CL-006

ブロックチェーンのための認証基盤に基づいた NFT の使用権の信頼できる貸与と借用を実現する方法の提案
A Trustable NFT Lending Method Using Self-Sovereign Identity for Blockchain

首藤 健一† 山﨑 重一郎†
Kenichi Shutou Shigeichiro Yamasaki

1. はじめに

本研究の目的は NFT によって管理される資産を所有権を移転することなく使用権のみを一時的に貸与する安全で信頼できる方法を提案するものである。その応用例として,個人がスマートロックを備えた自分の部屋を旅行者に貸与するシェアリングサービスを想定しそのリスクを回避するための当事者の認証基盤とトラストサービスを試作した.

2. 目的

本研究の大きな目的はブロックチェーンの利点を損なうことなくブロックチェーンを信頼できる社会基盤にする方法を提案することである。本研究では特に以下の２点に注目する。

2.1 デジタル資産の使用権のみの貸与を可能する方法の提案

デジタル資産に対して使用権のみ を他者に貸与する方法の実現である。例えば、資産(スマ ートロックなど)の所有権は保持したままその排他的使用 権のみを特定の者(借用者)に一時的に貸与することを可 能にする。

2.2 ブロックチェーン上の当事者のトラスト基盤の提案

現在のブロックチェーン上のサービスを利用し個人間で取引を行おうとした場合、当事者の実在性を もう一方の当事者側から確認できない点、責任を負っている信頼可能な主体がいない点において、 経済活動や社会基盤として利用するには不向きな側面が見られる。

ブロックチェーン上で資産を個人間で貸与する際に必要となる要素としてトラストが必要である という観点から貸与の為のトラストの元となる構造を構築することを目的とする。 「トラスト」は、Roger・Mayer らの文献の定義より、"トラストとは,その相手への監視や制御かどうか に関係なく,相手が自分にとって重要な行動をとってくれるという期待に基づいて,相手の行動に自身の 「ヴァルネラビリティ(vulnerability)」を託す意思である"とあり、この定義に登場する ヴァルネラビリティという用語は、ここでは人が何か行動しようとする時にそれを阻む「弱点」や「リスク」など,人が感じる恐怖や不安の対象一般のこととします。

2.3 ブロックチェーンによる革新と課題

ブロックチェーンは、希少性,唯一性を持つデジタルデータ(デジタル資産)を実現した。これらは、ソフトウェアのみで人から人への転々譲渡が可能になった。デジタル資産は、ブロックチェーン上のトークンを通じた所有権の移転に関するプロトコルなども整理された。

しかし、デジタル資産やそれと連携する現実の資産の使用や収益の実現方法は未整備であるため唯一性を持つデジタル資産（NFT)の使用権に関するプロトコルが必要であると考える。

また、ブロックチェーンは、トラストレストラストと呼ばれる他の参加者の誰も信じていない、信頼できる第三者が存在しないネットワークの、暗号技術とコードの透明性によるトラスト上で多くの資産を預けている。

しかし、トラストレストラストはマネーロンダリング,経済制裁,違法取引など,重要な規制と対立する可能性を持っている。

3. 前提

本研究ではデジタル資産を NFT と結びつけていることとし、ユーティリティトークンと呼ばれる特定の商品やサービスへのアクセスを有効とするトークンを使用していることを前提とする。

3.1 NFT

Non-Fungible-Token (NFT) は EIP-721(Ethereum Improvement Proposals)で導入された、Deed と呼ばれる不動産などの 所有を証明する法的証書のような代替え不可能なトークン のことである。価値によって定義される他の古典的な暗号通貨と異なり、NFT は独自の特性によって定義されるため、他のトークンと交換することはできない。NFT は、イーサリアムブロックチェーンを公開台帳として使用することで追跡可能な、あらゆるデジタルデータの一意の部分の所有者を割り当てたり特定したりする機能を提供する。歴史的には、NFT は主にデジタルアートや収集品の所有権を表すために使用されてきたが、車の権利証書、イベントのチケット、法的文書、署名など、物理的で実世界のアイテムを表すためにも使用できる。”

3.2 ユーティリティトークン

EBA（欧州銀行協会）の定義によれば、ユーティリティトークンは、特定の商品やサービスへのアクセスを有効にするものです．多くの場合，DLT プラットフォームを使用して提供されますが，商品やサービスの支払い手段としては使われません。

4. 本研究の想定シナリオ

ある学生が長期休暇中で帰省中の自身の部屋を旅行者(大学生)に貸し出すサービスを想定し、このサービスを信頼して利用されるものにする。

†近畿大学 大学院 産業理工学研究科 Kindai University Graduate School of Humanity-Oriented Science and Engineering

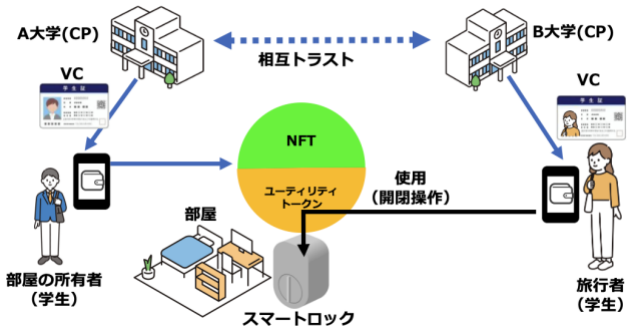

図 1 学生アパートのシェアリングサービス

4.1 想定するシナリオにおけるリスク

今回の想定するシナリオにおいてのリスクは、部屋の貸与者からの視点と旅行者からの視点で分かれる。

部屋の貸与者の視点でのリスクは、

- 部屋を汚される。
- 備品や家具などの破損
- 電気代や水道やガスなどの浪費
- 騒音などの評判の毀損

などが挙げられる。

旅行者からの視点でのリスクは、

- スマートロックが壊れていて部屋を利用できない
- 備品や家具や寝具が壊れていて利用できない
- 不注意による破損や汚損発生時の賠償金が高額
- 周辺環境が事前情報と異なって悪い

などといった両者とも様々なリスクが考えられる。

4.2 提案するトラスト構造（decentralized 4 コーナーモデル)

Payment Card Industry Data Security Standard (PCI DSS) によって標準化されているモデルであり、

この構造により、図 2 のようなクレデンシャル発行者がリスク評価を行い，トラスト情報として提供する。

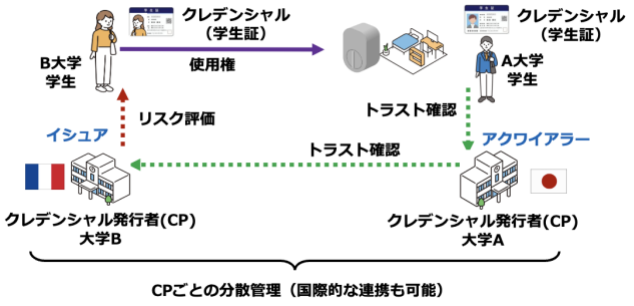

図 2decentralized 4 コーナーモデル

5. NFT の使用権のみを貸与する方法の提案

5.1 所有権とは

所有権は日本の法律では、民法(明治二十九年法律第八十 九号)第二編第三章 所有権 (以下「所有権」とする)に 関する記述の第二百六条にて書かれている。その中で、”所有者は、法令の制限内において、自由にその所有物の使用、収益及び処分をする権利を有する。” とある。つまり、所有権は資産への排他的な支配を行う，物権(有体物)に対 する処分する権利、使用する権利、収益を得る権利を含む 統合的な権利であるので、無体物(デジタルデータなど) に対する所有の法的根拠はない。

5.2 NFT の構造における資産と所有者の関係

NFT は、ブロックチェーン上に Deed を実現する手段であり、所有者という概念は NFT の属性データの一つに過ぎない。

5.3 ERC721

ERC721 は、Ethereum ブロックチェーンの NFT の標準仕様の一つである。主キーは、ERC721 で実現する Deed を識別する ID としている。参照する資産の所有関係の証明意図したデータ ERC721 Metadata と呼ばれるものを参照する。

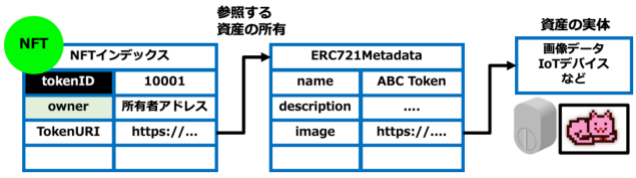

図 3 ERC721

5.4 NFT の処分

NFT の処分は、資産(NFT)を所有する主体が，他者に所有権を渡すことである。所有者は、その主体が所持するワレットと呼ばれるソフトウェアの公開鍵と秘密鍵のペアによって識別される。

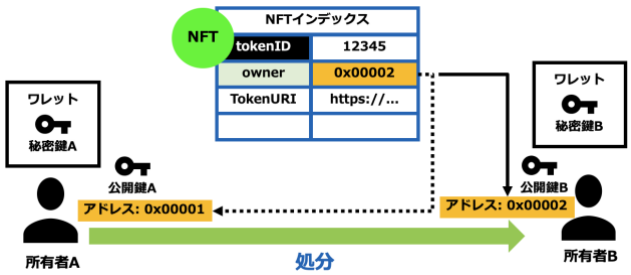

図 4 NFT の処分

5.5 NFT の使用

NFT 自体には排他的な使用権は存在しない。NFT の機能は 本質的にそれが参照する対象の所有権の証書に過ぎない。NFT 自体には排他的な使用権を実現する手段は存在しない。

5.6 NFT の収益

NFT 自体には排他的な使用権を設定できれば、使用権の貸与（使用料）による収益が可能になると考えられる。

5.7 ERC4907 (貸与可能な NFT の標準)

ERC4097 は、EIP-721 の拡張であり、User という追加のロールと Expires という User に対して付与できる時間およ

び、User ロールが自動的に取り消される時間に関する値を記録できる。この仕様により、NFT は他者に対して貸与することが容易となった。

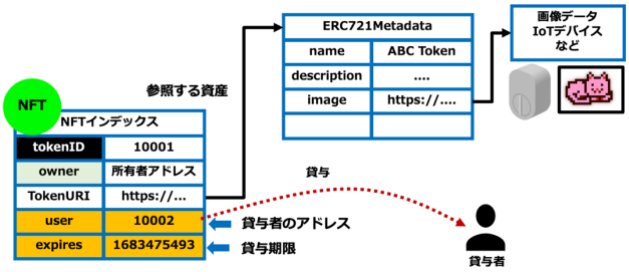

図 5 ERC4907

5.8 ユーティリティトークンによる使用権の表現

ユーティリティトークンはサービスへアクセスするものであり、サービスの支払い手段ではない。

本研究では、ユーティリティトークンは部屋の鍵を操作するスマートロックの使用権を意味する。

5.9 提案する使用権の貸与が可能な NFT

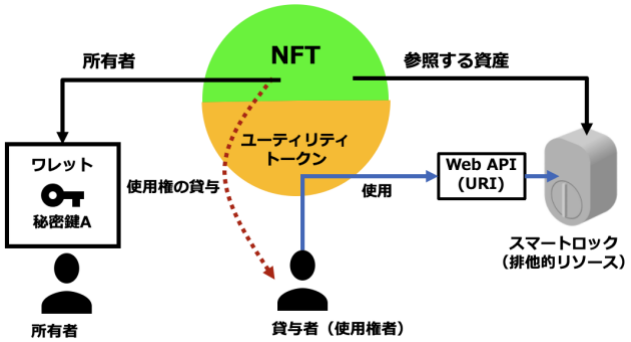

図 6 ERC-4907NFT とユーティリティトークンを一体化することで実現

6. ブロックチェーンのトラスト基盤の提案

6.1 ブロックチェーン上の当事者のトラストの問題

ブロックチェーン上では、当事者の実在性を もう一方の当事者側から確認できない点、責任を負っている信頼可能な主体がいない為、個人間でのサービスでは相手の当事者を信頼することは難しい。

6.1.1 decentralized な当事者のトラストの実現の問題

（国際的な広がりを持つなど）中央集権的でないトラスト基盤であり、リスクに応じたトラストを担保する現実的な手段が必要。特に本人確認と信頼できるアイデンティティが必要である。

6.1.2 当事者のプライバシの問題

トラストのために必要な当事者のアイデンティティ情報の入手可能性と自己情報コントロール権の保証がされている必要がある。

6.1.3 当事者の本人認証の問題

法規制の遵守に関わり、マネーロンダリング防止，テロ資金規制，経済制裁，などの規制対応につながる。

また、ブロックチェーンなどの分散的な組織やネットワークに対してのシビル攻撃対策やガバナンス投票の公平性なども重要である。

6.2 提案するトラスト基盤

6.2.1 本人認証基盤

本人認証基盤として、JPKI などの国民登録に基づく本人認証：FIDO2 とマイナンバーカードの連携または、譲渡不可能トークンによる Web3.0 における本人認証、SBT（ソールバウンド．トークン）が有効であると考える。

6.2.2 W3C 標準による分権的アイデンティティ管理

W3C による分権的なアイデンティティ管理として、自己主権的アイデンティティ管理（SSI）、分権的識別子(DID),検証可能なクレデンシャル(VC)を利用できる。

6.2.3 VC と CP（クレデンシャルプロバイダ）による当事者のトラスト

本研究で想定する、サービスの当事者は大学生であるので検証可能なクレデンシャルは学生証などであり、検証可能なクレデンシャルの発行主体は大学となる。

我々は、de centralized 4-corner model による CP を起点とするトラスト基盤を提案する。

6.2.4 W3C の VC (Verifiable Credentials)

個人の能力や属性を証明するものとして、運転免許や大学の学位やパスポートなどの資格証明が我々の日常生活の一部となっている。VC (Verifiable Credentials) は、このような資格証明を暗号によって安全を確保し、プライバシーを尊重して、機械的に資格証明の検証を Web で表現するものである。

6.2.5 想定するシナリオにおける VC と CP

想定するシナリオとして、アイデンティティを構成する属性である Credential は、発行主体が検証可能でこれはデジタル署名付きのデータとなる。また、Credential を発行する主体はアイデンティティの正真性を確認することができる。

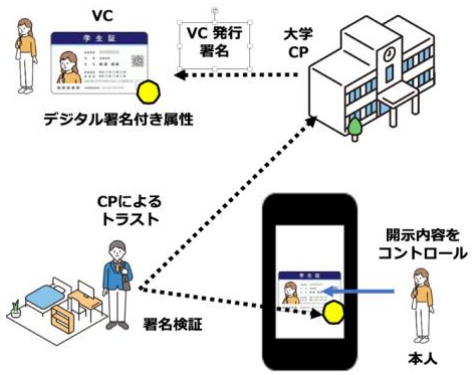

図 7 想定するシナリオにおける VC と CP

7. ブロックチェーンレイヤの要件

スマートロック操作はオフチェーンで実行する必要がある．その理由の一つはガス代の問題あり，もう一つはリアルタイム操作の問題である．さらにリプレイ攻撃対策も必要である．

7.1 オフチェーン処理による使用権の確認方法

オフチェーン実行は下図のような構成によりスマートコントラクトの状態変数の参照のみで更新を伴わないようにすることで実現した．また，タイムスタンプを入力に入れることでリプレイ攻撃への対策を行った．

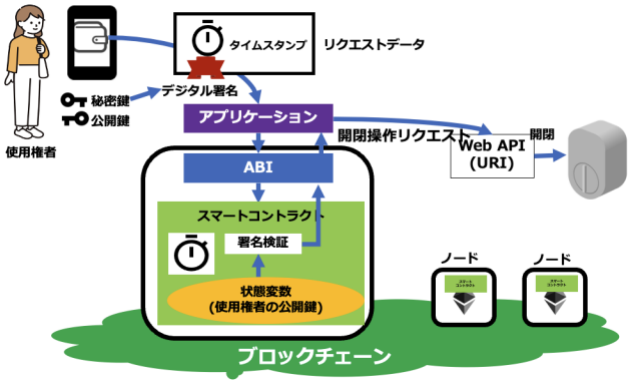

図 8 スマートコントラクトで使用権者のデジタル署名の検証して操作を実行

8. 開発したシステム

8.1 ユーティリティトークン機能を持つ貸与可能な NFT の構成

ERC4907 トークンの仕様をさらに拡張して VC を格納した．

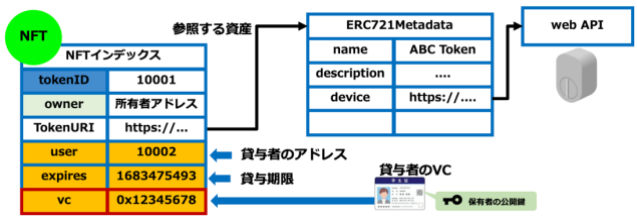

図 9 ERC4907 トークンの仕様をさらに拡張して VC を格納

9. まとめと今後の課題

NFT によって管理される資産を所有権を移転することなく使用権のみを一時的に貸与する安全で信頼できる方法を提案し，その応用例として，個人がスマートロックを備えた自分の部屋を旅行者に貸与するシェアリングサービスを想定しそのリスクを回避するための当事者の認証基盤とトラストサービスを試作した．

参考文献

[1] W3C,Drummond Reed,Manu Sporny,Markus Sabadello,Dave Longley,Christopher Allen, ”Decentralized Identifiers (DIDs) v1.0 W3C Recommendation 19 July 2022”, https://www.asahi-net.or.jp/~ax2s-kmtn/internet/did/REC-did-core-20220719.html
[2] William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs, "EIP-721: Non-Fungible Token Standard," Ethereum Improvement Proposals, no. 721, January 2018. [Online serial]. Available: https://eips.ethereum.org/EIPS/eip-721.
[3] V. A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris and G. C. Polyzos,
[4] "OAuth 2.0 meets Blockchain for Authorization in Constrained IoT Environments,"
[5] 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019, pp. 364-367, doi: 10.1109/WF- IoT.2019.8767223.
[6] 森山 光一,”マイナンバーカードの機能を利活用した民間 ID の認証におけるセキュリティと使い勝手の高いレベルでの両立に向けて”, FIDO Alliance, https://www.soumu.go.jp/main_content/000737274.pdf ,2021
[7] Fido alliance, ”使用概要”, https://fidoalliance.org/
[8] Jeff Hodges (Google), J.C. Jones (Mozilla), Michael B. Jones (Microsoft), Akshay Kumar (Microsoft) , Emil Lundberg (Yubico) , ” Web Authentication:An API for accessing Public Key CredentialsLevel 2”, https://www.w3.org/TR/webauthn/,2021
[9] ”ION”, ,https://identity.foundation/ion/, 2021.
[10] ケビン・ワーバック(著)，山崎重一郎(監修)，山﨑裕貴(翻訳).ブロックチェーンの技術と革新~ブロックチェーンが変える信頼の世界~.ニュートンプレス.2021 年 6 月 15 日.