博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目 ： 非中央集権型ブロックチェーンにおける確率論的マイクロペイメント方式に関する研究
（原題：Probabilistic Micropayments in Decentralized Blockchain）

申請者 ： 高橋 大成

審査委員会 ： 主査　教授　有田 正剛
副査　教授　櫻井 幸一(九州大学)
副査　准教授　面 和成(筑波大学)
副査　教授　大塚　玲

Ⅰ. 論文内容の要旨

本論文は“非中央集権型ブロックチェーンにおける確率論的マイクロペイメント方式に関する研究”と題し、6 章からなっている。

第 1 章では、研究の背景として、ブロックチェーンやスマートコントラクトの登場により，通貨の革新が期待されることに触れ、その上で、現在のブロックチェーン上の暗号通貨がマイクロペイメント（少額決済）の決済手段として普及するためには、即時決済、高スループット化、匿名性の実現の 3 点が課題であることを指摘している。それぞれの課題について、解決に導くコアアイディアの概要を述べている。

第 2 章では、準備として、ブロックチェーンの安全性概念や確率的マイクロペイメントに関わる用語の定義と、次章以降で用いる代表的な匿名署名方式である DAA (Direct Anonymous Attestation) および、その改良版である EPID (Enhanced Privacy ID)と、現代的な耐タンパーデバイスの理論的枠組みである AESP (Attested Execution Secure Processor)等の基礎概念の定義を整理している。

第 3 章では、第一の課題である即時決済について、耐タンパーデバイスを用いた解決策を提案している。耐タンパーデバイスや銀行等の信頼機関に頼らない方式では、二重支払いリスクを避けられないことが従来研究で指摘されている。また、耐タンパーデバイスを用いた暗号通貨の即時決済においては、ブロックチェーン上に公開された価値情報と耐タンパーデバイス内部の価値情報の同一性の保証が課題となる。本論文では、耐タンパーデバイスが当該価値情報のコントロールを掌握し、かつ二重支払いでないことを Remote Attestation により受信者に証明すること、および受信者が当該価値情報の有効性を、共通プレフィックス定理に基づいて、受信者自身がローカルに保持するブロックチェーンのみを用いて確認することで、同一性保証の課題を克服し、安全な即時決済方式を構成している。

第 4 章では、第二の課題である高スループット化について、オープンループ型確率的マイクロペイメントによる解決法を提案している。確率的マイクロペイメントは、ブロックチェーンに登録する取引を確率的に選別することで選別確率に反比例してスループットを向上させることが可能な技術である。従来法のクローズドループ型確率的マイクロペイメントは、選別確率を小さくすると大量の無効取引を生じること、確率的にしか二重支払いを検出できないことが課題であった。これに対し、オープンループ型確率的マイクロペイメントを可能とすることで、無効取引を一切生じず、完全に二重支払いを検出できる画期的な方式を構成し、現実的なパラメータ設定の例として選別確率を 1/100 に設定すれば、$1 の取引に要する手数料を¢10 に抑え、かつブロックチ

ェーンの取引処理スループットを最大 100 倍に向上できると試算している。

第 5 章では、第三の課題である匿名性の実現について、第 4 章に述べられている確率的マイクロペイメント方式に、匿名性を付与した方式を提案している。具体的には、銀行等の信頼機関が存在しない、非中央集権型ブロックチェーンにおける暗号通貨にも適用できるように対象モデルを拡張した匿名性概念を定義した上で、AESP の理想機能に EPID による匿名署名と不正デバイスの無効化を含むように拡張し、これを用いて構成した確率的マイクロペイメント方式が匿名性を満たすことを数理的に証明している。

第 6 章では、前章までの成果により、即時決済、高スループット化、透明性を備えた匿名性の実現の 3 つの課題に対応した提案を行い、それぞれの課題に対する研究成果の貢献および今後の課題について述べている。非中央集権型ブロックチェーンにおける確率的マイクロペイメント技術の普及に向けて、実社会において求められる要求の多くが解決可能であることを示している。

Ⅱ. 論文審査結果の要旨

本論文は、情報社会の基盤技術になりつつあるブロックチェーンに基づいた非中央集権型マイクロペイメント技術について、即時決済、高スループット化、匿名性の付与を達成するための、具体的かつ基盤的な方法を示したものであって、情報学ならびに情報社会の発展に貢献するところが大きい。よって、本論文は情報学における博士論文として十分価値のあるものと認める。

Ⅲ. 審査経過

本審査委員会は、2022 年 7 月 14 日に論文内容について口述試問を行い、その後， 2022 年 8 月 18 日に関連する事項の最終試験審査を行った。審査に当たっては、博士学位のディプロマ・ポリシーに基づいて総合的に評価し、申請者が学位取得にふさわしい知見を持つものと判断した。