ブロックチェーンを用いた P2P 型電子文書配布における処理速度向上の研究

指導教員　寺島 美昭
1958113　田川 勇希

1　はじめに

企業などで管理されている電子文書は、組織内で電子ファイルとして保存されていたとしても、他の企業などに共有される際には印刷、メールなどで共有されることが多い。そして、その電子文書のやり取りの履歴を管理するために紙で台帳を付ける企業は多く存在している。しかし、マルチベンダ開発などの共有が複数回行われるような状況では、この手法は非常に手間がかかる。これらの課題を解決する手法として P2P 型データ管理手法であるブロックチェーンを用いる研究 [1] が存在する。しかしこの研究の課題として配布時の処理速度が挙げられる。本稿ではこの処理速度における文書の変換処理に着目し、更なる処理速度向上を目指す。そのために、WEB ブラウザ上で文書の配布処理を可能にする WEB アプリケーションを実装する。これを用いて処理時間を指標とし実験を行い、その結果から処理速度改善を図ることができる電子文書変換手法を考察する。

2　研究課題

3　提案

4　設計

提案の処理速度向上手法を評価するために、試作システムを実装する。P2P モデルでシステム構築を行うため、それぞれのノードはクライアント機能とサーバ機能を有しており、クライアント PC がブラウザを介することでコントラクトにアクセスし、提案手法の処理を実行可能にする。図 6 に試作システムの概要を示す。電子書籍の閲覧が最も多いのはスマートフォンだが、良好な通信環境でのデータを取得するため有線を用いたローカルネットワークを用いて PC による実験を行う。試作システムの構成表は表 2 に示す。コントラクトとの連携には Web3.js というライブラリ機能を利用しなくてはならないことから、同一言語で実装でき、双方向の Socket 通信が容易に実装できることからサーバ機能とクライアント機能は Node.js で実装した。ブロックチェーンの開発基盤は Ethereum[3] を用いてテストネットには Ethereum と同一環境で実験を行える Ropsten ネットワーク [4] を利用した。ウォレットの秘密鍵の管理機能には GoogleChrome の拡張機能である Metamask を用いた。それ に対応するブラウザを用いる必要があったため使用ブラウ ザは GoogleChrome と Firefox とした。

表 1　試作システム構成図

データの型	宣言	ビット幅
文字型	char	8
整数型	int	32
倍精度実数型	double	64
倍々精度実数型	long double	96

5　評価手法

6　考察

7　まとめ

本稿では、電子文書をブロックチェーンで管理する際のパフォーマンス課題に触れた。

本稿では、文書の流通を管理するために管理要件の分析を行い、流通性、機密性、記録性、一貫性の 4 つのセキュリティ要件を定義した。ブロックチェーンを用いることで改ざんされにくい履歴機能を実現し、ハッシュ変換により文書の同一性を確保することができるため、記録性と一貫性は解決できる。流通性と機密性の解決には通貨規格をベースとした関連閲覧権を提案した。また、それらの機能を確認するための試作システムの構成についても述べた。

参考文献

[1] 川島悠太「ブロックチェーンを用いた電子文書 P2P セキュリティ管理手法に関する研究」(2021)
[2] コンセンサス・ベイス株式会社「図解即戦力 ブロックチェーンのしくみと開発がこれ一冊でしっかりわ

かる教科書」(2019)
[3] 赤羽喜治, 愛敬真生編 「ブロックチェーンの仕組みと理論: 増補改訂版」 株式会社リックテレコム出版 (2019)
[4] 加嵜長門、篠原航「ブロックチェーンアプリケーション開発の教科書」マイナビ出版 (2018)