Effects of a Simple Relay Network on the Bitcoin Network

Kai Otsuki
Tokyo Institute of Technology
Tokyo, Japan
ootuki.k.aa@m.titech.ac.jp

Yusuke Aoki
Tokyo Institute of Technology
Tokyo, Japan

Ryohei Banno
Tokyo Institute of Technology
Tokyo, Japan
banno@computer.org

Kazuyuki Shudo
Tokyo Institute of Technology
Tokyo, Japan
shudo@is.titech.ac.jp

ABSTRACT

Bitcoin has a low transaction throughput. In order to allow for an increase of this throughput without increasing orphan blocks, decreasing the block propagation time is important. One of the techniques to improve its block propagation time is to utilize relay networks. However, the effects of utilizing relay networks is not apparent. Existing studies and measurements on relay networks have not focused on the effect of relay networks on the individual miners. Moreover, the relation between the degree of the effect and relay network utilization rate is unknown. Herein, we performed simulations while finely changing the proportion of nodes utilizing a relay network. Moreover we quantitatively evaluated the effect of relay networks on the entire Bitcoin network and individual miners. Results show that the propagation time decrease to approximately 77% of the original value if the utilization rate is set to 3%. This rate is close to the actual utilization rate of relay network "Falcon". We also found that the probability of blocks created by utilizing nodes to become orphan blocks is surprisingly smaller than that of the non-utilizing nodes. Even in the worst case, the value of utilizing nodes is 15% of the value of non-utilizing nodes.

KEYWORDS

relay network, bitcoin network, blockchain

1 INTRODUCTION

Several blockchains such as Bitcoin have fault tolerance and make it possible to manage distributed ledger information without a specific management entity even when multiple malicious nodes are present [11]. Although Bitcoin possesses these advantages, it has some limitations. A low transaction throughput is one of the biggest problems of Bitcoin. The transaction throughput is the number of transactions that a system can process within a certain time. At most, Bitcoin's throughput is 7 TPS owing to its design. In comparison, this value is below Visa's and PayPal's average throughput of 1700 TPS [6] and 290 TPS [5] , respectively. It means that Bitcoin can't support a system with the same scale as these centralized systems.

Shortening of the block interval is essential to increase the throughput. However, it is still difficult to simply shorten the block interval because the interval is set as the time essential for a block to be spread sufficiently within the network. In addition, A shorter block interval can cause more orphan blocks [12], which means a occurrence of a fork, and greatly damages the security of a blockchain network and the consistency of the ledger. To improve the throughput while avoiding an increase in orphan blocks, an increase in the block propagation speed is essential[8]. In other words, sufficient block propagation speed improvement safely achieve a shorter block interval.

An effective method to increase the block propagation speed is to utilize a relay network (cf. Figure 1), formed by a group of nodes that is capable of initiating a fast block distribution. Nodes using a relay network can send a block to other utilizing nodes simultaneously. Fast internet Bitcoin relay engine (FIBRE) and Falcon are relay networks used in Bitcoin. Falcon [3] is developed by Cornell University's research team, and FIBRE is a relay network developed by Matt Corallo, one of the developers of Bitcoin Core/citecore.

Presently, it is unclear what effect relay networks have on the Bitcoin network and individual miners. Existing measurements done by these relay network operators are partial because they measure real data. Moreover, no studies have measured the effect of relay networks while finely changing a utilization rate in a relay network, the proportion of blockchain nodes utilizing a relay network, and no studies has also paid attention to the influence on individual miners. Herein, we simulated while changing the utilization rate in a relay network. We quantitatively evaluated blockchain network-level and miner-level effects. As the blockchain network-level effect, we investigated the effect on the Bitcoin network such as the orphan block rate. Also, we examined the effect on individual miners such as mining success rate.

Knowing the relation between the relay network effect on a blockchain network and a utilization rate in a relay network helps

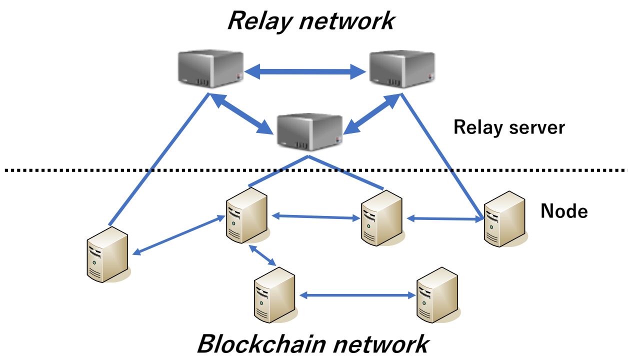

Figure 1: Relation between relay network and blockchain network: A relay network is an external network of a blockchain network. The relay network is composed of relay servers, and the blockchain network consists of blockchain nodes. Each Node utilizing the relay network can send and receive blocks to/from the relay server.

to understand usefulness of relay networks for throughput improvement. By understanding the effect on each miner, we can know if there is an incentive to use a relay network for miners.

The summary of our findings is as follows:

- The block propagation time improves as the utilization rate in a relay network increases. When the utilization rate is 3%, which is close to actual relay networks utilization rate, the propagation time is reduced to approximately 77% of the original value.
- A relay network decreases the orphan block rate, and when half of the nodes join the relay network, the value is reduced to less than 15% of the original value.
- In any utilization rate in a relay network, there is almost no difference in the number of discovered blocks between non-utilizing and utilizing nodes. In other words, relay networks have little impact on mining success rate.
- Nodes utilizing a relay network have a surprisingly low probability of creating orphan blocks compared to non-utilizing nodes. Remarkably, even in the worst case, the value of utilizing nodes is approximately 13% of the value of non-utilizing nodes.

The rest of this paper is organized as follows. In Section 2, as background knowledge, we describe the transaction handling in Bitcoin and the problems associated with it, and then we will look at a relay network that is one of the approaches to decrease the block propagation time. In Section 3, we describe a simulator and models of the Bitcoin network and a relay network used in this study. In section 4, we present our experimental results. In Section 5, we overview related work, and we conclude the paper in Section 6.

2 BITCOIN NETWORK

In this section, we explain our research background. We look at transaction handling in the Bitcoin system and describe problems of transaction confirmation. Finally, we refer to relay networks in Bitcoin.

2.1 Handling transactions in Bitcoin

We look at the flow from transaction issues to confirmation of transactions of the Bitcoin system. Then, we focus on orphan blocks.

2.1.1 Transaction issue. A transaction is recorded in a distributed ledger called a blockchain. When a node attempts to send coins to someone, it issues a transaction and broadcasts the transaction over the Bitcoin network. When nodes receive it, they verify it. If the transaction is valid, it will be stored in a memory called a transaction pool.

2.1.2 Block creation. To create a block containing the pooled transactions, miners repeat the hash calculation until they find a hash value that meets certain criteria. This process is called proof of work (PoW) and prevents invalid blocks from being generated. When nodes succeed in mining a block, they broadcast the block across the network and can obtain mining rewards. Basically, miners join the Bitcoin network in search of rewards.

2.1.3 Transaction confirmation. When nodes receive a block, they verify it. They add the block to their ledgers if it is valid. At this stage, the transactions contained in the newly added block are confirmed. A distributed ledger held by each node is a chain from the first generated block to the current block, which is a huge transaction register. A block is generated by using a hash value of the previous block, and it decides the order of blocks and the continuity of the ledger is guaranteed.

2.1.4 Orphan block. Forks are defined as the situations where a ledger is branching and they occur when a plurality of blocks are added after the same block. When a fork occurs in Bitcoin, the branch with the largest number of blocks is adopted as a formal ledger. At this time, the blocks in the pruned branches become orphan blocks.

Presence of forks is a big problem because it means that nodes with different ledgers exist on the blockchain network and transaction consistency among such nodes is temporarily lost. In addition, transactions in an orphan block are invalid, and computational resources for an orphan block creation are wasted.

2.2 Problems in Bitcoin

2.2.1 Problem Regarding Confirmation Time. A Transaction is confirmed when the block including it is confirmed. In Bitcoin, the block interval is set to 10 min [1]. Since It is considered that transactions are not overwhelmed if the six blocks are confirmed. Therefore, the time of six blocks confirmation is required to ensure that the transactions are definitely valid. The property becomes a crucial problem in trades having a deadline such as auctions or trades whose price fluctuate within seconds such as currency transactions. To overcome the problem, a reduction in the 10-minute block interval is required. However, achieving this reduction is difficult as a fork occurs when another node generates a block before a block propagates sufficiently. To reduce the block interval while suppressing the orphan block rate, an improvement of the block propagation time is necessary.

2.2.2 Problem regarding throughput. A throughput which is defined by the number of transactions which can be received from users could be improved in proportion to the increase in the number of nodes. The problem here is the transaction throughput.

The upper limit of Bitcoin's transaction throughput is approximately 7 TPS as the upper limit of the number of transactions included in a block is about 4000 and the block interval is 10 minutes. This is much smaller than the values such as Visa's and PayPal's average throughput of 1700 TPS and 290 TPS, respectively. Since these numbers are average values, much larger throughput is required at its peak.

The transaction throughput is determined by the number of transactions in a block divided by the block interval. Two schemes for improving the throughput are available. One is to increase the block size and the second is to reduce the block interval. Basically, the former does not contribute to the improvement because an increase in the block interval is necessary to suppress the fork when the block size increases. As a result, the improvement is canceled out. To perform the latter without increasing the orphan block rate, it is necessary to reduce the propagation time as mentioned earlier.

2.3 Relay networks

Utilizing relay networks is a method to improve the propagation time. Blockchain networks are not always suitable for efficient block distribution because they have other issues to deal with, such as malicious nodes. The relay network is a network suitable for efficient block distribution and can perform more efficient block propagation than a blockchain network.

Next, we describe the overview of block distribution using relay networks (cf. Figure 1). Relay networks are constructed outside the Bitcoin network ,and speed-up methods used in relay networks differ depending on its implementations. However relay networks have roughly the same basic structure. The flow of the block distribution is roughly as follows: First, relay servers constituting a relay network have been arranged all over the world. A node utilizing the relay network transmits blocks to the relay server in the same area. Then, the blocks propagate throughout the relay network, and utilizing nodes get the block from relay servers in the same area.

Several Bitcoin relay network projects are avilable and these include Bitcoin Fast Relay Network (BFRN) [2], Falcon [3], Fast Internet Bitcoin Relay Engine (FIBRE) [4] and bloXroute [10]. We briefly summarize their characteristics below and in Table 1.

Bitcoin Fast Relay Network (BFRN)
BFRN is the first Bitcoin relay network,which was set up by Matt Corallo in 2014. It has nine servers scattered around tshe world. This relay network has been shut down and is not currently in operation.

Falcon
Falcon was launched in 2016 by a Cornell University research team. They use a cut-through routing as the fast block propagation method. This relay network consists of ten servers around the globe.

Fast Internet Bitcoin Relay Engine (FIBRE)
FIBRE was developed by Matt Corallo in 2016 and has a unique UDP based relay protocol. It has six servers around the world. This relay network is especially designed for compact blocks, a relatively new relay protocol in Bitcoin.

Table 1: Summary of each relay network.

Project	Year	Number of servers	Developer
BFRN	2014	8	Matt Corallo et al.
Falcon	2016	10	Cornell University
FIBRE	2016	6	Matt Corallo et al.
bloXroute	2018	Unknown	Cornell University

bloXroute
bloXroute is a recent relay network. It published a white paper in 2018. However it is not yet in operation. Several developers of Falcon are involved in this relay network, and they focus on the existing relay networks problem that nodes using relay networks have to trust the relay networks.

3 SIMULATING RELAY NETWORKS

In this section we refer to the simulator used in our experiments. Then we introduce our models of the Bitcoin network and a relay network.

3.1 Simulator

We performed experiments using the simulator to investigate the effect of relay networks. The advantages of using a simulator are as follows.

- A simulator makes it possible to acquire the data of each node and the structure of the network, which are difficult to obtain from the actual network.
- The cost of setting up and implementing a simulator is lower than that of preparing an experimental private network.
- With a simulator, it is possible to freely set parameters such as hash power and a utilization rate in a relay network.

In this research, we used a blockchain simulator SimBlock [7]. Because SimBlock can simulate a situation where an inter-node delay fluctuates, it is suitable for measuring the effect of relay networks.

3.2 Blockchain Network Model

First, we are going to look at the parameters of this blockchain simulator and its settings.

In our experiments, the unlisted parts of parameters simulate the Bitcoin environment in 2015 examined by Gervais et al. [9]. The parameters in Table 2 were used by Aoki et al [7] except for hash power. To compare the mining success rates of nodes utilizing a relay network and non-utilizing nodes, we set the hash power of all nodes uniformly.

In this simulator, each node has an upstream bandwidth and a downstream bandwidth, and the transmission time is determined as follows.

$$TransmissionTime = Delay + \frac{BlockSize}{Bandwidth} + ProcessingTime$$

$$Bandwidth = \min\{Upstream\,Bandwidth\,of\ a\,Sender,\ Downstream\,Bandwidth\,of\ a\,Receiver\ \}$$

The delay is determined by the region of a sending node, region of a receiving node, and random number. Moreover, the processing time represents a time required to validate a block.

Table 2: Parameter settings of blockchain network.

# of nodes	6000
Block interval	10 min
Block size	534 KiB
Hash power	Uniform
Geographical Distribution	Distribution according to Bitcoin
Bandwidth	6 regional bandwidth
Delay	6 regional propagation delay

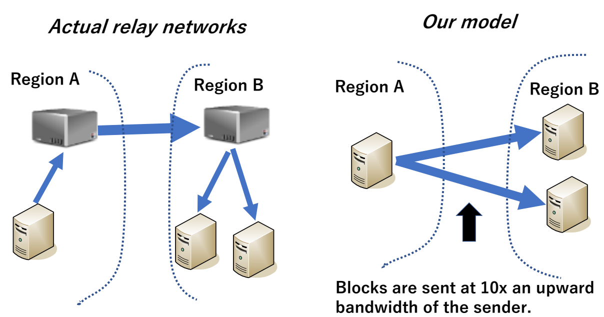

Figure 2: Actual relay networks and our simple relay network model.

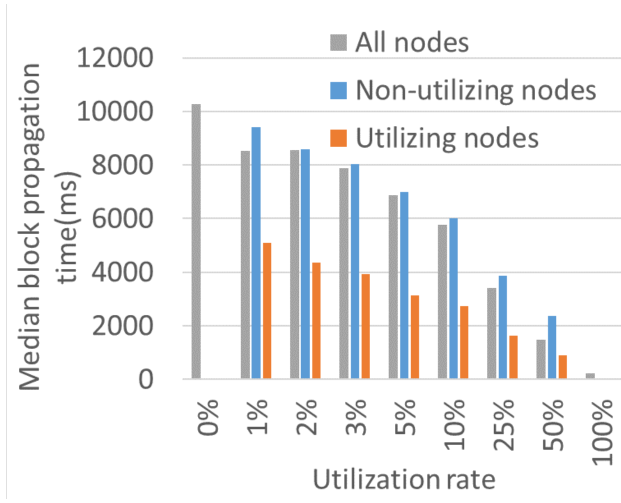

Figure 3: Median block propagation time.

3.3 Our Simple Relay Network Model

We will introduce our simple relay network model. Herein, we aim to investigate the effect of relay networks rather than a specific relay network. Therefore, we used a relay network model that abstracts and simplifies the actual relay networks. Before explaining our relay network model in detail, we review how the actual relay networks work.

Relay server communication is generally faster than a ordinary inter-node communication because relay networks use methods like cut-through routing, optimization of its topology and so on to transmit blocks faster, and they are likely to have large bandwidth. When a node utilizing a relay network sends blocks to the relay server in the same area, and the relay server broadcast the blocks to its relay network and other utilizing nodes can get the blocks from relay servers.

Then, in our relay network, we assume that nodes utilizing the relay network can transmit blocks to the other utilizing nodes by using 10 times their original upstream bandwidths. The Fig. 2 shows this. Thus, this simple relay network enable nodes to transmit blocks to other nodes directly or with one hop. Since downstream bandwidths are sufficiently larger than upstream bandwidths, the improvement in the upstream bandwidths help to make full use of the downstream bandwidths.

In this experiment, we changed the utilization rate in the relay network. The utilization rate represents the proportion of blockchain nodes using a relay network. We performed the experiments at utilization rates of 0%, 1%, 2%, 3%, 5%, 10%, 25%, 50% and 100%. We focused on low utilization rates considering the utilization rate of real relay networks. For example, from the data collected on January 27, 2019, Falcon utilization rate is 2.65%. Also, We randomly selected the utilizing nodes.

4 EXPERIMENTAL RESULTS

Two effects of relay networks are the blockchain-network-level effect and the miner-level effect. Herein, we examined the two effects and each simulation was run independently for 10000 consecutive blocks.

4.1 Effects on blockchain network

We use median block propagation time and orphan block rate to measure the relay network influence on the Bitcoin network.

4.1.1 Block propagation time. The effects of relay networks on block propagation time are discussed. We measured the median block propagation time for three groups of nodes, namely, all nodes in the Bitcoin network, the nodes utilizing the relay network, and the nodes not utilizing the relay network. All nodes consist of the nodes utilizing and not utilizing the relay network. The results are shown in Fig. 3.

We observe that the block propagation time for the Bitcoin network improves as the utilization rate in the relay network increases. This shows that using relay networks leads to an improvement in the propagation time. Even if the utilization rate is 3%, which is close to the actual relay network utilization rate, the propagation time is reduced to approximately 77% of the original value. Moreover, we observe that the propagation time improves in proportion to the utilization rate, even when observing each of the utilizing nodes and non-utilizing nodes separately. In other words, relay networks also improve the propagation time for non-utilizing nodes. Also, we can see that the median of the block propagation time of utilizing nodes has been always lower than that to non-utilizing nodes.

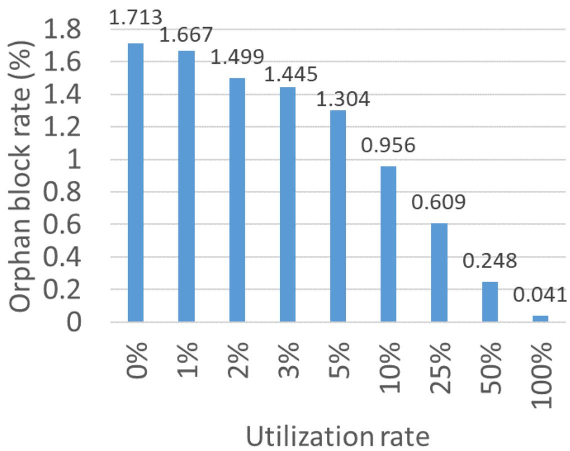

Figure 4: Orphan block rate.

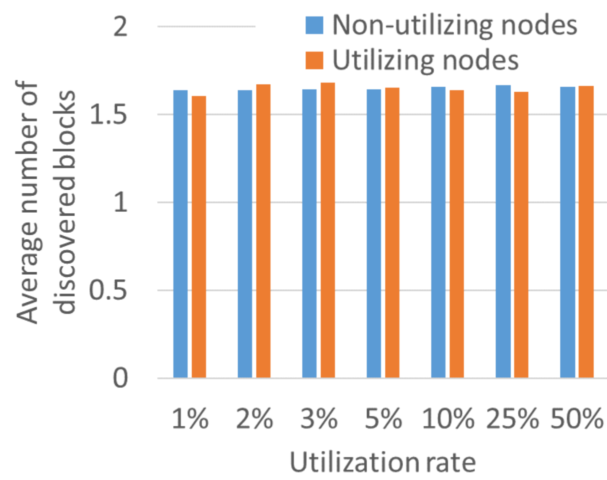

Figure 5: Average number of discovered blocks.

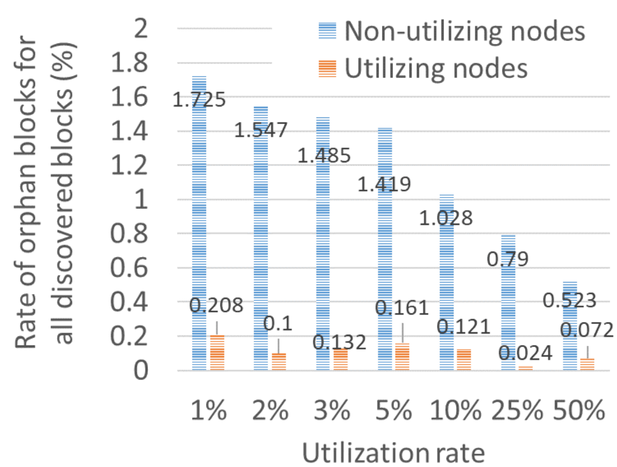

Figure 6: Rate of the number of orphan blocks for the number of discovered blocks.

4.1.2 Orphan Block Rate. We investigate the effect of relay networks on the orphan block rate. Fig. 4 shows the orphan block rates in each utilization rate.

We see that the orphan block rate decreases as the utilization rate in the relay network increases. With a utilization rate of 3%, the orphan block rate improve to approximately 85% of the initial value, and when half of the nodes join the relay network, the value is reduced to less than 15% of the original value.

An improvement in the block propagation time contributes to this decrease because a shorter block propagation time decreases the orphan block rate and the relay network decreases the time as the Fig. 3 shows.

4.2 Effects on each miner

We measured the average number of discovered blocks and the proportion of orphan blocks in all discovered blocks for utilizing and non-utilizing nodes to understand the influence on individual miners. Our experimental results are as follows:

4.2.1 Mining success rate. We investigate whether relay networks affect mining. In Fig. 5, we compare the average discovered block numbers of utilizing and non-utilizing nodes. Note that the number of discovered blocks does not include blocks that become orphan blocks and only blocks that are included in the longest chain of the blockchain are counted.

We observe that the relay network has a little effect on mining and no difference in the number of discovered blocks between utilizing and non-utilizing nodes. Moreover, the numbers of successful mining of utilizing and non-utilizing nodes are higher or lower regardless of the utilization rate.

Hash power and time to start mining determine a great part of mining success. In this experiments, we assume that all nodes have the same hash power. Thus, we can say that the improvement of the block propagation time produced by the relay network is not enough. Since our simulations use a strong relay network model, the mining success difference between utilizing and non-utilizing nodes is smaller for an actual relay network.

4.2.2 Proportion of Orphan Blocks. We investigated other relay network influence on each miner in addition to the mining success rate. We show the rate of the number of orphan blocks for the number of blocks discovered by utilizing nodes and non-utilizing nodes in Fig. 6. In Fig. 4, we focused on the relay network impact on orphan blocks for all the nodes on the Bitcoin network, and we then focus on the impact on orphan blocks for nodes utilizing and nodes not utilizing the relay network.

Our results show that utilizing nodes have a much lower probability of creating orphan blocks than non-utilizing nodes, regardless of the utilization rate. Even when the utilization rate is 50%, which is the case where the difference between the two is the smallest, the value of utilizing nodes is approximately 13% of non-utilizing nodes. The 25% utilization rate is the best case and the former value is approximately 3 % of the latter value. Note that this difference is true even if the utilization rate in the relay network is lower than the actual utilization rate such as 1% and 2%.

This shows that utilizing a relay network allow miners to put their created blocks on the longest chain. Therefore, this newly discovered effect shows miners an incentive to use relay networks.

5 RELATED WORK

Measurements on relay networks have not been widely investigated. In this Section, we refer to measurement values by operators of each relay network [2–4] and the research by Gervais [9].

Relay network operators publish measured values, for instance block propagation time to nodes utilizing a relay network or number of blocks discovered by utilizing nodes whose IP addresses are known. They can only make measurements on relay servers and utilizing nodes because these values are actual data. In other words, they cannot compare data between utilising nodes and non-utilizing nodes. We performed measurements by simulation, so we can obtain data on the whole, not part, and also compared the difference between utilizing and non-utilizing nodes.

Gervais discussed the security of PoW blockchains and did not cover the miner-level effect. They measured the effect on the blockchain network such as the orphan block rate and the median block propagation time. But they conducted experiments only when the utilization rate of a relay network is 0% and 100%. Since BFRN only existed at that time, they only considered BFRN as a relay network. In this research, we aimed to investigate the effect of relay networks rather than a specific relay network. Moreover, we measured the data while changing the utilization rate to 0%, 1%, 2%, 3%, 5%, 10%, 25%, 50%, and 100%.

6 CONCLUSION

Herein, we investigated the blockchain-network-level and miner-level effect of relay networks quantitatively while changing a utilization rate in the relay network. Regarding the effect on the blockchain network, we found that relay networks improve the block propagation time and reduce the orphan block rate. These effects become stronger as utilization rate in the relay network increases. Also, for individual miners, we saw that relay networks do not affect the mining success rate, but they significantly affect the probability of creating orphan blocks. utilizing nodes are surprisingly less likely to create orphan blocks than non-utilizing nodes.

These results help to understand the effectiveness of a relay network in improving blockchain scalability. If the effect is considered to be above a certain level, the results will motivate the development of relay networks. Our results show that there is an incentive to use a relay network for individual miners and help miners to decide whether to use a relay network.

We plan to investigate the influence of relay networks on other blockchain networks such as Ethereum. Also, the relay network model assumed in this research is a simplified model and the propagation protocol is assumed to be of the 2015 model, which is the same setting developed by Gervais [9]. After further refining the relay network model, we would like to evaluate the effectiveness of relay networks under new propagation protocols such as compact blocks. Herein, we assume that upstream bandwidth is 10 times as a strong relay network model and we intend to investigate the relation between relay network performance and its effect, such as how the results would change if the bandwidth is doubled, three times, and so on.

7 ACKNOWLEDGMENT

This work was supported by SECOM Science and Technology Foundation.

REFERENCES

[1] [n. d.]. Bitcoin Core : Bitcoin. https://bitcoincore.org. accessed Jan. 28, 2019.

[2] [n. d.]. Bitcoin Relay Network. http://bitcoinrelaynetwork.org/.

[3] [n. d.]. Falcon - A Fast Bitcoin Backbone. https://www.falcon-net.org/. accessed Jan. 27, 2019.

[4] [n. d.]. FIBRE Fast Internet Bitcoin Relay Engine. www.bitcoinfibre.org/. accessed Jan. 28, 2019.

[5] [n. d.]. PayPal Reports Second Quarter 2018 Results | PayPal, Inc. https://investor.paypal-corp.com/news-releases/news-release-details/paypal-reports-second-quarter-2018-results?ReleaseID=1072972. accessed Jan. 28, 2019.

[6] [n. d.]. VisaNet | Electronic Payments Network. https://usa.visa.com/about-visa/visanet.html. accessed Jan. 28, 2019.

[7] Yusuke Aoki, Kai Otsuki, Takeshi Kaneko, Ryohei Banno, and Kazuyuki Shudo. 2019. SimBlock: A Blockchain Network Simulator. In *Proc. CryBlock 2019 (in conj. with INFOCOM 2019)*.

[8] Christian Decker and Roger Wattenhofer. 2013. Information propagation in the Bitcoin network. In *Proc. IEEE P2P 2013*. IEEE, pp.1–10.

[9] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. 2016. On the security and performance of proof of work blockchains. In *Proc. ACM CCS 2016*. ACM, pp.3–16.

[10] Uri Klarman, Soumya Basu, Aleksandar Kuzmanovic, and Emin Gün Sirer. 2018. bloXroute: A Scalable Trustless Blockchain Distribution Network WHITEPAPER.

[11] Satoshi Nakamoto et al. 2008. Bitcoin: A peer-to-peer electronic cash system.

[12] Yonatan Sompolinsky and Aviv Zohar. 2015. Secure high-rate transaction processing in bitcoin. In *International Conference on Financial Cryptography and Data Security*. Springer, pp.507–527.