講演番号：35

ブロックチェーンを用いたトラストレス匿名選挙システムの検討

A Study of Trustless Anonymous Voting System using Blockchain

渡辺 拓斗† 小川 猛志†

Takuto WATANABE† Takeshi OGAWA†

† 東京電機大学システムデザイン工学部情報システム工学科

† School of System Design and Technology, Tokyo Denki University

1. はじめに

ブロックチェーンを活用した選挙システムの提案があるが，選挙管理者自身による不正の可能性や匿名性が不十分などの課題がある．本稿では国政選挙への適用を想定し，それらを解決する手法を提案する．

2. 先行研究の概要と課題

2.1 先行研究1の概要

1 つ目は，オフチェーンでブラインド署名により投票を匿名化しブロックチェーンで集計を行う提案である[1]．手順の概略を以下に示す．①投票者が，候補者名を記した投票内容にブラインド処理を施し，管理者に送付．②管理者が，投票者である条件を満たすことと，二重投票でないことを確認し，ブラインド署名を施して投票者へ送付．③投票者が，投票内容にアンブラインド処理をし，選挙用のスマートコントラクトに送付．④スマートコントラクトが管理者の署名を検証し，投票締切後に投票結果を集計．

2.2 先行研究2の概要

2 つ目は，電子マネーの取引(誰から誰への支払いか)を匿名化できる Tornado Cash コントラクトを応用しオンチェーンで匿名化と集計を行う提案である[2]．手順の概略を以下に示す．①管理者が選挙用の Tornado Cash コントラクト(以下，TCC)内の投票者のアドレス1に選挙券となる ERC-20 トークンを配布．②投票者が TCC の匿名 ERC-20 トークンプールに選挙権を付け替え．③投票者がアドレス 1 に紐づいていないアドレス2を使用して TCC の ERC-20 トークンプールから TCC 内の候補者のアカウントに選挙権(1 票)を移動．④投票締切後に候補者毎の得票数を集計．

2.3 先行研究の課題

課題1：両研究共に有権者の認証を管理者が行う為，管理者が有権者以外へ投票を許可する不正が可能．

課題2：研究 2 は以下の手順により匿名化を解除可能．

(1) 選挙終了後，投票に使用された全トランザクション(以下 Tx)をブロックチェーンからコピー．
(2) ローカル環境のブロックチェーンに手順②の Tx の一つのみを除外して他の全 Tx を入力
(3) ローカル環境の各候補得票数を上記選挙結果と比較
(4) 上記(2)，(3)を繰り返す．

課題3:研究 1 では投票の有効性は管理者の署名のみで判断されるため,管理者が有権者になりすまして複数の投票を行う不正が可能．

3. 提案手法

各有権者は住所や氏名，居住年等を自治体が保証したデジタル証明書(マイナンバーカードや VC)を保持していると仮定し，以下のように各課題を解決する．

課題1：スマートコントラクト上で有権者の認証を行うことで管理者による不正な認証を防ぐ．

課題2：オフチェーンでの匿名化(ブラインド署名)で防止．

課題3：投票後に投票者による投票数の確認を行うことで，管理者による不正な投票を困難とする．

詳細な手順を以下に示す．

①投票者が，候補者を記した投票内容と匿名識別子(十分な長さの乱数)にブラインド処理を施し(以下 BM)，投票者の VC を添付し選挙用スマートコントラクト(以下 VSC)に送付．

②VSC が VC により投票権(住所，年齢など)の確認と VC の署名検証を行い，投票者リストに重複がないことを確認した後，当該 BM をコントラクト内の投票者リストに登録．

③署名者はブロックチェーンから BM を取得し，BM に対してブラインド署名を施し(以後 BSM)，投票者に送付．

④投票者は BSM に，アンブラインド処理をして(以後 UBM)，使い捨てのアドレスで VSC に送付．

⑤VSC が署名者の署名を検証し，有効投票リストに登録．

⑥投票期間を終了し，検証期間を開始．投票者は有効投票リストを確認し，自身の匿名識別子が確認出来なかった場合は，再度 UBM を VSC に送付．VSC は署名を検証し匿名識別子の衝突がなければ未投票リストに登録．

⑦検証期間終了後，式(1)を計算し，満たさない場合は，署名者が不正を行ったと判断し，投票を無効とする．

$$\text{投票者リストの長さ} \geq \text{有効投票リストの長さ} + \text{未投票リストの長さ} \quad (1)$$

4. まとめと今後の課題

選挙管理者自身の不正も困難でかつ匿名性を保証できる選挙システムを提案した．国政選挙では投票者リストが大きくなるため，効率の良い管理方法が必要である．また，選挙終了まで各候補の得票数を隠蔽し，かつ，終了後には確実に公開できる手法が必要である．

参考文献

[1] Carcia, et al., "Blockchain-based system for e-voting using blind signature protocol." 2021 IEEE GLOBECOM.

[2] Bistarelli, et al., "An E-Voting System Based on Tornado Cash." ETAA 2022, Springer.