日本オペレーションズ・リサーチ学会
2021年 秋季研究発表会

ゼロ知識証明を使った投票モデル Zvote の提案

申請中　早稲田大学院　*木佐木雄太　KISAKI Yuta
01307080　早稲田大学　豊泉洋　TOYOIZUMI Hiroshi

1. はじめに

近年の情報技術の発展に伴い, 世界各国で実際の選挙におけるインターネット投票の試験的, 部分的な導入が進められている [1]. 暗号理論において, インターネット投票システムに要求される安全性として匿名性をはじめとする 7 つの性質が挙げられている [2] が, 既存のインターネット投票システムの多くは信頼できる第三者機関 (Trusted Third Party, TTP) を介在させることでこれらを達成している [3]. 本研究では, ブロックチェーン技術と公開鍵暗号方式, そしてゼロ知識証明 (Zero-Knowledge Proof, ZKP) を利用した暗号通貨である Zerocoin[4] のスキームを応用することで, TTP を介さずに安全性の 7 性質を達成するインターネット投票モデルを提案する. この投票モデルは, 権利を有する者のみが参加可能でありながら匿名性が保持される性質を持つことから, EC サイトにおける購入者限定の商品レビューなど選挙における投票以外の活用も期待できる.

2. Zvote

Zerocoin は ZKP を応用した Bitcoin の拡張機能である. Zerocoin では, Bitcoin を一度 Zerocoin に変換 (Mint) し, 再び Bitcoin に復元 (Spend) する際に ZKP を用いることで元のコインと復元後のコインのリンクを不可視化する (図 1).

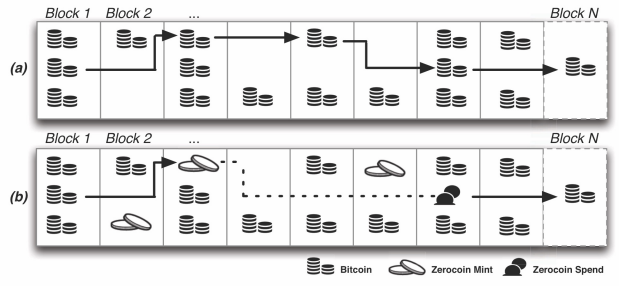

図 1: Two example block chains (出典: [4])

本稿で提案する投票モデル (Zvote) では, このスキームを応用することで TTP を介することなく匿名性と適格性を両立する. Zvote は, 準備期間, 投票期間, 集計期間の 3 段階に分けられる. Zvote の各期間と, 従来の選挙における投票プロセスの対応関係を表 1 に示す.

表 1: Zvote と従来の投票プロセスの対応

Zvote	従来の投票プロセス
準備期間	投票所に赴き, 入場整理券と交換で投票用紙を受け取る.
投票期間	投票用紙に候補者名を記入し, 投票箱に投じる.
集計期間	票の集計が行われ, 得票結果が報じられる.

また, Zvote の主要技術である Zerocoin スキーム, ブロックチェーン, 公開鍵暗号方式が果たす主な役割を従来の投票プロセスになぞらえたものを表 2 に示す.

表 2: Zvote における主要技術の役割

主要技術	役割
Zerocoin スキーム	有権者が持つ記名式の入場整理券と, 無記名の投票用紙の 1 対 1 対応関係を保証する.
公開鍵暗号方式	投票期間中に自分以外の投票内容が見えないようにする.
ブロックチェーン	入場整理券の配布や票の集計を公開の場で行うことで, 管理者による不正を防ぐ.

候補者 n 人の選挙区 X(以下では選挙区 X の管理者のことも同様に X と記す) の有権者 A が Zvote で投票を行う一連のプロセス, 及びその概略 (図 2) を以下に示す.

準備期間: X は, ECElgamal 暗号 [5] に用いる楕円曲線及びその上の巡回群 $\langle G \rangle$ を適切に選び, ハッシュ関数 H を用いて自身の秘密鍵 sk_X, 公開鍵 pk_X, アドレス $H(pk_X)$ を生成する. さらに, n 人

の候補者を $\langle G \rangle$ の各点に重複を避けて対応させた後に以下を公開する.

- 楕円曲線の共通パラメータ及びハッシュ関数 H
- $H(pk_X)$
- 各候補者と $\langle G \rangle$ の点との対応表

A は公開された情報をもとに X と同様の手順で秘密鍵 sk_A, 公開鍵 pk_A, アドレス $H(pk_A)$ を生成し, pk_A と $H(pk_A)$ を本人証明と共に X に提出する. 提出したアドレスが X に承認され選挙人名簿に登録されると, ブロックチェーン上で $H(pk_X)$ から $H(pk_A)$ へ" 投票トークン" が送信される. A は Zerocoin スキームを用いて受け取った投票トークンを Mint する. 以下では A によって Mint された投票トークンを C_A と記す.

投票期間: A は新たに秘密鍵 $sk_{A'}$ を生成し, 同様の手順で公開鍵 $pk_{A'}$, アドレス $H(pk_{A'})$ を生成する. このアドレスの持ち主が A であることは誰も (X でさえ) 知ることは出来ない. 次に, A は投票したい候補者に対応する点を ECElgamal 暗号の手順に従って $pk_{A'}$ を用いて暗号化し, 投票メッセージ $m_{A'}$ を生成する. A は C_A を Spend し, リンクの切れた投票トークンに $m_{A'}$ を添付してブロックチェーン上で $H(pk_{A'})$ に送信する.

集計期間: A は $sk_{A'}$ と投票トークンをブロックチェーン上で $H(pk_{A'})$ から $H(pk_X)$ へ送信する. X は受信した秘密鍵を用いてそのアドレスが投票期間中に送信していた投票メッセージを復号し, 各候補者の得票数を集計する.

集計期間終了後, X は各候補者 $i \in \{1, \ldots, n\}$ に対応する得票結果トランザクション $\{TX_i\}_{1 \leq i \leq n}$ を生成, ネットワークに送信し, 全てがブロックチェーンに記録されたことを確認して選挙を終了する. このとき, TX_i は候補者 i への投票メッセージを含む全てのトランザクションのハッシュ値を参照する.

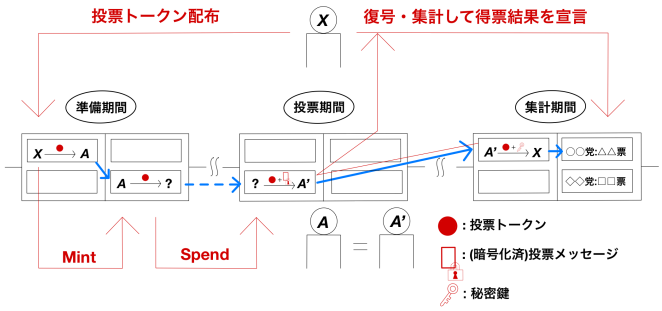

図 2: Zvote の概略

3. 安全性の評価

インターネット投票プロトコルに要求される安全性の 7 つの性質 [2] について, Zvote を評価, 検討する. 匿名性, 適格性, 二重投票の防止は Zerocoin スキームの性質, 公平性は $pk_{A'}$ による投票メッセージの一時的な暗号化, そして頑健性, 個別検証可能性, 総合検証可能性はブロックチェーンの性質及び $sk_{A'}$ の公開により満たされる. 以上より, Zvote は TTP を介することなく安全性の 7 性質を達成する.

参考文献

[1] 湯淺 墾道, “ インターネット投票の実現に向けた検討状況について ”, in 地方自治情報化推進フェア 2018 J-LIS セミナー (2018-10)

[2] 久保田 貴大, “ 日本における安全なインターネット投票の導入に向けて ”, 情報処理学会研究報告, Vol.2014-IS-127, No.1(2014-3).

[3] Electronic Voting Committee. General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia(2016-5).

[4] I. Miers, C. Garman, M. Green, and A. D. Rubin, “ Zerocoin: Anonymous distributed e-cash from bitcoin, ” in Proceedings - IEEE Symposium on Security and Privacy, 2013, pp. 397?411, doi: 10.1109/SP.2013.34.

[5] 清藤武暢, 四方順司, “公開鍵暗号を巡る新しい動き : RSA から楕円曲線暗号へ”, 金融研究, Vol.32, No.3(2013-7).