氏　名	Yangfei Lin
学位の種類	博　士（工学）
学位記番号	博　甲　第　10246　号
学位授与年月日	令和　4　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	Study on Blockchain-Based Cloud Data Integrity Auditing (ブロックチェーンに基づくクラウドデータの完全性検証に関する研究)

主　査	筑波大学　教授	博士（工学）	亀山　啓輔
副　査	筑波大学　教授	博士（理学）	建部　修見
副　査	筑波大学　教授	博士（工学）	國廣　　昇
副　査	筑波大学　准教授	博士（情報科学）	面　　和成
副　査	筑波大学　准教授	博士（情報科学）	木村　成伴

論　文　の　要　旨

審査対象論文は，ブロックチェーンを利用して，クラウドに格納されたデータの完全性を検証する方式を提案したものである．

本論文の第１章では，クラウドストレージやブロックチェーンの現状について述べ，本論文の研究を行った動機について説明している．第２章では，本論文で用いる予備知識として，パブリッククラウドデータの完全性の監査モデル，暗号プリミティブ，ブロックチェーンとスマートコントラクトなどについて説明している．第３章では，本論文に関連する研究について述べられている．

第４章では，最初の提案である Consortium Blockchain-based Public Integrity Verification (CBPIV)について述べている．この方式では，IoT (Internet of Things)デバイスなどの計算資源が限られている装置を対象に，クラウドストレージに格納されたデータの完全性の証明の検証を TPA (Third-Party Auditor)に依頼するが，これをスマートコントラクトが検証した結果を，ブロックチェーンに出力することによって，信頼できない TPA に備えている．そして，従来方式と計算のオーバヘッドや計算コスト，検証に要する時間などを比較することで，提案方式の有用性を示している．

第５章では，２番目の提案である Blockchain-based Public Auditing Outsourcing system without TPAs (BPAO)について述べている．この方式では，クラウドストレージに格納されたデータの完全性の証明を，スマートコントラクトに検証させるが，その計算は複数の CSP (Cloud Service Provider)にアウトソーシングすることで，信頼できない CSP に備えている．そして，ユーザの実行時間やブロックチェーンの費用を評価することで，提案方式の有用性を示している．

最後に，第６章で本論文をまとめ，今後の課題について述べている．

審　査　の　要　旨

【批評】

近年，Dropbox や OneDrive などに代表されるクラウドストレージサービスの利便性が注目されており，スマートフォンの普及とネットワークデバイスの高速化に伴い，USB メモリやメモリカードなどのストレージデバイスからクラウドストレージへの移行が急速に進んでいる．これによって，クラウドストレージへ大量のデータが蓄積されているが，クラウド側の故意，もしくは偶然による障害などにより，データの一部，もしくは全体が損傷している可能性がある．このような事態は，ユーザの気が付かないうちに生じており，クラウド側もその事実を隠蔽する可能性があることから，データの量が多くなれば多くなるほど，損傷の発生を検証することは困難となる．審査対象論文は，計算資源が少ないデバイスであっても，機密性を保持しつつ，クラウドデータの完全性を検証する方式を 2 つ提案したものであり，今後，このような研究はますます重要になると考えられる．

本論文の第 4 章で提案されている方式では，限られた人しかデータを記録できないコンソーシアムブロックチェーンを信頼できる記憶領域と仮定して，クラウドデータの完全性の証明の TPA による検証結果をブロックチェーンに出力させ，これをスマートコントラクトで確認するところが特徴である．検証するデータブロックが増えると，TPA での計算コストは他方式と同様に増えるものの，他の方式と比べて，通信オーバヘッドは増えず，スマートコントラクトの検証時間は短く，ユーザの計算コストも増えないところが，優れた点である．

本論文の第 5 章で提案されている方式では，TPA は利用せず，また，プライベートブロックチェーンを用いて，第 4 章の方式を実現している．そのために，クラウドデータの完全性の証明を，ユーザが難読化した上で，スマートコントラクトに検証させるものの，証明に要する計算を CSP にアウトソーシングしてスマートコントラクトの負荷を軽減させるところが特徴的である．ユーザが行う処理もあるが，1000 ブロックでも 1 秒程度であり，他の処理も無視できる程度である．但し，スマートコントラクトが処理する時間は短いものの，処理に要するコストが高いところは懸念される．

以上の提案方式は，ローカルの計算機とテスト用のブロックチェーンネットワークを用いて実装され，その性能が評価されていることから，工学的に貢献するところが極めて大きいと考えられる．今後は，これらの提案方式をクラウドサーバと実ブロックチェーンネットワーク上に実装し，実際の環境で運用することで，これらの方式の有効性を示すことが望まれる．

【最終試験の結果】

令和 4 年 2 月 7 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．