Vol.2018-MPS-120 No.24
2018/9/26

電子投票システムにおけるブロックチェーンの有用性に関する一考察

栗栖 遼馬[†1]　小板 隆浩[†1]

概要：日本では選挙の投票率が低い．国政選挙では投票率は 60%以下に低下している．投票率の低下は民意が反映されなくなる原因になる．投票率の低下を解決する方法の一つとして，電子投票システムが有効である．しかし，国政選挙に電子投票システムを用いた国では，国が投票を管理していたため，投票処理がブラックボックス化されていた．既存の電子投票システムは，紙に比べて利便性が高いが，透明性が低く，第三者の不正には気付くことができない．本稿では，電子投票システムの透明性，秘匿性を高めることを目的として，既存のブロックチェーンを用いた電子投票システムを比較し，電子投票システムに対するブロックチェーンの有用性について考察する．

キーワード：ブロックチェーン，電子投票

A Study on the usefulness of Blockchain in EVM

RYOMA KURISU[†1]　TAKAHIRO KOITA[†2]

Abstract: One of the problems with the electronic voting is lack of transparency and anonymity. As a solution, it is conceivable to employ a Blockchain for electronic voting. This report discusses issues related to transparency and anonymity of electronic voting and the effectiveness of Blockchain to solve them.

1. はじめに

日本では，選挙の投票率が低い．平成 29 年に行われた第 48 回衆議院議員総選挙では，投票率が全体で 54．68%であった．投票率が低いと民意が正しく反映されない．投票率向上の方法として，ネットワークを用いた電子投票システムが有用であり，投票所に向かう手間が省ける．しかし，電子投票システムの問題点の一つとして，システムがブラックボックス化されていることが挙げられる．電子投票システムにおける投票作業のブラックボックス化により，選挙管理委員会等の第三者の投票管理者の不正に気づくことができない．解決策としては，投票処理に関して透明性を担保する必要がある．しかし，投票者の情報は投票者以外には知られてはいけない．文献[1]では，電子投票システムにおいて，ブロックチェーンを用いることで階層的な統治による第三者の不正に対して，透明性を担保し不正を防ぐと論じている．文献[2]でも，ブロックチェーンを用いた電子投票システムの透明性について論じている，本稿では，投票処理の透明性を担保し，投票者の投票情報を秘匿化することを目的として，電子投票システムに対して，ブロックチェーンの有用性について考察する．

†1 同志社大学
Doshisha University.

2. 関連研究

電子投票システムの満たすべき基準について述べ，電子投票システムに用いられるブロックチェーンについて説明する．

(1) 電子投票システム

電子投票システムには，投票所での投票が電子化されている場合と，ネットで投票する場合がある．文献[3]において，両方の電子投票システムにおいて必要とされる基準は以下のようなものがある．

- 投票資格と本人確認
- 投票の一意性
- 投票の正確性
- 投票の改変不能性
- システムの信頼性
- 個人の投票内容の秘匿性
- 投票の方法の秘匿性
- 投票処理の透明性(全行程の可視化)
- システムの運用コスト

これらの基準の中から，個人の投票内容の秘匿性と透明性について考察する．

(2) Enigma

ブロックチェーンを用いた電子投票に関して，ブロック

チェーン上にあるデータの秘匿化に有用であるのが，文献[4]で論じられている Enigma である．現在のパブリック型のブロックチェーンでは，改ざんを防ぐために，ブロックチェーン上のデータがそのまま公開されている．Enigma はブロックチェーン上のデータを暗号化したまま検証することができる．

(3) **Agora: voting systems**

文献[2]では，Agora 社がブロックチェーンをベースとした電子投票システムについて論じている．Agora 社の電子投票システムは既にアフリカのシエラレオネの大統領選挙に対して，同時並行で実証実験を行った．Agora は Skipchain, Cotena，Valeda，Votapp，Cothority という 5 つのシステムを用いた構成になっている．開票作業は認証されたノードが行い，その他の検証はパブリック型のブロックチェーンを用いている．ログも Bitcoin のブロックチェーンに保持されている．投票処理の透明性，秘匿性，実用性，アクセス性という基準を満たしていると論じている．

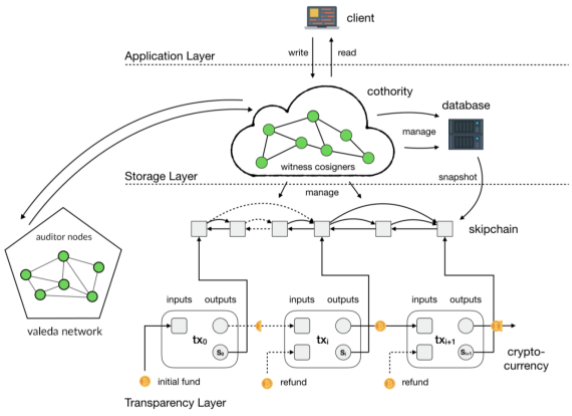

図 1　Agora の投票システム構成[2]

3. 現状の課題

ブロックチェーンを用いた電子投票システム中から，Agora 社の電子投票システムを取り上げに現状の課題について検討する．

3.1 透明性

投票の開票は，コンソーシアム型のブロックチェーン上で行う．大学など信頼される機関を検証ノードとして，データの整合性を確認する．データベース上に投票データのログを保持していて，逐次ログをブロックチェーンに追記してき，ユーザは自分の投票はアプリケーションで確認できる．しかし，検証ノードは認証型で，開票作業自体が中央集権化されているため，検証ノードの不正は，パブリック型のブロックチェーンに比べて，容易である．

3.2 秘匿性

コンソーシアム型のブロックチェーンでの検証のため，投票データが公にならない．しかし，透明性を高めるために，パブリック型のブロックチェーンにすると，投票データが公開されてしまう．透明性を高めようとすると，投票データの秘匿性が失われてしまう．

4. 提案手法

Agora はまだ実験段階だが，ブロックチェーンを用いることで，投票者の個人の内容が一般ユーザからは秘匿化し，結果に対してはパブリックチェーンで透明性を担保しているため，電子投票システムに対するブロックチェーンの有用性が示されている．しかし，開票作業はコンソーシアム型のブロックチェーンを用いているため，第三者の不正が容易である．また，第三者の不正を防ぐために，パブリック型のブロックチェーンにすると，投票データの秘匿性が失われてしまう．透明性と秘匿性を担保する解決策として，Enigma を用いると，パブリック型のブロックチェーン上で，投票内容を暗号化したまま計算できるため，検証ノードには生の投票データを与えないまま，検証できる．また，パブリックブロックチェーンであるため，第三者の不正が難しくなる．

5. まとめ

本稿では，透明性，秘匿化に電子投票システムにおけるブロックチェーンを対象として，既存システムについて述べ，有用性を考察した．

Agora では，開票作業を認証された検証ノードのみで行なっているため，検証ノードの不正が行われる可能性がある．電子投票において，ブロックチェーンを用い，透明性，秘匿性を高めることが，電子投票の実用化により近づくことができると考えられる．

参考文献

[1] 社会を変えるブロックチェーン技術 : 5. ブロックチェーンの分散台帳を利用した電子投票による集合知の構成 -対称的な非集監査と絶対中立的な非可逆的記録-, 情報処理 Vol. 57 No. 12 (2016).
[2] Agora: Bringing our voting systems into the 21st century https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5b6c38550e2e725e9cad3f18/1533818968655/Agora_Whitepaper.pdf
[3] Gritzalis, D. : Secure Electronic Voting : New Trends, New Threats, New Options, 7th Computer Security Incidents Response Teams Workshop (2002).
[4] Guy Zyskind, Oz Nathan , Alex Sandy Pentland, Enigma: Decentralized Computation Platform with Guaranteed Privacy, https://enigma.co/enigma_full.pdf