then send the collected data to the doctors via a secure channel, all in the pursuit of improving their overall health. Many researchers consider the use of an intermediary for person-to-person or person-to-business trading as a personal information marketplace [39,40] for data exchanges.

The easiest way to implement a personal data sharing system is by allowing direct sharing between the data owner and the data requester without the participation of a third party [41,42]. However, within the personal information marketplace, a direct sharing method is not appropriate because of the data management burden it places on the data owner. For instance, to provide personal information for requesters, the data owner should maintain a secure channel with a shared secret key to transfer his data securely. Moreover, the data owner should perform the encryption process multiple times with different shared secret keys and convert his data into ciphertexts for multiple requesters.

Therefore, to reduce the management burden, we can consider two approaches. First, we use a cloud server to separate the data management task from the data owner. In general, the data are stored in a semi-trusted third-party server; the server administrator can access this data without the permission of the data owner. Accordingly, to overcome the above problem, the data owner can encrypt his data under his secret key before storing it in the cloud server. The easiest way to share encrypted data with other users is to create a shared secret key. However, this method, as mentioned earlier, puts pressure on the data owner to perform the encryption process multiple times for requester. In this paper, we use a proxy re-encryption scheme [43,44] as a solution to this problem.

In [43], the authors introduced a proxy re-encryption (PRE) scheme. The data owner generates a proxy re-encryption key to transform the ciphertext under their public key to the public key of the requester, then gives it to the proxy. However, when the data requester colludes with the proxy, their scheme cannot protect the private key of the data owner from attackers. In [45], the authors proposed a certificateless PRE scheme based on bilinear pairing. The proposed scheme can prevent the proxy from launching a coordinated attack and provides security against the chosen ciphertext attack. Even if the requester colludes with the cloud server, they cannot reveal the private key of the data owner.

The second approach is to use a Kerberos protocol [46] as an authentication method in the data sharing system to improve management efficiencies. A client who wants to access the service sends a request message for authorization. Only authorized clients can receive the ticket via secure, as shown in Fig. 12.

However, the Kerberos authentication protocol uses a session key based communication to authenticate users and manage the ticket. Therefore, the management burden of the data owner remains. Moreover, when the Kerberos server (i.e., data owner) is down, new users cannot access the service until the server is restored (single point of failure). Thus, we consider using blockchain technology to provide management efficiencies without the use of a trusted third-party entity.

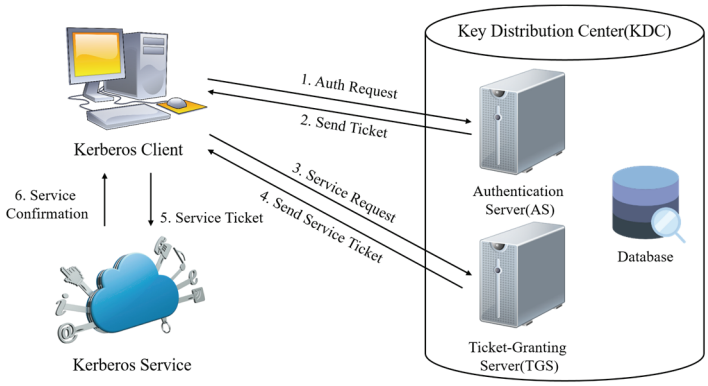

Fig. 12. The architecture of Kerberos service.

As we mentioned earlier, the blockchain consists of consecutive blocks in which each block contains a hash value of the previous block and transactions. Transactions created by users are propagated to P2P networks, and nodes in the blockchain network propagate received transactions after completing a validation process. If the transaction is invalid, it cannot be forwarded to the blockchain network anymore. Moreover, nodes store a copy of the blockchain to their local storage database. If someone wants to modify data on the blockchain, a specific value in the block header must be changed entirely. Thus, it is not possible without the alteration of all subsequent block headers for all users in the network. The immutability and transparency of stored data in blockchain is used to build a decentralized system in a variety of areas such as finance, food, health, etc. As a result, applying the blockchain to the data sharing system makes it possible to manage credentials for the requester without a centralized administrator.

The first distributed blockchain was conceptualized by Nakamoto [47] and it was implemented as a bitcoin, an essential component of cryptocurrencies, in the following year. In a bitcoin payment system, users create a transaction to transfer their funds with their signature to prove the ownership of the consumed funds. Nodes verify these transactions based on the validity of the attached signature and the previous transaction stored in the blockchain. The transaction can only be disseminated by network members if the transaction has a valid signature and the output of the previous transaction is unspent.

The objective of a blockchain-based access control system [48-50] is similar to operating principle behind the transfer of funds in a bitcoin payment system. In [48,50], each activity provides access to rights and policies. In contrast to the Kerberos protocol, all transactions are publicly visible on the blockchain, as shown in Fig. 13. In [49], the authors proposed blockchain-based data sharing for electronic medical records stored in a cloud server. Verifiers can verify the membership of a user by using cryptographic keys that are generated by the issuer before storing the request to the blockchain. Therefore, all users can efficiently manage their data without the help of a third party.

However, verifiers do not consider user privacy and the limited throughput of the public blockchain. A public blockchain system has a maximum capacity due to the constant interval and the limited block size. In the case of the Bitcoin payment system, it can only process seven transactions per second. The number of confirmed Bitcoin transactions per day has been increased by 150,000 over the past 5 years. For this reason, many cryptocurrency developers consider re-parameterization (i.e., modify system

parameters) to enhance the throughput of a blockchain network. However, Croman et al. [7] show that such scaling by re-parameterization can achieve only limited benefits. For instance, an increase in the block size leads to a propagation delay, along with an increased blockchain fork rate [21]. Therefore, to solve the low-latency problem in the blockchain system, we can use a payment channel [51,52]. Two parties establish point-to-point channels between each other and exchange their balance states on the off-chain (i.e., outside of the blockchain network). In the payment channel, users do not need to wait for the transaction confirmation. Unlike the original bitcoin payment system, both parties exchange their balance state as an off-chain transaction until the channel is closed without broadcasting it. In the payment channel, only the most recent state (i.e., off-chain transaction) is valid.

The blockchain access control system recorded the credentials of the requester in the public blockchain to ensure that the user was authorized. The practical scheme can be seen in Fig. 13. However, in environments where certification tickets for access to data are regularly updated as considered in this paper, the number of renewals raises the transaction processing overhead. Bitcoin transactions consist of input and output fields. Input fields include a hash value, public keys, signatures, and output fields include the address of the recipient. The system requires the consumption of the output of existing tickets to generate transactions that include a new access policy to update tickets. However, this puts the burden on the blockchain network and the transaction processing fee on the user. In contrast, in the payment channel based system, the size of transactions recorded on-chain is fixed (614 Byte), regardless of the number of renewals for tickets. The size of transactions recorded on off-chain increases with the number of renewals in the ticket, but this is handled outside the blockchain and therefore does not incur any transaction processing burdens or fees.

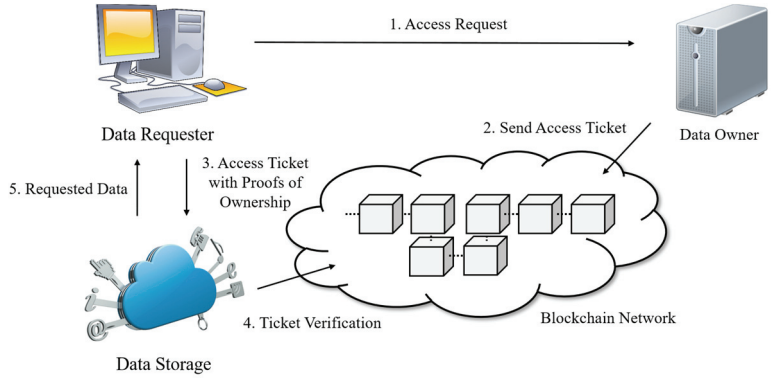

Fig. 13. Blockchain-based access control system.

6. Future Work Direction

The decentralized application based on blockchain technology is growing due to its advantages. The most prominent properties are tamper-proof, no third party involvement, and reduce the operating costs. Therefore, the systems based on blockchain technology are widely adopted in diverse fields of use cases such as healthcare, e-voting, digital identity, and so forth. However, the development of this technology faces many challenges, especially related to blockchain parameters that can be changed according to its application. In the previous sections, we discussed the impacts that would occur if blockchain parameters re-parameterized without proper calculation. It can affect the stability of the blockchain system and can be the forerunner to various attacks such as withholding attack and double-spending attack. Taking into account these factors, for future work direction requires a depth-analysis for the overall parameters of the

blockchain (excluding the propagation time and block size parameters). Meanwhile, the relationship between propagation time and block size indicates that there is a strong relationship between them. There are pros and cons for every decision taken (by not following the existing default setting of a blockchain platform). Thus, we suggest that blockchain users and developers also consider the remarks we have presented in this paper.

7. Conclusions

In this paper, we provide essential information regarding on the parameters and restrictions that influence the propagation delay in the blockchain P2P network topology. We discussed the performance of an attack which might occur due to propagation time issues. Based on our implementation along with the information from several works of literature, we conclude that the enhancement of the performance of the decentralized blockchain in the P2P network topology requires a very articulated analysis since it is directly affected to its security. The trade-off between the performance and security needs to be carefully considered before being applied in the real-world application. For further research, a new design protocol which is secure and faster in terms of managing every blockchain transaction is a necessity. Our which is in the initial stage of achieving a better blockchain protocol.

Acknowledgement

This work was supported by a Research Grant of Pukyong National University in 2019.

References

[1] V. Gramoli, "From blockchain consensus back to byzantine consensus," *Future Generation Computer Systems*, vol.107, pp. 760-769, 2020.

[2] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840-852, 2016.

[3] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18-27, 2018.

[4] S. Rahmadika and K. H. Rhee, "Toward privacy-preserving shared storage in untrusted blockchain P2P networks," *Wireless Communications and Mobile Computing*, vol. 2019, article no. 6219868, 2019.

[5] A. H. Lone and R. N. Mir, "Forensic-chain: Ethereum blockchain based digital forensics chain of custody," *Scientific and Practical Cyber Security Journal*, vol. 1, no. 2, pp. 21-27, 2018.

[6] S. Wei, S. Li, P. Liu, and M. Liu, "BAVP: blockchain-based access verification protocol in LEO constellation using IBE keys," *Security and Communication Networks*, vol. 2018, article no. 7202806, 2018.

[7] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, et al., "On scaling decentralized blockchains," in *Financial Cryptography and Data Security*. Heidelberg: Springer, 2016, pp. 106-125.

[8] I. Eyal and E. G. Sirer, "Bitcoin-NG: a secure, faster, better blockchain," 2015 [Online]. Available: https://hackingdistributed.com/2015/10/14/bitcoin-ng/.

[9] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: an efficient blockchain consensus protocol," in *Proceedings of the 1st Workshop on System Software for Trusted Execution*, Trento, Italy, 2016, pp. 1-6.

[10] G. Pappalardo, T. Di Matteo, G. Caldarelli, and T. Aste, "Blockchain inefficiency in the bitcoin peers network," *EPJ Data Science*, vol. 7, article no. 30, 2018.

[11] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 760-763, 2018.
[12] A. Kiayias and G. Panagiotakos, "Speed-security tradeoffs in blockchain protocols," *IACR Cryptology ePrint Archive*, vol. 2015, article no. 1019, 2015.
[13] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal pricing-based edge computing resource management in mobile blockchain," 2017 [Online]. Available: https://arxiv.org/abs/1711.01049.
[14] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," in *Proceedings of the 1st International Conference on Peer-to-Peer Computing*, Linkoping, Sweden, 2001, pp. 101-102.
[15] M. Hearn, "Bitcoinj: a Java implementation of a bitcoin client," 2013 [Online]. Available: https://bitcoinj.github.io/.
[16] S. Feld, M. Schonfeld, and M. Werner, "Analyzing the deployment of Bitcoin's P2P network under an AS-level perspective," *Procedia Computer Science*, vol. 32, pp. 1121-1126, 2014.
[17] M. Fadhil, G. Owenson, and M. Adda, "A bitcoin model for evaluation of clustering to improve propagation delay in bitcoin network," in *Proceedings of 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th International Symposium on Distributed Computing and Applications for Business Engineering (DCABES)*, Paris, France, 2016, pp. 468-475.
[18] M. Fadhil, G. Owenson, and M. Adda, "Locality based approach to improve propagation delay on the bitcoin peer-to-peer network," in *Proceedings of 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, Lisbon, Portugal, 2017, pp. 556-559.
[19] M. Fadhil, G. Owen, and M. Adda, "Bitcoin network measurements for simulation validation and parameterization," in *Proceedings of the 11th International Network Conference – INC2016.* Plymouth, UK: University of Plymouth, 2016, pp. 109-114.
[20] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *Proceedings of the 25th USENIX Security Symposium*, Austin, TX, 2016, pp. 279-296.
[21] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Proceedings of IEEE International Conference on Peer-to-Peer Computing*, Trento, Italy, 2013, pp. 1-10.
[22] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in *Proceedings of 2017 IEEE International Congress on Big Data*, Honolulu, HI, 2017, pp. 557-564.
[23] R. Dennis and G. Owen, "Rep on the block: a next generation reputation system based on the Blockchain," in *Proceedings of 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, 2015, pp. 131-138.
[24] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A taxonomy of blockchain-based systems for architecture design," in *Proceedings of 2017 IEEE International Conference on Software Architecture (ICSA)*, Gothenburg, Sweden, 2017, pp. 243-252.
[25] S. Rahmadika, K. Lee, and K. H. Rhee, "Blockchain-enabled 5G autonomous vehicular networks," in *Proceedings of 2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC)*, Bandung, Indonesia, 2019, pp. 275-280.
[26] Y. Sompolinsky and A. Zohar, "Accelerating Bitcoin's transaction processing: fast money grows on trees, not chains," *IACR Cryptology ePrint Archive*, vol. 2013, article no. 881, 2013.
[27] C. Decker and R. Wattenhofer, "Bitcoin transaction malleability and MtGox," in *Computer Security – ESORICS 2014.* Cham: Springer, 2014, pp. 313-326.
[28] S. Rahmadika and K. H. Rhee, "Blockchain technology for providing an architecture model of decentralized personal health information," *International Journal of Engineering Business Management*, 2018. https://doi.org/10.1177%2F1847979018790589
[29] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *financial Cryptography and Data Security*. Heidelberg: Springer, 2014, pp. 436-454.

[30] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Financial Cryptography and Data Security*. Heidelberg: Springer, 2016, pp. 515-532.

[31] E. Heilman, "One weird trick to stop selfish miners: fresh bitcoins, a solution for the honest miner," in *Financial Cryptography and Data Security*. Heidelberg: Springer, 2014, pp. 161-162.

[32] S. Rahmadika, B. J. Kweka, H. Kim, and K. Rhee, "A scoping review in defend against selfish mining attack in bitcoin," *IT Convergence Practice*, vol. 6, no. 3, pp. 18-26, 2018.

[33] S. Rahmadika and K. H. Rhee, "Preliminary of selfish mining strategy on the decentralized model of personal health information," in *Advanced Multimedia and Ubiquitous Engineering*. Singapore: Springer, 2018, pp. 679-685.

[34] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, "Tampering with the delivery of blocks and transactions in bitcoin," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver, CO, 2015, pp. 692-705.

[35] A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 2016, pp. 3-16.

[36] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: routing attacks on cryptocurrencies," in *Proceedings of 2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2017, pp. 375-392.

[37] R. Khalil and A. Gervais, "Revive: rebalancing off-blockchain payment networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas, TX, 2017, pp. 439-453.

[38] X. Fu, H. Wang, P. Shi, Y. Fu, and Y. Wang, "Jcledger: a blockchain based distributed ledger for JointCloud computing," in *Proceedings of 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, Atlanta, GA, pp. 289-293.

[39] X. Ren, P. London, J. Ziani, and A. Wierman, "Datum: managing data purchasing and data placement in a geo-distributed data market," *IEEE/ACM Transactions on Networking*, vol. 26, no. 2, pp. 893-905, 2018.

[40] S. Spiekermann and J. Korunovska, "Towards a value theory for personal data," *Journal of Information Technology*, vol. 32, no. 1, pp. 62-84, 2017.

[41] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: a strong privacy-preserving scheme against global eavesdropping for ehealth systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 365-378, 2009.

[42] H. Yang, H. Kim, and K. Mtonga, "An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1059-1069, 2015.

[43] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology – EUROCRYPT'98*. Heidelberg: Springer, 1998, pp. 127-144.

[44] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *Proceedings of the 14th ACM conference on Computer and Communications Security*, Alexandria, VA, 2007, pp. 185-194.

[45] C. Sur, C. D. Jung, Y. Park, and K. H. Rhee, "Chosen-ciphertext secure certificateless proxy re-encryption," in *Communications and Multimedia Security*. Heidelberg: Springer, 2010, pp. 214-232.

[46] S. P. Miller, B. C. Neuman, J. I. Schiller, and J. H. Saltzer, "Kerberos authentication and authorization system (*Project Athena Technical Plan, Section E.2.1*)," 1988 [Online]. Available: http://web.mit.edu/Saltzer/www/publications/atp.html.

[47] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008 [Online]. Available: https://git.dhimmel.com/bitcoin-whitepaper/.

[48] A. Ouaddah, A. Abou Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*. Cham: Springer, 2017, pp. 523-533.

[49] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, article no. 44, 2017.

[50] D. Di Francesco Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *Distributed Applications and Interoperable Systems*. Cham: Springer, 2017, pp. 206-220.

[51] J. Poon and T. Dryja, "The bitcoin lightning network: scalable off-chain instant payments," 2016 [Online]. Available: https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf.
[52] G. Gutoski and D. Stebila, "Hierarchical deterministic bitcoin wallets that tolerate key leakage," in *Financial Cryptography and Data Security*. Heidelberg: Springer, 2015, pp. 497-504.

Sandi Rahmadika **https://orcid.org/0000-0002-7848-6579**

He received his Master of Engineering degree from the dual master degree program between Institut Teknologi Bandung (ITB), Indonesia and Pukyong National University (PKNU), South Korea in 2016. He is currently a PhD student in the Laboratory of Information Security and Internet Applications (LISIA), PKNU. His research interests include applied cryptography, privacy-preserving in the decentralized system, and AI with blockchain integration.

Siwan Noh **https://orcid.org/0000-0003-0261-3444**

He received his M.S. degree in Interdisciplinary Program of Information Security from Pukyong National University, Republic of Korea in 2018. He is currently a doctor course student of Pukyong National University. His research interests are related with blockchain, applied cryptography, and communication security.

Kyeongmo Lee **https://orcid.org/0000-0002-2641-9593**

He received his B.S. degree in Computer Science from Credit Bank System, National Institute for Lifelong Education, Republic of Korea in 2016. He is currently a Master candidate in the Laboratory of Information Security and Internet Applications (LISIA), Pukyong National University, Republic of Korea. His research interests include blockchain and its application, Security management, applied cryptography, and network security.

Bruno Joachim Kweka **https://orcid.org/0000-0001-8958-2577**

He received the bachelor's degree of information technology from Kampala International University in 2014. He joined the Pukyong National University for his master's degree of Information Security in 2017. His research interests include design of blockchain application and security as well as IoT with blockchain integration.

Kyung-Hyune Rhee **https://orcid.org/0000-0003-0466-8254**

He received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Republic of Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide, the University of Tokyo, and the University of California, Irvine. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a professor in the Department of IT Convergence and Application Engineering, Pukyong National University, Republic of Korea. His research interests center on key management and its applications, mobile communication security and security evaluation of cryptographic algorithms.