Tulips R
University of Tsukuba Repository

A study on High Scalable Blockchain and the Application to Data Existence and Integrity Authentication

著者	高 月菲
発行年	2019
その他のタイトル	ブロックチェーンの拡張性向上とデータの存在性と完全性の証明への応用に関する研究
学位授与大学	筑波大学 (University of Tsukuba)
学位授与年度	2018
報告番号	12102甲第9007号
URL	http://hdl.handle.net/2241/00156994

氏　名	高　月菲
学位の種類	博　士（　工学　）
学位記番号	博　甲　第　９００７　号
学位授与年月日	平成　３１年　３月　２５日
学位授与の要件	学位規則第４条第１項該当
審査研究科	システム情報工学研究科
学位論文題目	A study on High Scalable Blockchain and the Application to Data Existence and Integrity Authentication （ブロックチェーンの拡張性向上とデータの存在性と完全性の証明への応用に関する研究）

主　査	筑波大学　准教授	博士（工学）　延原　肇
副　査	筑波大学　教授	博士（工学）　古賀　弘樹
副　査	筑波大学　助教	博士（工学）　澁谷　長史
副　査	筑波大学　助教	博士（工学）　河合　新
副　査	筑波大学　助教	博士（工学）　高安　亮紀

論　文　の　要　旨

本論文は、ブロックチェーンに関する拡張性向上とブロックチェーンインフラを利用した応用展開に関するものである。ブロックチェーンは、近年、社会インフラおよびサービスを抜本的に改革する可能性を有する情報処理技術として注目されている一方で、いくつか改善の余地が残されている。本論文では、その中でも、ブロックチェーンの拡張性の向上に着目している。具体的には、ブロックチェーンに新たなブロックを追加認証する時間が長い点であり、これを短くし、単位時間あたりの認証速度を向上させるための新たな手法を提案するとともに、クラウドを利用した比較的大規模な実証実験により有効性を示している。さらにブロックチェーンの応用展開として、代表的な金融サービスであるビットコインのインフラを利用することで、即時性が高く、また低コストで著作権保護支援を実現するシステムを構築し、実環境での実験を行っている。

本論文は 5 章より構成されている。1 章では研究の背景および目的について述べている。2 章では、ブロックチェーンに関する基礎および周辺動向について述べている。また、ブロックチェーンによって変わってゆく社会環境の現状および今後の予想を述べ、今後必要になってくる必要技術の抽出と、本論文で提案する枠組みの位置付けについて述べている。3 章では、ブロックチェーンに新たなブロックを追加認証する時間が長い点について問題提起している。従来の認証方式は、PoW（Proof of Works）という手法に基づいているため、利用ユーザ数が増加した場合においても、単位時間あたりの認証速度を向上させることが困難であった。一方、本論文では、それに代わる手法として、PoS（Proof of Stake）という認証方式および利用ユーザをクラスタリングする Sharding を融合させることで、単位時間あたりの処理速度の向上を実現している。提案手法の有効性を確認

するため、クラウド環境を利用した 100 ノード規模のシミュレーションを行い、従来手法の PoW に比べ、提案する PoS と Sharding の統合手法の認証速度が向上していること示している。

4 章では、ブロックチェーンによって変革がもたらされる分野として、CGM（Consumer Generated Media）における著作権保護を設定し、不正利用などを防ぐための即時性の高い、また低コストで実現できる著作権保護支援システムを提案している。この提案システムでは、自身の投稿したコンテンツ著作権を主張したいユーザが、ビットコインの取引であるトランザクションを投げ銭のような形で発生させ、その際にトランザクション内の自由に書き込めるフィールドに、ハッシュ関数を利用してコンパクト化した自身のコンテンツをコードとして埋め込む仕組みとなっている。提案手法の有効性を確認するため、実際のビットコインを利用した実験環境を構築し、投げ銭の金額をいくつかの段階に設定し、認証速度の計測を行っている。その結果、数円程度の投げ銭を利用すれば、約 10 分後には認証され、世界中のユーザが共有するブロックチェーンに書き込まれることを確認している。最終章では本論文の結論、今後の課題について述べている。

審　査　の　要　旨

【批評】

本論文では、今後の情報社会のインフラおよびサービスを大きく変革させることのできる可能性を有するブロックチェーンに関する拡張性向上とブロックチェーンインフラを利用した応用展開に着目し、(1) PoS および Sharding による認証速度向上、(2) ビットコインインフラを利用した著作権保護支援システムを提案している。(1)に関しては、クラウド環境を利用した比較的大規模な実証実験を通して有効性を示している。(2)に関しては、ビットコインを利用した実験環境を構築し、実環境での実験を行い有効性を示している。ブロックチェーンに関して、改善の余地がまだ残されており、それらに対するアプローチは今後の課題であるが、本論文で提案された手法・システムおよび実証実験で得られた知見は、ブロックチェーン領域における研究に非常に大きなインパクトを与えるとともに、有用な学術資料ともなり、博士論文に値するものと考えられる。

【最終試験の結果】

平成 31 年 2 月 5 日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。その結果、学位論文審査委員全員によって、合格と判定された。

【結論】

上記の学位論文審査ならびに最終試験の結果に基づき、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。