A Scoping Review in Defend Against Selfish Mining Attack in Bitcoin

Sandi Rahmadika[1], Bruno Joachim Kweka[1], Hyunwoo Kim[1], and Kyung-Hyune Rhee[2*]
[1]Interdiscplinary Program of Information Security, Graduate School
Pukyong National University, Busan, Republic of Korea
{sandika, drbruno}@pukyong.ac.kr, kper951@naver.com
[2]Department of IT Convergence and Application Engineering
Pukyong National University, Busan, Republic of Korea
khrhee@pknu.ac.kr

Abstract

Bitcoin is widely adopted due to its popularity as a decentralized cryptocurrency. Regardless of its reputation, Bitcoin has been shown that its protocol is not incentive compatible for the miners. The adversary network enables to gain the unfair revenue by adapting the selfish mining strategy. To do so, the attacker does not have to possess 51% power of the total network. Moreover, this attack affects the rational miner to adopt the selfish mining strategy due to this strategy is more profitable than the honest. Selfish mining will damage the structure of Bitcoin blockchain if the attack continues to occur. The minority of adversary network will increase until becomes a majority network in the Bitcoin blockchain. In this sense, they will be able to take over the network and invalidate the transaction of the parties. In this paper, we thoroughly review the existing defenses against selfish mining strategy. In the last session, we remark several points that related to the strategies to prevent the selfish mining attack based on the prior works of literature.

Keywords: Bitcoin Blockchain, Selfish Mining, Strategy Defense, Unfair Revenue

1 Introduction

Blockchain technology offers to radically transform the way parties exchange the digital asset securely without having to trust the third party nor a central authority [10]. Due to no an intermediary involved in the system, the blockchain automatically gets rid of the single failure (typical of the centralized system) and reduce the transaction cost. The security of blockchain is settled by a chain of cryptographic puzzles which is solved by the miners. The miners get the revenue once they succeed in solving the cryptographic puzzle and adding a new block of the transaction to the main chain [15]. One of the prominent in the adapting of blockchain technology is Bitcoin. In nutshell, Bitcoin blockchain literally is a distributed ledger which is a chronologically ordered chain of blocks protected by solving proof of work [4].

A block of the blockchain contains a set of transactions, a hash value from the previous block, timestamp, block reward, block number and many others. Bitcoin hits a new price $8,211.46 per July 2018 as shown in Figure 1 with the market capitalization is $140,981,877,022 [2]. Hence, the Bitcoin become the highest rank among the other cryptocurrencies such as Ethereum, Litecoin, Dogecoin and to name a few. The Bitcoin cryptocurrency with all of its advantages, however, it has been shown that the Bitcoin protocol is not incentive compatible due to the adversary enables to adapt the selfish mining to get an unfair revenue [7]. More precisely, the adversary does not necessary to have a very large mining

IT CoNvergence PRActice (INPRA), volume: 6, number: 3 (September 2018), pp. 18-26
*Corresponding author: A12-1305, Daeyeon Campus, Pukyong National University, Yongso-ro 45, Nam-gu, Busan (48513), Republic of Korea. Telp: +82 51 6296247, Fax: +82 51 6264887

Figure 1: Bitcoin market value [2]

power to obtain the unfair revenue. The other bad news, based on the optimal selfish mining strategy by Sapirshtein [17], the adversary only needs 23,21% of hash rate by following the selfish mining strategy to obtain the unfair revenue in the Bitcoin blockchain network.

The intuition of selfish mining attack is to keep the finding block secret until their network becomes the longest chain in the Bitcoin network. Whenever the adversaries find a new block, they keep the block secret in their pool. The adversaries publish the block to the public network if the honest network comes close to the adversary network. Once the adversary network reaches the longest chain in a particular network, the adversary will be able to invalidate the transaction of the parties (see Figure 2) It could happen because the Bitcoin relies on the tie-breaking protocol (trusting to the longest chain). Simply, if there are two blocks come to the miner, the longest one will be chosen by the miner. Since the revenue from selfish mining attack is larger than the honest miner, it affects the rational miner to do mining by adapting the selfish mining protocol. Therefore, the strategy is necessary in order to prevent the selfish mining attack in a Bitcoin.

In this paper, we thoroughly elaborate the prior strategies to prevent the selfish mining attack in Bitcoin. The objective of this paper is to provide and explore insight into the selfish mining attack and the strategy to prevent it. Several strategies to prevent the selfish mining attack have been conducted such as [19], [18], [11], and [6]. By considering the comprehensive discussion, we remark several points of strategies to prevent the selfish mining attack based on the prior works of literature.

The roadmap of the paper is organized as follows. Section 2 presents an overview of selfish mining attack in Bitcoin blockchain network, whilst Section III describes in detail about the prior strategies to prevent selfish mining attack. We remark several points in Section IV based on the comprehensive discussion, and finally, some concluding are given in Section V.

2 The Essential of Selfish Mining

Selfish mining attack is crucial in Bitcoin and decentralized cryptocurrency system in general. It affects directly to the integrity of the Bitcoin network. The integrity of system is essential since it is maintaining and assuring accuracy and consistency of data over its entire life-cycle [16]. Since the selfish attack in Bitcoin was discovered in 2014, it attracts tremendous interest among researchers. In the pioneer paper of Bitcoin, Satoshi [12] mentioned that as long as the majority of mining power is controlled by the adversary node, they will generate the longest chain and enable to obtain any unfair advantages. Bitcoin is secure as long as honest nodes collectively control more CPU power than the attacker nodes.

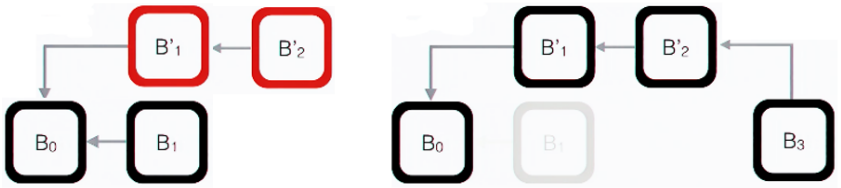

Figure 2: (a) Competing between honest and adversary block; (b) Adversary outpace the honest block

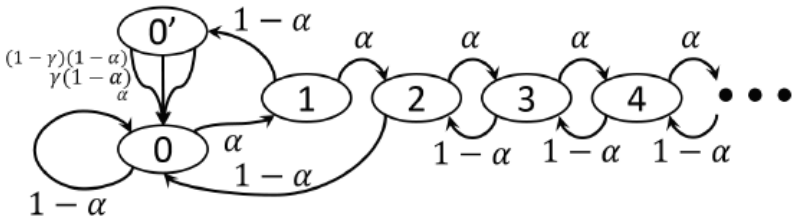

Figure 3: State machine of discovering block [7]

Bitcoin adapted the *tie-breaking protocol* to resolve the fork problem in the network. Bitcoin fork happened during the block propagation time due to an obligation for the miner who finds the block to propagate the block to the entire network. The propagation block of Bitcoin transaction occurs rapidly. Thus, it brings up the chance for the nodes to receive more than one block for the same transaction. In this sense, the node chooses the longest chain with the most accumulated difficulty of proof-of-work. By leveraging the *tie-breaking protocol*, it a bit risky for the parties since the dishonest network has the ability to invalidate and outpace the honest block once they become the longest chain in the Bitcoin network. In order to get a better knowledge about the proof-of-work consensus, we suggest to the reader to refer the [9] literature.

The Bitcoin blockchain as prescribed is assuming secure as long as more than 50+1% of the mining power belongs to the honest miners($\gamma > 50\%$). The assumption of the majority is secure in Bitcoin is refuted by selfish mining attack. The selfish miner still manages to gain the revenue although they have less than 50% of computing power in the network ($0 \leq \alpha \leq 0.5$). Recently, the optimal selfish mining strategy using Markov Decision Process [17] showed that the adversary allows gaining their revenue in the pool with only 23,21% of hash rate. Nayak et al. [13] discovered that the selfish mining is not optimal for a large parameter space, and surprisingly in some cases, the victims of an eclipse attack enable to get any benefit from being eclipsed.

Figure 3 illustrates the state machine of discovering block by the miners. State 0 describes the state where there is no branch, whilst state 0' is the condition where there are two public branches with an average frequency of the hash rate from the attacker α and honest miner $1 - \alpha$. Whenever the selfish miner finds one new block, it increases one block lead. The attacker publishes the block if the honest network comes close to the adversary network. When the adversary keeps the block secret, they get no revenue, but once they publish the block the will get the revenue depends on how many blocks they manage.

The instinct behind the attacker of selfish mining strategy is to keep the new block secret instead publish the block to the public network. Once the adversary's pool outperforms of the honest network, the adversary enables to invalidate the honest block straightforwardly. As the result, the block found by the honest network becomes an orphaned block (stale block). In this regard, if the honest network does mining in the orphaned block, he/she will not get any reward for solving the cryptographic puzzle of

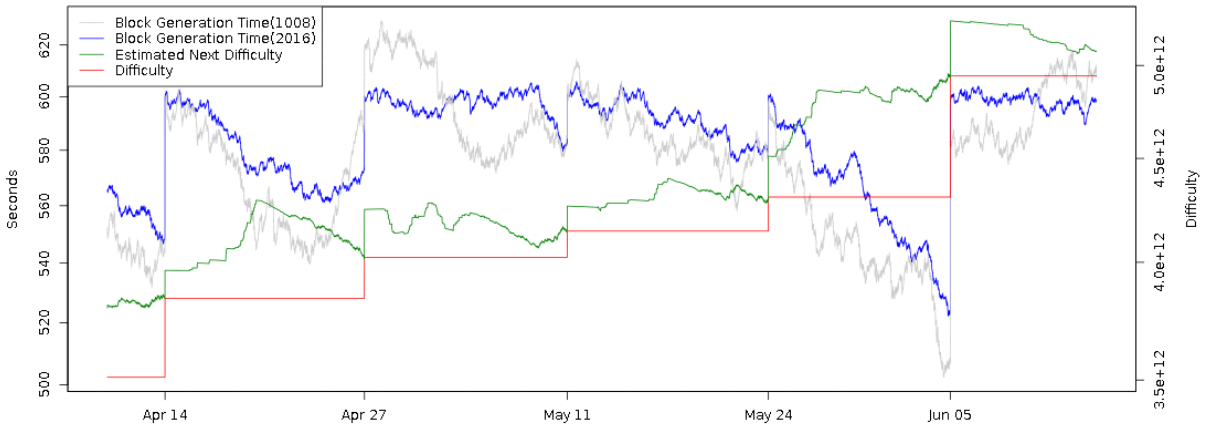

Figure 4: Bitcoin block generation time vs difficulty

proof-of-work. The key insight behind this strategy is to force the honest miners into performing wasted computation on the orphaned block.

3 Existing Defense Against Selfish Mining Attack

Zeroblock model. Solat [18] proposed a solution for the selfish mining attack which is conducted by the dishonest node or selfish nodes in order to either get unfair rewards and waste the resources of the honest miners. The authors introduced *Zeroblock* solution, a strategy to prevent selfish mining using a *free of forgeable timestamps* approach. An *expected time* is essential in this strategy. All of the transactions must be generated and executed by the parties within an *expected time*. In this regard, if the transaction time exceeds the expected time, the transaction becomes an invalid transaction (null block). Due to an invalid block occurs (beyond *expected time*) the honest node in the network creates a dummy block called as *Zeroblock*. The *expected time* depends on the difficulty of proof-of-work consensus and the total size of the network. Currently, the generation block of Bitcoin is around 10 minutes [1]. The red line in Figure 4 presents the difficulty in mining Bitcoin, whilst the green line is the estimated mining for the next puzzle. The average block generation time of 2016 blocks can be seen in the blue line, which is literally known, as a confirmation time.

$$ET = BGT + BT \tag{1}$$

Where:
ET=expected time
BGT=block generation time
BT=block propagation time

Publish or perish strategy. Zhang [19] proposed a backward-compatible defense scheme against the dishonest miner which outperforms of the predecessor similar defense. The original Bitcoin protocol relies on the *fork-resolving policy*, which literally means the node chooses the longest chain whenever the fork occurred. In this sense, the author filed a change in the Bitcoin protocol (*fork-resolving policy*) to choose the heaviest chain instead of the longest chain. By leveraging the proposed scheme, the block found by the dishonest miner that is kept secret until a competing block is broadcasted, it would contribute to neither for both branches. More precisely, the dishonest miner gets no reward by keeping the

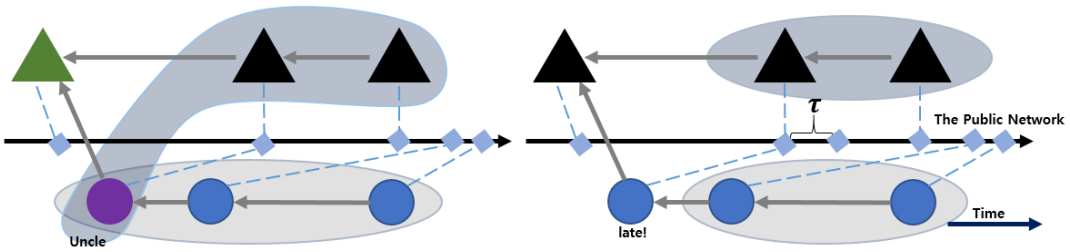

Figure 5: The block found completely nullifies the advantage for the selfish miner

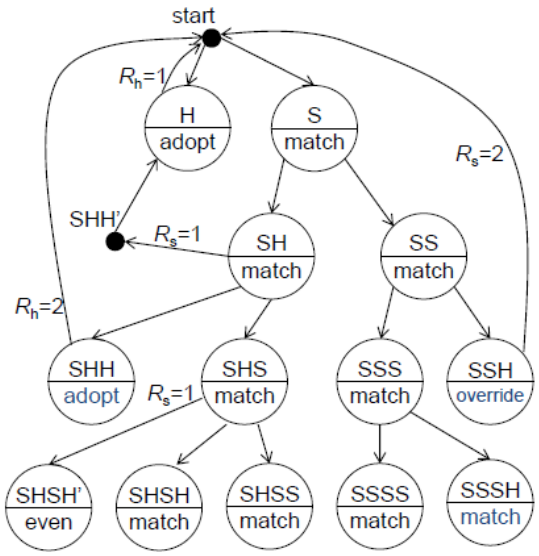

Figure 6: Publish or perish ($\alpha = 0.48$)

block secret nor publish the block to the network (see Fig. 5). Whilst, the relative revenue selfish and honest miner can be defined as follow:

$$\frac{\Sigma Rs}{\Sigma Rs + \Sigma Rh} \tag{2}$$

Rs = Revenue of selfish miner; Rh = Revenue of honest miner

One of the selected results of publish or perish strategy can be found in Figure 6. All the states and transitions of the strategies are written in the first four blocks, which are mined in as a race between honest and dishonest miner. In the state of "SHH", the selfish miner chooses the "adopt" strategy when the honest chain is longer than the selfish chain. As opposed to this strategy, the selfish miner in the uniform tie-breaking defense would choose the "hide" strategy instead of direct give-up and accept an "adopt" strategy. Therefore, the authors claim that publish or perish (backward-compatible) strategy is the first-rate strategy against selfish mining attack in Bitcoin compared with the preceding strategies.

In 2014, Heilman [11] proposed the threshold changes in the Bitcoin protocol. The authors introduce a new mechanism against selfish attack by raising the threshold of hash rate to profitably mining from 25% to 32% under all circumstances. The threshold is re-parametrized as follows:

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

$$threshold of \alpha needed \frac{1-(1-e\frac{1-\alpha}{600})xt}{3-2(1-\frac{1-\alpha}{600})xt} \tag{4}$$

In the case of the value of ratio honest mining power $\gamma = 0.99$ then selfish mining strategy is profitable at 0.9% or $\alpha \leq 0.009$ (it cannot be fixed all γ for all α). In order to prevent selfish mining, the authors also propose *Freshness Preferred* method. It decreases the profitability of selfish mining attack by using unforgeable timestamps to penalize miners that kept the secret block. Eyal [7] actually discovers the selfish mining strategy and propose a simple solution as well to prevent selfish mining attack in Bitcoin by raising the threshold. Accurately, the threshold of honest miner 0.5, which in turn yields a threshold of 0.25. A *fork-punishment rule* model is proposed by Bahack [5]. In this model, the competing blocks get no revenue. Moreover, the first node who consolidates a proof of the block fork in the network gets partly of the forfeited revenue.

4 Some Remarks

We elaborate on the prominent strategies to prevent selfish mining attack in the Bitcoin. The scenario of this attack may result in a situation where the selfish mining chain becomes a majority of the public blockchain. This will collapse bitcoin's decentralized nature and a selfish pool manager will control the system. The literature reviews were thoroughly discussed and the papers were carefully chosen from the scholarly paper. Since the selfish mining attack was first discovered in 2014, it attracted a lot of attention among researchers either the strategies to prevent selfish mining attack. It can be seen from the online database, i.e. Google Scholar which displays around 28,100 results in terms of selfish mining attack and the strategy to prevent it.

We also note that the selfish mining strategy affects the rational miner to adapt it due to this strategy is more profitable, therefore the well-defense strategy against selfish mining is necessary for Bitcoin protocol. Moreover, in the stubborn mining attack, the attacker's victim gets some advantages being eclipsed. The stubborn mining strategies concept is the attacker should not give up quickly rather than the attacker often increases its gain by mining on its private chain more often (stubborn), even under the conditions where the attackers chain will fall into the public chain. Under this strategy, outperform selfish mining up to 25% depends on parameters α and γ. Stubborn mining shows its exploitation at network level for further increase its profit. The eclipse attacks (at network level) isolates victims from the rest of its peers by the attacker control their incoming and outgoing connections. Hence, with this combination stubborn and eclipse attack can result to 30% of gains and surprisingly in some parameter ranges the attacker can collude with eclipse nodes and help the victims to gain little incentive with the reason not to be detected or react to such attack. Attacker force the eclipsed nodes to cooperate as a stubborn miner and they would maintain single private chain and eclipsed nodes would accept all the blocks generated by an attacker.

In contrast to the previously outlined research, Marlow [3] on his writing provides other information related to the acquisition of revenue from an attacker based on his mining power (resources). The author presents the expected gross return of selfish miner without addressing the flaws in the system. It might be the finest scenario of the attacker, although it is difficult for the attacker to achieve this level of strategy. Based on the results obtained as shown in Figure 7, it shows that the selfish miner only gains the unfair revenue when they reach 50% mining hash point.

One plausible way to prevent selfish mining attacks is to set up a block confirmation depth as proposed by Ansgar [8]. The author model the majority attack in Uppaal, and analyze how long it will take for an attack to succeed depending on the mining power of the attacker. To secure against double spending and the majority attack, a transaction should not be considered as a valid transaction until it reaches

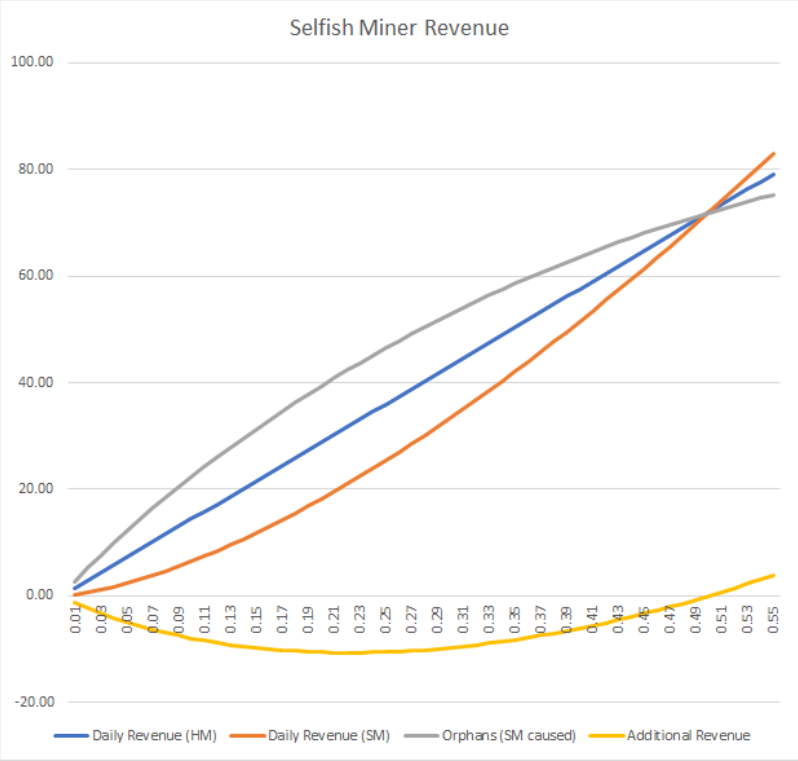

Figure 7: The revenue model of selfish miner

a certain number of confirmation depth (6 confirmation blocks) [14]. By increasing the confirmation depth from 6 blocks through 10 blocks, it remarkably affects on the time for the attacker to successfully implement their strategy. The data recorded for 10 blocks confirmation depth takes about 29600 minutes (20d:10h:20m) to succeed.

Regardless of the various strategies that have been proposed by several authors in various sources of literature, the selfish mining strategy is still in doubt of its existence due to selfish mining is simple to detect without any change to the protocol. The block releases should be regular within a certain time interval, and if there are any irregularities in the sense that no new blocks are published to the public network, they will be detected. The presence of selfish mining in Bitcoin is still a debate among researchers because it was until this paper was written selfish mining has not happened.

5 Conclusion

The scoping review research papers that are related to the strategy in defend against selfish mining attack in Bitcoin have been discussed and elaborated carefully. A number of prominent strategies were comprehensively chosen from the scholarly paper and the essential information was also gingerly written. Selfish mining attack which performs by the dishonest miner attracts the attention of the researcher since it was first discovered. Various strategies to prevent this attack was proposed from the threshold changes to the block structure changes. This paper offers an understanding of the current strategies of the selfish mining attack in Bitcoin even though selfish mining attack so far has not happened and still a debate among researchers.

Acknowledgments

This research was supported by the MSIT(Ministry of Science, ICT),Korea, under the ITRC(Information Technology Research Center) support program (IITP-2018-2015-0-00403)supervised by the IITP(Institute for Information &communications Technology Promotion) and partially supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2018R1D1A1 B07048944)

References

[1] Bitcoin difficulty. `https://bitcoinwisdom.com/bitcoin/difficulty` [Online; accessed on August 20, 2018].

[2] Bitcoin market info. `https://markets.bitcoin.com/` [Online; accessed on August 20, 2018].

[3] Selfish mining fallacy. `https://medium.com/@ProfFaustus/` [Online; accessed on August 20, 2018].

[4] 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*, pages 1–1, 2016.

[5] L. Bahack. Theoretical bitcoin attacks with less than half of the computational power (draft). *arXiv preprint arXiv:1312.7013*, December 2013.

[6] M. Bastiaan. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. `http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf` [Online; accessed on August 20, 2018], 2015.

[7] I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7):95–102, January 2018.

[8] A. Fehnker and K. Chaudhary. Twenty percent and a few days–optimising a bitcoin majority attack. In *Proc. of the 10th International Symposium of NASA Formal Methods Symposium (NFM'18), Newport News, Virginia, USA*, volume 10811 of *Lecture Notes in Computer Science*, pages 157–163. Springer, April 2018.

[9] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun. On the security and performance of proof of work blockchains. In *Proc. of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16), Vienna, Austria*, pages 3–16. ACM, October 2016.

[10] V. Gramoli. From blockchain consensus back to byzantine consensus. *Future Generation Computer Systems*, Sepember 2017.

[11] E. Heilman. One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. In *Proc. of the 2014 International Conference on Financial Cryptography and Data Security (FC'14), Christ Church, Barbados*, volume 8438 of *Lecture Notes in Computer Science*, pages 161–162. Springer, March 2014.

[12] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `http://bitcoin.org/bitcoin.pdf` [Online; accessed on August 20, 2018], 2008.

[13] K. Nayak, S. Kumar, A. Miller, and E. Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *Proc. of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P'16), Saarbrucken, Germany*, pages 305–320. IEEE, March 2016.

[14] S. Rahmadika, D. R. Ramdania, and M. Harika. Security analysis on the decentralized energy trading system using blockchain technology. *Jurnal Online Informatika*, 3(1):44–47, June 2018.

[15] S. Rahmadika and K.-H. Rhee. Blockchain technology for providing an architecture model of decentralized personal health information. *International Journal of Engineering Business Management*, 10:1–12, January 2018.

[16] S. Rahmadika, P. H. Rusmin, H. Hindersah, and K. H. Rhee. Providing data integrity for container dwelling time in the seaport. In *Proc. of the 6th Engineering Seminar (InAES'16), Yogyakarta, Indonesia*, pages 132–137. IEEE, August 2016.

[17] A. Sapirshtein, Y. Sompolinsky, and A. Zohar. Optimal selfish mining strategies in bitcoin. In *Proc. of the 20th International Conference on Financial Crypto (FC'16), Christ Church, Barbados*, volume 9603 of *Lecture Notes in Computer Science*, pages 515–532. Springer, February 2016.

[18] S. Solat and M. Potop-Butucaru. Zeroblock: Preventing selfish mining in bitcoin. arxiv preprint. *arXiv preprint arXiv:1605.02435*, May 2016.

[19] R. Zhang and B. Preneel. Publish or perish: A backward-compatible defense against selfish mining in bitcoin. In *Proc. of the 2017 Cryptographers' Track at the RSA Conference (CT-RSA'17), San Francisco, California, USA*, volume 10159 of *Lecture Notes in Computer Science*, pages 277–292. Springer, February 2017.

Author Biography

Sandi Rahmadika received his B.E. degree in Electrical Engineering, Instrumentation and Control from Universitas Bengkulu, Indonesia in 2013. He completed the dual master degree program between Institut Teknologi Bandung (ITB), Indonesia and Pukyong National University (PKNU), Rep. of Korea in 2016. He is currently a PhD candidate in the Laboratory of Information Security and Internet Applications (LISIA), Pukyong National University, Rep. of Korea. His research interests include applied cryptography and privacy preserving in blockchain.

Bruno Joachim K. received the Bachelor of information technology from Kampala International University in 2014. He joined the Pukyong National University for his Master degree of Information security in 2017. His research interests include design of blockchain application and security as well as IoT with blockchain integration.

Hyunwoo Kim received his B.S. degree in Information and Communication Engineering from Dongseo University, 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 applications, data sharing, applied cryptography, and network security.

Kyung-Hyune Rhee 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.