論 文 内 容 の 要 旨

博士論文題目

The Bitcoin Network as Platform for Role-Based Access Control and Electronic Voting: Using Blockchain-Based Technology to Create Innovative Systems

ロールベースアクセス制御および電子投票方式の実現に向けた Bitcoin 基盤の応用：ブロックチェーン技術を利用した新しいアプローチ

氏 名 Jason Paul Miranda Cruz

（論文内容の要旨）（1，200字程度）

情報通信機器の発達と普及により，日常活動における様々な行為を電子的に行うことが可能となりつつある．その一方，デジタル情報の特性により，通常の世界では容易に行えることでも，コンピュータネットワーク上で実現するのが非常に難しくなる場合もある．この現象はセキュリティ的要因が関連する場合に顕著であり，たとえば，身分証や公文書の複製・偽造が困難であることに安全性を依拠する行為の多くは，そのままの形では，デジタルの世界で実現できないことが多い．本論文では，そのような問題に対処するため，仮想通貨として知られるビットコインを利用して，属性証明と電子投票のサービスを安全に実現する手段を検討している．

本論文第１章では，ビットコインの概要と本研究の発想について述べたあと，属性証明を中核として構成されるロールベースアクセス制御方式，選挙管理者に対しても秘匿性の確保される電子投票について，既存研究を概観し，問題点を指摘している．

第２章は，ビットコインに関する詳細な説明である．ビットコインアドレスやトランザクション，ブロックチェーン，マイニングの仕組み等について詳細に述べ，懸念される事項等についても問題点が整理されている．また，ビットコイン専用の ATM やプリペイドカードなど，仮想通貨とリアルの世界との接点についての説明も本章にて与えられている．のちの第４章の議論では，リアルの世界におけるモノ（プリペイドカード）を用いて匿名性を確保していることもあり，現実世界という文脈のなかでビットコインを認識しておくことは重要である．また，ビットコインを単なる仮想通貨と理解するのではなく，様々な

サービスを実現するための基盤としてとらえる着眼点についても，本章で紹介されている．

第３章では，ビットコインを基盤として利用することで，属性証明を実現する方法について議論が展開されている．ここで問題とされているのは，ロール（個人の属性や肩書等）を発行する組織と，サービスを提供する組織とが異なる場合の属性証明の実現方式である．現実の世界では，デジタル証明書の利用や組織間でのフェデレーション構築等により標記問題に対処しているが，実現コストが高い，既存フェデレーションへの参入に障壁がある場合が多い等，運用上の問題が生じてしまう．本研究では，ロール発行の事実をトランザクションとして表現することにより，導入ハードルの低い属性証明を実現する方式が検討されている．

第４章では，電子投票の実現にビットコインを利用する方式が検討されている．物理的な制約により不正行為を抑止可能な現実の選挙とは異なり，電子投票においては，選挙管理者に非常に大きな権限と自由度が与えられることになる．公正な投票を実現するためには，そのような選挙管理者からも投票内容を秘匿できる方式が必要となる．本研究では，選挙に関連する各種行為をビットコインのトランザクションとして表現することで，安全でスケーラブルな電子投票の方式を提案している．

第５章は論文全体の総括である．多くのセキュアサービスでは，信頼できる情報共有基盤の実現が重要な鍵となる．ビットコインやブロックチェーンの仕組みは，本論文で直接議論した属性証明や電子投票だけでなく，他の多くのサービスの実現にも貢献できる可能性を持つ旨が指摘されている．

氏　名	Jason P. M. Cruz

（論文審査結果の要旨）（1枚　1，200字程度）

本論文では，セキュリティ的な要件が必要となるサービスの実現にあたり，仮想通貨として知られるビットコインのメカニズムを情報共有・流通の基盤として利用するアプローチが検討されている．具体的には，(1) 複数の組織にまたがる属性証明，(2) 投票内容の秘匿性を備えた匿名性電子投票の 2 種のサービスに対するケーススタディとなっており，それぞれのサービスの実現方法およびその安全性について議論が展開されている．

機密情報や有価サービス等へのアクセスを適切に制御するためには，個人が持つロール（属性や身分，肩書等）を確認できる仕組み，いわゆる属性証明が必要となる．不正者はロールを偽ってアクセスを試みる可能性があるため，ロール偽装を防ぐことが属性証明の重要な要件となる．個人に身分や肩書を付与する主体（ロール発行者）と，情報やサービスへのアクセスを提供する主体（サービス提供者）が異なる場合，組織の壁をまたがって属性証明を行う必要があり，従来は，デジタル署名の利用や組織間の連携（内部データの相互参照）等により標記問題に対応することが多かった．これに対し本研究では，ロール発行の事実をビットコインのトランザクションとして表現することで，属性証明を実現する手法が提案されている．個人の属性の検証が容易である，ロール偽装がきわめて困難であるといった基礎的要件に加え，比較的小さなコストで，誰でもロール発行が可能になるといった優位性が示されている．

電子投票は様々なセキュリティ要件が複雑に絡み合うサービスであり，基礎的な研究が 1980 年代から盛んに行われてきた．理論的には安全とされる方式がいくつか提案されているが，完全な匿名通信路の存在等，現実性に乏しい前提条件が必要になったり，参加者全員の協調計算が必要になる等，スケーラビリティに問題があったりするため，実用化には結びついていないのが現状である．本研究では，有権者登録や投票行為等をすべてビットコインのトランザクションとして表現する方式が提案されており，提案方式が，電子投票に求められる様々な要件を満足することが示されている．方式の一部にビットコインのプリペイドカードを利用することで匿名性を確保しており，サイバースペースの弱点をリアルスペースでの運用で回避するという点が興味深い．

誰でも内容を確認でき，事後に内容を改ざんすることの困難な情報共有基盤は，多くのセキュリティサービスの実現に役立つと考えられる．本研究の貢献は，そのような基盤の実現に，ビットコインの仕組みが流用可能であることを明らかにした点である．この着眼点は高い汎用性を有するものであり，属性証明や電子投票以外の様々なセキュアサービスについても，同様のアプローチを適用できる可能性が高い．セキュリティ基礎研究の実用化に大きな貢献を与える可能性があると判断されるため，本論文を博士（工学）の学位論文として価値あるものと認める．