(410) 情報その他

インターネット投票におけるブロックチェーンとサーバ間のデータ共有方法の提案

Between blockchain and server in Internet voting Proposal of data sharing method

石川 遼太 †　國島 丈生 ††
Ryota Ishikawa † Takeo Kunishima††
† 岡山県立大学大学院　情報系工学研究科 システム工学専攻　†† 岡山県立大学 情報工学部 情報通信工学科

1　はじめに

投票の電子化は、集計の容易さや投票率の向上など多くのメリットが存在しており、現在も多くの研究がされている。しかし、電子投票システムの問題点として投票運営者の不正という問題点があげられる。票がデータとして扱われるため投票運営者の不正が容易であり、票の書き換えや票の複製による水増しなどが行われる危険性がある。その解決策として、暗号資産技術に使用されているブロックチェーンを用いた投票方式が提案されている [5] [6]。

ブロックチェーンの特徴である改ざんが困難な点や取引に透明性があることを用いて、運営者の不正が困難な投票が可能となると考えられている。しかし、ブロックチェーンは透明性を確保するためにデータに誰でもアクセスが可能となっており、そのためインターネット投票においては、票内容の秘匿が問題点としてあげられる。本稿では、ブロックチェーンを用いた場合のインターネット投票の問題点を解決するために、票内容について中央集権型のサーバを用いて投票中の投票者に対して票内容を秘匿しつつつ、ブロックチェーンの特徴を生かした透明性の確保が可能なインターネット投票の方式を提案する。

2　研究背景

Fujioka ら [3] は、以下の条件を満たすインターネット投票プロトコルを安全である（secure）と定義している。

1. 完全性... 全ての票は正しく数えられる.
2. 健全性... 投票が悪意を持った第三者に妨害されない.
3. 匿名性... 投票内容が秘匿にされること.
4. 二重投票の防止.
5. 適格性... 投票の権利を持たない人が投票できない.
6. 公平性... 何も投票への影響を与えない.
7. 検証可能性... 投票者が結果を参照できる.

本稿においても、これらの条件を満たすような手法を提案する。

2.1　ブロックチェーン

ブロックチェーンはデータの追加のみが可能なデータ構造を持つ台帳を，分散的に保持することによりデータの改ざんと消去を不可能とする分散型台帳技術である．ブロックチェーンには以下の大きく 3 つの特徴がある．

1. 不変性 : 台帳に追加されるブロックは直前のブロックを必ず参照する必要がある．それぞれのブロックが直前のブロックのハッシュ値を保持し, そのブロックが連鎖的に繋がっていくことにより改ざんが不可能となっている.
2. 検証可能性 : 台帳は分散的に保存され，同期されることにより，1 つのノードが破壊されても他のノードがネットワークを維持することができる．また，誰でもネットワークに参加できることからオープンな取引が可能となっている.
3. 分散型コンセンサスアルゴリズム : ネットワーク内ではコンセンサスアルゴリズムがデータの追加について決定権を持ち，ノードはデータの追加についてそのアルゴリズムに従う必要がある．ビットコイン [4] では，Proof-of-Work というアルゴリズムが存在しネットワーク参加者の金銭的欲求に基づいて，ネットワークの維持がなされている.

P2P ネットワークの参加者には固有のアドレスが割り当てられており、そのアドレスを用いて金銭のやり取りが行われている。そのやりとりはトランザクションと呼ばれる。

2.2　スマートコントラクト

スマートコントラクトとは、ブロックチェーン上でプログラムを動かす手法であり、ブロックチェーンの特性を生かしたアプリケーションの開発が可能となっている。例として、金銭のやりとりなどがブロックチェーンに記録されるため、より安全な取引が可能となる。その代表的なプラットフォームとして Ethereum[2] があげられる。Ethereum は現在 Dapp（Decentralized Application）の開発の主流であり、本稿でも Ethereum を用いることとする。

3 関連研究

[5] は，初めてブロックチェーンを用いた投票の実験が行われた研究であり，現在も Ethereum[2] のパブリックチェーンにがデプロイされている．パブリックチェーンでの実験のため投票者は 50 人ほどが限界である．

[1] は，2018 年のシエラレオネでの大統領選挙で部分的に使用された投票システムであり，投票の運営局がトークンを購入し，それを投票者に配布することにより投票者は投票権を得るという手法である．このシステムの問題点は購入したトークンを投票者に配布した後に，もし投票者が投票しなかった場合に損失が生じることである．

日本でも [6] において，ブロックチェーンを用いた投票が行われている．本人認証として，マイナンバーカードをリーダにかざして認証を行い，その際にカードの IC チップに内蔵している電子証明書の署名用パスワード（6 桁から 16 桁の英数字）の入力を必須要件としている．この動作により本人認証を行い，投票内容をブロックチェーンに記録している．その後投票者はブロックチェーンに記録された投票データを見直すことができる．

4 提案プロトコル

本手法では個人認証については P2P ネットワークのアドレスによって本人認証がすでに行われており、サーバにそのアドレスが登録されているものとする。また本手法ではハッシュ関数を使用する。ハッシュ関数の特徴である、同じハッシュ値が得られる異なる入力を見つけることが非常に困難である点を用いて不正の困難な投票プロトコルの実現を目指す。

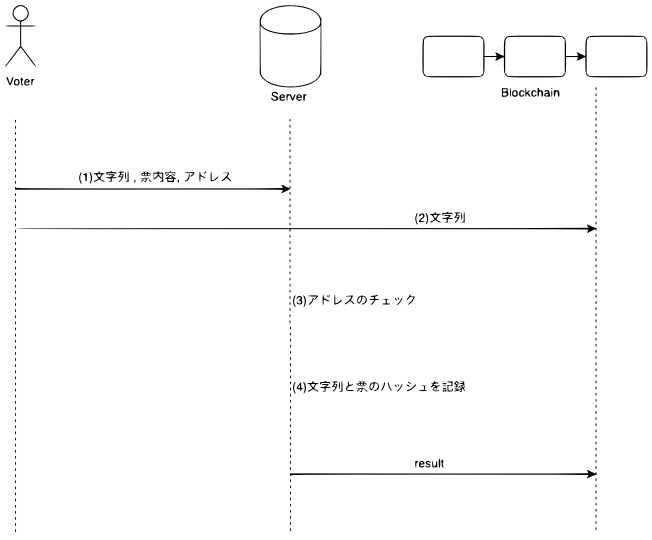

図 1: 投票プロセス 1

図 1 に投票の流れの前半を示す。

(1) はじめに投票者は「ある文字列」と「票」と「自身が保持しているブロックチェーン上でのアドレス」の 3 つをサーバに送信する。ある文字列は文字数制限を設け、投票者が任意に決める。票は候補者の名前を送信する。

(2) 投票者はブロックチェーンに文字列を送信する。

(3) サーバは送られてきたアドレスが登録されている正規のものかを確認し、仮に登録されていないアドレスの場合はその票を破棄する。また、アドレスを送信してきた投票者がブロックチェーンに文字列を送信しているかを確認し、送信されていないアドレスからの票も破棄する。この作業により、投票者はブロックチェーンに必ず自身の票を送信していることが確約される。アドレスからの票がすでに投票されている場合は二重投票とみなし、新たな票を破棄する。

(4) 以上の作業の終了後、全ての文字列を結合したもののハッシュ（H_1）を計算する。また、全ての票を結合したもののハッシュ（H_2）も作成する。これら 2 つのハッシュを結合し、さらに結合後の文字列のハッシュ（H_3）も作成する。そのハッシュ（H_3）をブロックチェーンに記録する。

図 2 に投票の流れの後半を示す。

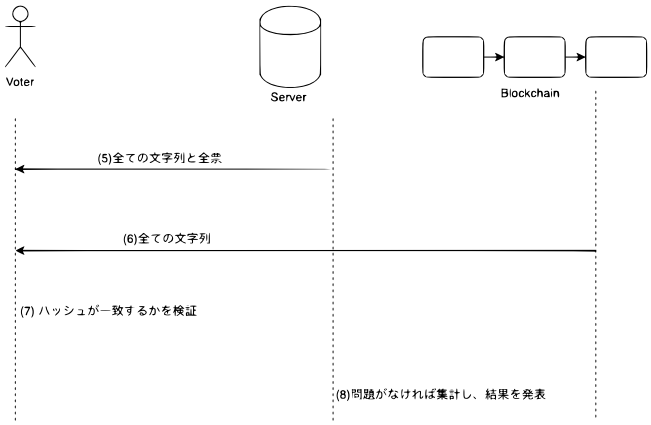

図 2: 投票プロセス 2

(5) 検証のため、投票者は全票と全文字列をサーバから取得する。

(6) 投票者はさらにブロックチェーンからは文字列を取得する。

(7) 投票者は、ハッシュ関数の性質である入力が少しでも変われば出力は異なるものとなる性質を用いて、票が正しく取り扱われているかを確認する。「票のハッシュとブロックチェーンからの文字列のハッシュ（H_4）」と「票のハッシュとサーバからの文字列のハッシュ（H_5）」の 2 組についてハッシュ

を計算し、2 組が一致するかを検証する。ハッシュ関数の特性から 1 文字でも改変されていればハッシュが一致することはない。投票プロセスの前半で投票者がブロックチェーンに記録した文字列はブロックチェーンの改竄できないという特性から変更は不可能である。したがって、$H4 = H5$ となる場合は正しく票が扱われていることがわかる。

(8) 問題がなければ集計し投票結果を発表する。

5 考察

まず、第二章で述べた Fujioka ら [3] のインターネット投票が満たすべき要件について考察する。

1. 完全性... 票内容の変更や票の削除が行われた場合にはハッシュ関数の性質から、投票者は票が正しく扱われていないことを検知できる。
2. 健全性... 投票が悪意を持った第三者に妨害されない.
3. 匿名性... アドレスと票内容の関連性についての情報を持つのはサーバのみであるため、投票運営者が情報を秘匿している限り投票者の匿名性は守られる。
4. 二重投票の防止... 一アドレスにつき一票のみの制約を設けることにより二重投票は防止できる。
5. 適格性... アドレスにより投票権を持つ者のみが投票できる。
6. 公平性... ブロックチェーンに送信された文字列のトランザクションの送信個数を数えることにより、現時点での投票者数が明確になってしまうため公平性については満たしていない。
7. 検証可能性... 第 4 章で述べたとおり、自身で計算したハッシュが一致するかを検証することにより投票者は自身の票が正しく取り扱われているかを検証できる。

本提案システムは投票プロセスの前半にサーバに票と文字列とアドレスを送る際に、同様の文字列をブロックチェーンにも送信する。ブロックチェーンは改竄困難であり、したがって送信された文字列も同様に改竄困難である。その文字列を用いてハッシュの計算をすることにより、ハッシュ関数の出力が一致しているかを確認することでサーバが正しく票を取り扱っているかを投票者はチェックすることができる。何事も投票への影響を与えないという公平性については、ブロックチェーンの性質である取引がオープンである点からトランザクションの数を数えることにより投票数がわかってしまう。この問題点に関しては、取引がある一定のユーザにしか見えないようなブロックチェーンを使用するなどの方法があげられる。

6 結論

ブロックチェーンを用いたインターネット投票において問題となる票内容の秘匿について、投票運営者の不正を防ぎつつ投票者の票内容の秘匿が可能なシステムを提案した。今後の課題としては、ブロックチェーンの選定や構築、公平性を満たすシステムの検討などがあげられる。

参考文献

[1] Agora. https://www.agora.vote/.

[2] Ethereum. https://www.ethereum.org.

[3] Atsushi Fujioka, Tatsuaki Okamato, and Kazuo Ohta. A practical secret voting scheme for large scale elections. *In Advances in cryptology-AUSCRYPT'92*, pages 244–251, 1993.

[4] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical report.

[5] Siamak F.Shahandashti Patrick McCorry and Feng Hao. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. 2017. https://eprint.iacr.org/2017/110.pdf.

[6] 湯淺 墾道. マイナンバーカードとブロックチェーン、つくば市のネット投票で実証したこと. 都道府県選挙管理委員会連合会, 選挙：選挙や政治に関する総合情報誌選挙 : 選挙や政治に関する総合情報誌, pages 9–15, 2018.