N-015

プライベートチェーンを用いたインターネット投票
Using private blockchain for evoting

石川 遼太[1)]　　國島 丈生[1)]
Ryota Ishikawa　Takeo Kunishima

1　序論

インターネット投票はその利便性から多くの研究がなされている. しかし, インターネット投票には多くの問題点が存在している．票をデータとして扱うことによる運営の不正の容易さや不透明性などである．本研究では, 暗号資産に用いられている分散型台帳技術であるブロックチェーンがもつ取引の透明性と記録の不可逆性を用いてインターネット投票の問題点の解決を目指す.

2　背景

2.1　インターネット投票

インターネット投票は, 遠方からの投票が可能になる点や集計の容易さなどのメリットから多くの研究が行われている. 電子投票での研究はブラインド署名 [5] を用いたものと MIX-net [6] を用いたものに大別される．ブラインド署名とは，第三者が送信者の送信内容を見る事なく，その内容について署名をすることで，送信者のプライバシーを守りつつ送信内容の正しさを保証する方式である. MIX-net [6] とは，票の暗号化を複数回かけて，復号時にいくつかのサーバで順に復号していくことにより票の秘匿性を保証するものである. 単一のサーバで復号しない事により，投票内容を秘匿するという方式である．

2.2　ブロックチェーン

ブロックチェーンとは，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, それら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の決定権を持ち，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 [7] 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．

本稿ではこれらのブロックチェーンの特徴を活かしてインターネット投票の不透明さの改善を測ると共に，実際のブロックチェーンを用いたアプリケーションの構築についても検証する．

2.3　ブロックチェーンの種類

ブロックチェーンには, パブリックチェーンとプライベートチェーンの大きく 2 つの種類がある. パブリックチェーンは，誰でもデータを見ることや書き込むことができ，一方プライベートチェーンは，データを見ることができる人を制限することができる. また, パブリックチェーンは利用者が多く, 取引速度の遅さや手数料の高騰が起こることがある. 一方プライベートチェーンは, 利用者を制限することにより, これらのスケーラビリティについての問題が解決可能であると考えられている.

また，近年ブロックチェーン上でプログラムを動作させるというスマートコントラクトの開発が盛んであり，パブリックチェーンにも多くのアプリケーションがデプロイされている．スマートコントラクトは，ブロックチェーン上にコントラクト（契約）を記録し自動で処理を行うシステムのことであり，ブロックチェーンの特徴を生かすことにより不動産登記などへの応用が期待されている．

3　関連研究

[2] 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，実際に Ethereum[1] のパブリックチェーンにデプロイされている．前述の通り，現在の Ethereum パブリックチェーンはネットワーク参加者の増加やトランザクションの増加からスケーラビリティに懸念が残る状態であり，[2] においても投票者は 50 人ほどが限界である．

[3] 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，そのトークン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．投票人数が確定している会議などでの投票ならば，発行したトークンは無駄なく使用されることが想定されるが，確定していない場合には，投票行為自体を行わない者もいるため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がある．

日本でも [4] 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，本人認証システムからの承認を得たのちに投票を行うという手法である．投票内容はブロックチェーンに記録されており，投票後，投票者は記録された投票データを確認できる．

4　提案手法

本研究の特徴は 2 点ある．1 つ目は，パブリックチェーンではなくプライベートチェーンを用いる点であ

1）　岡山県立大学 Okayama Prefectural University

る．パブリックチェーンではトランザクションの手数料が発生し，投票者と運営局ともに金銭的コストがかかる．運営局は投票者の数に比例して手数料が増えるため人数が増加すると多大なコストがかかる．プライベートチェーンの場合には金銭的コストはかからないため，プライベートチェーンを用いることで金銭的コストを減らすことができる．

２つ目は，ブロックチェーンとユーザの間にサーバーを介さない点である．サーバを介した場合には，ブロックチェーンに記録したデータをユーザを呼び出す場合にサーバを経由するため透明性が落ちてしまう問題がある．そのため本研究では透明性を重視するためサーバを介さない．

本研究のスマートコントラクトのプラットフォームとしては，現在の分散型アプリケーションの開発がもっとも活発である Ethereum[1] を選択し，ブラウザから投票できるシステムを構築した．

以下では, プライベートチェーンの構築, 投票コントラクトの作成について説明する．

4.1　プライベートチェーンの構築

今回は Ethereum クライアントとして geth[8] を用いた．また, 投票者が投票できるためには作成したブロックチェーンがどこからでもアクセスできる必要がある．そこで今回はクラウドにプライベートチェーンをデプロイし，IP アドレスを指定すればアクセスできるようにした．

4.2　投票コントラクト

投票コントラクトは，Ethereum プライベートネット上にデプロイし geth[8] を用いてアクセス可能となっている．投票の流れは図 1 のようになっている．

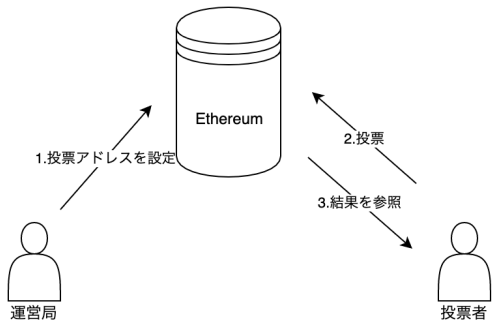

図 1　投票プロセス

1. 運営者が投票者のアドレスを認定.
2. 投票者が自身の票を送信する.
3. 結果をブロックチェーンから読み取る.

投票コントラクトは投票アドレス以外の投票は受け付けないように設定しており，同アドレスからの投票は一回までとして，二重投票も受け付けないようにしている．

また，大量のデータが送信されることが考えられるが，プライベートチェーン上にデプロイすることにより手数料がかからず無料で投票を行うことが可能となっている．投票の終了については，運営アドレスからのみ投票の終了を設定することができ，投票終了の場合にはコントラクトの全ての機能を停止するように構築した．

4.2.1　アプリケーションの構築について

ブラウザとデプロイしたコントラクトとの連携には MetaMask [10] を使用した．Metamask を使用することにより, プライベートチェーンに接続することができ, ユーザのアドレスを用いて図 2 のようにフロントエンドからコントラクトの機能を呼び出すことができる．

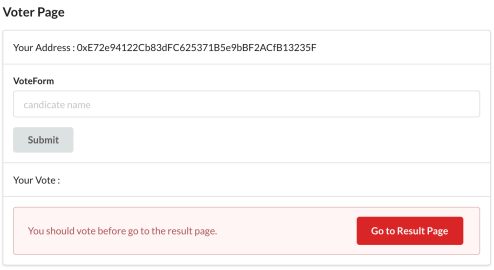

図 2　投票フォーム

4.3　問題点

本研究の問題点として, 本人認証の方法に課題があると考えられる. 投票者のアドレスの承認をどのように行うかは問題である. 実際の実験が行われた [4], [9] では，どちらも IC カードを利用しており，本研究では, 本人認証について有効な手法は取られていないと考えられる．

また，投票結果をブロックチェーンに記録することにより常にオープンになっており，投票結果に影響してしまう可能性がある. そこで，フロントエンド側では,「投票者が投票を終えている」かつ「投票が終了している」条件ではないと結果を見れないように実装した．

5　結論

本稿では，プライベートブロックチェーンを用いたインターネット投票のシステムの構築について述べた．ブロックチェーンと投票者が直接通信することにより，よりオープンな投票が可能となり運営の不正が困難な投票が可能になると考えられる．

ブロックチェーンの持つ特徴を生かしてインターネット投票システム面での問題点を解決することは可能であると考えられるが，本人認証などのシステム外の問題を解決することは難しく今後の課題として挙げられる．

参考文献

[1] Ethereum https://www.ethereum.org
[2] Patrick McCorry, Siamak F.Shahandashti and Feng Hao. A Smart Contract for Boardroom Voting with Maximum Voter Privacy https://eprint.iacr.org/2017/110.pdf, 2017
[3] Agora. https://www.agora.vote/
[4] 市ノ澤 充 . 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 71(12),9-15,2018-12
[5] David Chaum. Blind signatures for untraceable payments.
[6] David L.Chaum.Untraceable electronic mail, return addresses,and digital pseudonyms. Communications of the ACM, 1981.
[7] Satoshi Nakamoto.Bitcoin: A Peer-to-Peer Electronic Cash System. Technical report.
[8] Go Ethereum https://geth.ethereum.org
[9] 湯淺 墾道. エストニアの電子投票. 九州国際大学 社会文化研究所紀要, pages 39-71, 2009.
[10] MetaMask https://metamask.io