

including the latency and bandwidth, was quite different from the current one. In this study, we used a more realistic relay network model and performed exact and in-depth analyses of each relay network effect in the latest network.

VI. CONCLUSION

In this study, we used a realistic relay network model and performed exact and in-depth analyses of the relay network effects in the latest network. The investigation of relay network effects under the most current network state is one of the major contributions of this study. In terms of the effects on the Bitcoin network, we observed a decrease in the orphan block rate and in the 50th percentile of block propagation time, as indicated in previous studies. However, a new finding is that the improvement of the orphan block rate by the relay network became smaller as the Internet speed increased. We also found that the relay network improved the 90th percentile of block propagation time, and this paper is the first to investigate the relay network effect on the 90th percentile of block propagation time. Moreover, the comparison of the 90th and 50th percentiles of block propagation time revealed that relay networks have a larger influence on the 50th percentile. Furthermore, the degree of block propagation time improvements were approximately the same for utilizing and non-utilizing nodes. However, the propagation times of utilizing nodes were always better.

Regarding the effects on individual nodes, we confirmed that blocks of utilizing nodes were quite unlikely to become orphan blocks even in the current fast network. Moreover, we investigated the outcome when non-utilizing and utilizing nodes produced blocks simultaneously. The result confirmed that blocks of utilizing nodes are far more likely to become main blocks than those of non-utilizing nodes, which seems to be a significant benefit of the use of relay networks by utilizing nodes. This finding is also a major contribution of this study. As this study and other studies have indicated, when more nodes utilize a relay network, the effects of the relay network are greater. Hence, it seems desirable to encourage more nodes to utilize the relay network, and our results may provide a motive for these nodes to do so. In terms of the mining success rate, we observed that the relay network did not exert a significant influence: the differences between utilizing and non-utilizing nodes were below 0.1 at any utilization rate.

Some limitations are worth noting. Although our results found effects of relay networks when they worked ideally, their effects when they are not working ideally, for example, because of heavy load, are not clear. Therefore, future work should include a follow-up investigation of the effects when relay networks do not work well. In addition, the effects on other blockchain networks, such as Ethereum, should be examined.

ACKNOWLEDGMENT

This work was supported by SECOM Science and Technology Foundation.

REFERENCES

- [1] "VisaNet — electronic payments network," <https://usa.visa.com/about-visa/visanet.html> (accessed Feb. 13, 2020).
- [2] "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 Feb. 13, 2020).
- [3] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *Proc. IEEE P2P 2013*. IEEE, 2013, pp. 1–10.
- [4] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 507–527.
- [5] "Falcon - A Fast Bitcoin Backbone," <https://www.falcon-net.org/> (accessed Feb. 13, 2020).
- [6] "Bitcoin relay network," <http://bitcoinrelaynetwork.org/> (accessed Feb. 13, 2020).
- [7] 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. ACM CCS 2016*. ACM, 2016, pp. 3–16.
- [8] K. Otsuki, Y. Aoki, R. Banno, and K. Shudo, "Effects of a simple relay network on the bitcoin network," in *Proceedings of the 15th Asian Internet Engineering Conference (AINTEC 2019)*. ACM, 2019, pp. 41–46.
- [9] R. Nagayama, K. Shudo, and R. Banno, "Identifying impacts of protocol and internet development on the bitcoin network," in *Proc. 25th IEEE Symposium on Computers and Communications (IEEE ISCC 2020)*. IEEE, 2020.
- [10] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [11] "FIBRE Fast Internet Bitcoin Relay Engine," www.bitcoinfibre.org/ (accessed Feb. 13, 2020).
- [12] T. Neudecker, "Security and anonymity aspects of the network layer of permissionless blockchains," Ph.D. dissertation, Ph. D. thesis, KIT, 2019.
- [13] U. Klarman, S. Basu, A. Kuzmanovic, and E. G. Sirer, "bloxroute: A scalable trustless blockchain distribution network whitepaper," *IEEE Internet of Things Journal*, 2018.
- [14] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo, "SimBlock: A blockchain network simulator," in *Proc. CryBlock 2019 (in conj. with INFOCOM 2019)*, 2019.
- [15] Y. Aoki and K. Shudo, "Proximity neighbor selection in blockchain networks," in *2019 IEEE International Conference on Blockchain (IEEE Blockchain 2019)*. IEEE, 2019, pp. 52–58.
- [16] "Bitcoin Nodes Distribution - Bitnodes," <https://bitnodes.earn.com/> (accessed Feb. 13, 2020).
- [17] A. Miller, J. Litton, A. Pachulski, N. Gupta, D. Levin, N. Spring, and B. Bhattacharjee, "Discovering bitcoin's public topology and influential nodes," *et al.*, 2015.
- [18] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer *et al.*, "On scaling decentralized blockchains," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 106–125.