公益財団法人 セコム科学技術振興財団

# 研究成果報告書

研究課題名
社会基盤たり得る分散台帳の研究

Study on distributed ledger technology to be social infrastructure

研究期間
平成 29 年 10 月　～　令和 3 年 9 月

報告年月
令和 3 年　12 月

研究代表者
東京工業大学 情報理工学院 数理・計算科学系 准教授
首藤 一幸

Department of Mathematical and Computing Science,
School of Computing, Tokyo Institute of Technology, Associate Professor
Kazuyuki Shudo

## Abstract

The goal of this research is to establish the methods for distributed ledger technology that can support our society on a national and global scale. The subtopics of this research were development of a research tool, performance, security, fairness, decentralization, and incentive mismatch problem.

A research tool SimBlock we developed not only strongly facilitate our own research, but also it has been utilized by other researchers. Our papers about the tool have been cited by more than 90 papers as of December 2021.

In study on performance, we proposed a number of techniques to improve the number of transactions confirmed in a unit of time (i.e. TPS). We also evaluated existing techniques quantitatively and realistically. An example of our results is a neighbor selection technique that reduces the block propagation time by several tens of percent. We showed that the Compact Block Relay protocol, that was adopted by Bitcoin in 2016, was highly effective though improvement of Internet was also moderately effective. The relay networks have merit for the whole blockchain network and also for node operators utilizing them.

In study on security, our tool SimBlock enabled experimental approaches in addition to mathematical approaches, and then it improved the precision of the research results. We simulated existing attacks, estimated effects on performance effects of countermeasures, and then proposed new attacks.

In study on fairness, we proposed a new measure of fairness between nodes. An existing measure is very rough and not enough for our study. We also proposed a block interval adjustment technique that keeps the proposed measure of fairness.

In study on decentralization, we proposed a new data structure that heavily reduces the amount of data that a node stores. The purpose is to increase the number of nodes, that is critical for decentralization, by lowering the cost of node operation.

We pointed out the incentive mismatch problem. It is still an open problem today. At best, we proposed an application migration technique between blockchains. It keeps an application from the failure of the blockchain that the application bases on.

We are working on the above subtopics after the fund-supported period. In performance, the block propagation time has been reduced much, but it is not enough. A blockchain will enjoy improvement of transaction confirmation performance by adjusting block interval. The results on our fairness study will contribute such adjustment. Neighbor selection techniques including ours may increase the risk of Eclipse attacks. Our next results will improve the performance without increasing such a risk. In security, our current targets are Internet-scale attacks and other aspects of security.