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

概　要

国家・人類規模での日常利用に耐える分散台帳の方式を研究、確立するという目的のもと、研究ツールの開発・提供、性能の研究、セキュリティの研究、公平性の研究、分権化の研究、インセンティブ不整合問題の研究に取り組んだ。

我々が開発した研究ツール SimBlock は、我々自身が様々な研究の基盤として用いただけでなく、多くの研究者に活用された。2021 年 12 月現在、SimBlock についての論文の被参照件数は 90 件以上となっている。

性能の研究では、単位時間あたりのトランザクション承認件数（TPS）を向上させるべく、いくつかの手法を提案するとともに、既存手法の定量的・現実的な評価に取り組んだ。例えば、ブロック伝搬時間を数十%短縮できる隣接ノード選択手法を提案した。インターネット自体の高速化の効果も大きいながら、Bitcoin が 2016 年に採用した Compact Block Relay プロトコルの効果が極めて大きかったことも定量的に示した。また、リレーネットワークを利用した場合のブロックチェーン全体のメリットに加えて、ノード運営者が得られるメリットを示した。

セキュリティについては、研究ツール SimBlock を開発したことで、従来からの数理的なアプローチに加えて実験的なアプローチを可能とし、より高精度な研究を可能とした。我々自身では、既存の攻撃手法の模擬、攻撃対策が性能に及ぼす影響の推定を行い、また、新たな攻撃手法の提案も行った。

公平性の研究では、ノード間の公平性の新たな指標を提案した。従来の指標は非常に大雑把なものであり、我々が目指した公平性を考慮した取り組みのためには不十分であった。続いて、提案した公平性の指標を用いて、公平性を維持するためのブロック生成間隔調整手法を提案した。

分権化の研究では、ノードが保持するデータの量を劇的に少なくするデータ構造を提案した。それにより、ノード運営の敷居を下げ、ひいては、分権化に重要なノード数を増やすことが狙いである。

インセンティブ不整合問題を指摘した。これは今日でも未解決問題だが、せめて、ブロックチェーンに引きずられてアプリケーションも破綻することを防げるよう、ブロックチェーン間の移行手法を提案した。

助成期間終了後も、各領域の研究に取り組んでいる。例えば、性能については、ブロック伝搬時間の短縮に成功したが、それだけでは充分ではない。ブロック生成間隔を適切に調整できて初めて、トランザクション承認性能（TPS）が向上する。調整のためには、公平性の研究で得た知見が活きるだろう。我々の提案を含め、隣接ノード選択には Eclipse 攻撃を容易にしてしまう恐れがあるが、そうした恐れのない性能向上手法を研究している。セキュリティについても、インターネット規模の攻撃への対策や、また別の新たな観点での研究を始めている。