講演番号：31

マイナンバーカードによる本人認証可能な ERC721 コントラクトの設計

Design of identity verifiable ERC721 by Individual Number Card

神野 ひかり　小川 猛志

Hikari KANNO　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

近年，ブロックチェーンで管理される仮想通貨やNFTなどの資産の盗難被害が増加している．本稿では，マイナンバーカードの電子署名を利用し本人認証を行う機能をスマートコントラクトで実現することで，ユーザの負担を極力増やさず既存ブロックチェーン上の資産の盗難被害を削減する仕組みを提案する．

2. ブロックチェーン上の取引の概要と課題

ブロックチェーンとは非中央集権型の電子台帳である．同一の台帳が取引参加者の端末に分散して記録されるため取引の透明性が高い．台帳の更新コマンド(トランザクション，以下 Tx)はブロックにまとめられ，ブロック単位で台帳に反映される．ブロックはハッシュ値で繋がってチェーン状の構造を持ち，ブロックの内容を書き換えるとハッシュ値が変化し前後の整合性を保つことが非常に難しいため，高い耐改ざん性を持つ．ある資産(例:仮想通貨)を端末 A から端末 B に送金する場合，端末 A は端末 B への送金要求に当該ブロックチェーンのアカウントの秘密鍵で署名した Tx を発行する．他ノードが当該署名を検証し有効であれば当該 Tx はブロックに格納され台帳に反映されて B の資産となる．秘密鍵が漏洩すると全ての資産を盗難される可能性があるため多要素認証の適用が望ましい．ただしユーザの負担を増やさず，また既存のブロックチェーンには影響せずに実現できる仕組みが必要と考えている．

3. 既存技術とその課題

従来銀行等では，秘密情報の複数化や，携帯電話やメール，生体情報などを多要素認証に活用する例が多いが，以下の理由によりマイナンバーカード(以下 MC)の適用が良いと考えた．

・普及率が高い

・MC 内の秘密鍵で署名可能であり，秘密鍵の抜き取りは困難．

MC をブロックチェーンの認証に適用する既存研究として，web3 ウォレットがある[3]．この研究では，主要なブロックチェーンの一つであるイーサリアムで今後実用化予定である Account Abstraction(以下 AA)を活用している．AA は，既存のイーサリアムでは実施できない「ユーザのアカウントからの自動引き落とし」などを可能にする仕組みとして期待されている．AA ではブロックチェーン外の集中サーバ(Bundler)が各ユーザと契約して，当該 Bundler 専用のスマートコントラクト内のデータとして各ユーザの資産を管理する．よってユーザはイーサリアムのアカウントは持たない．ユーザが送金をしたい場合は Bundler に送金を依頼し，Bundler が複数の依頼を束ねてひとつの Tx に集約して前述のコントラクト内データを書き換える．集中サーバが端末を認証する方法は自由に設計できるが，この研究では MC をカードリーダにかざして MC の署名を Bundler に送信し，MC の署名のみで取引を承認する仕組みを提案している．

この既存研究は AA を前提としているため以下の課題がある．

・トラストフルな Bundler が必要であり完全な非中央集権型ではない．

・現状のイーサリアムの仕様制限に依存しており汎用性が低い．

4. 提案手法

提案手法での資産の移動手順を図 1 に示す．ユーザは当該ブロックチェーンにアカウント(以下 OA)を持ち既存の資産がある，と仮定する．ユーザは「取引時に MC による認証も必要としたい資産」，「当該資産の所有者」，及び「所有者の MC の公開鍵」を 1 組として資産管理用スマートコントラクト(以下 AMC)に登録し資産を AMC に預ける．他ユーザに送金したい際には，OA と MC の双方の署名を付与した Tx を作成し AMC 宛に発行する．AMC はそれらを検証し有効であれば資産の移動を行う．

提案手法では Bundler 等のトラストポイントは存在せず，またイーサリアム以外の既存や今後登場するチェーンにも適用できる手法と考えている．

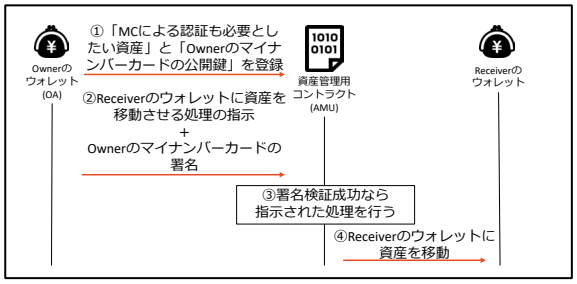

図 1. 提案手法での資産移動手順

5. 試作による実装結果

イーサリアム上で ERC721 標準準拠の NFT をユーザから預かる AMC を開発した．当該 AMC に疑似ユーザの MC 公開鍵と NFT 資産を登録し，当該ユーザの OA の秘密鍵と MC の秘密鍵で署名した Tx を発行して，当該 AMC が MC の RSA 署名を検証し，成功すると NFT の持ち主が正しく変更されることを確認した．

6. まとめと今後の課題

ブロックチェーンアカウントの署名に加えてマイナンバーカードの署名をスマートコントラクトにより確認することで，既存ブロックチェーン上の資産の盗難被害を削減する仕組みを提案し，試作により問題なく動作することを確認した．実サービスへの適用にはスマートコントラクトがインターネット内にある MC の証明書失効リストを確認する必要があるが未実装である．また現状の実装は RSA 署名検証の計算量が大きくガス代(Tx 手数料)が高くなる懸念があるため計算量の削減が課題である．

参考文献

[1] solidity-BigNumber | firoorg, https://github. com/firoorg/solidity-BigNumber/, 参照 2023-01-03

[2] ERC-721 マーケットを実装する方法 | Ethereum. org, https://ethereum. org/ja/developers/tutorials/how-to-implement-an-erc721-market/, 参照 2023-01-03

[3] マイナンバーカードを活用した web3 ウォレットのご紹介 | a42 株式会社, 1_mynawallet_public. pdf, 2023-06-07 発行