4L-01

web3 アプリに向けた自己主権型アイデンティティの管理・利用方法

木部龍駿 †　細野繁 †

東京工科大学　コンピュータサイエンス学部 †

1　はじめに

現在, 実生活で身分証明を行う際に用いられる公的証明書には個人情報が直接記載され, 悪用のリスクがある. 同様に, デジタルアイデンティティにも漏洩のリスクと, Web2.0 で影響力のある企業が個人情報を独占し, 中央集権型管理していることから, サイバー攻撃等のリスクからも厳格に保護する必要がある. 実生活とデジタル空間の双方で自らの個人情報を保護し，適切な情報提示とアイデンティティの活用をすることが課題である.

2　自己主権型アイデンティティ

自己主権型アイデンティティ [1] とは，個人が自分自身のアイデンティティを生成し，アルゴリズムに従ってコントロールすることを指す概念である．デジタル上での身分提示をアルゴリズムに従うことを条件に自身のアイデンティティを制御できるようになる．この概念は, ブロックチェーンを用いた分散型 ID 管理 [2] によって実現する.

3　検証可能なデジタル証明書

検証可能なデジタル証明書 [3] とは，資格情報をデジタルでやりとりするためのデータであり, 公的機関などが発行し, 分散台帳を用いて検証することで資格証明することができる.

4　スマートコントラクト

スマートコントラクト [4] とは，ブロックチェーン上で契約を自動化するための仕組みのことを指す．本人も第三者もデータの変更はできず，透明性に優れ，自動化により契約や取引を短時間で遂行し，人為的ミスを無くすことができる.

Self-sovereign identity management and use for web3.0 services

†Tatsuto Kibe,†Shigeru Hosono

†Tokyo University of Technology

5　研究目的

本研究は, 公的証明書を自己主権型の概念に則したデジタル化を行うことで個人情報をユーザの管理下に置くこと目指す. また, 将来的な自己主権型プラットフォーム確立とデジタル証明書を活用するための具体化を提案する.

6　提案手法

本研究の提案として，公的証明書のデジタル化と活用を提案する．具体的には，従来の個人情報が券面に記載される公的証明書について，デジタル化を行う．これにより，従来の公的証明書と異なりデジタルなやり取りが可能になるため，図 1のように，スマートコントラクトを用いたアイデンティティ利用の具体化を提案する.

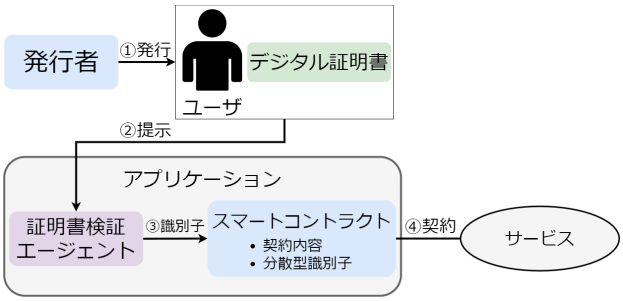

図1　スマートコントラクトを用いた具体化

6.1　分散識別子を用いたスマートコントラクト

図 1では，スマートコントラクトに対して，検証済み証明書の分散型識別子を書き込むことで，ユーザの真正性が②で確保できている状態での契約を行うことができる．ユーザへ発行された証明書をエージェントで検証することで認証を行う．図 1の③では検証済み証明書の分散型識別子をスマートコントラクトの契約に書き込むことで，検証されたユーザとしてコントラクトを実行する.

7　実証

7.1　実装環境

実装環境を下記の表 1に示す. 本研究では５台の VM を構築し，それぞれの構築を行う.

表1　実装環境

OS	Ubuntu Server20.04
分散型 ID	Hyperledger Indy
デジタル証明書	Hyperledger Aries
スマートコントラクト	Solana

7.2　デジタル証明書の発行

デジタル証明書の発行と検証について，実装モデルを図 2として示す．HyperledgerIndy と Aries を用いた実装を行い，証明書の発行と検証を行う．Aries を用いた発行者，ユーザ，検証者の３つの Agent と，Indy を用いた分散台帳の構築を行う.

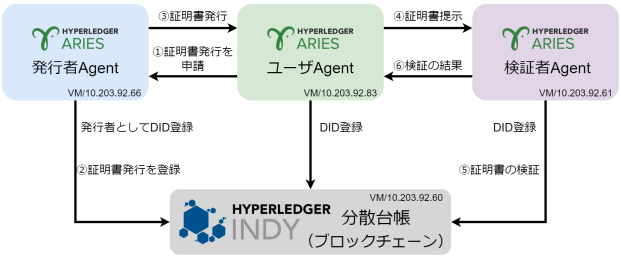

図2　デジタル証明書の発行と検証

7.3　分散型識別子を用いたスマートコントラクト

図 3のように，分散識別子をスマートコントラクトに書き込み，SolanaNetwork へデプロイする．ユーザがクリプト等を含むトランザクションを Solana に対して実行することで契約が執行され，ユーザに対してサービスを提供する.

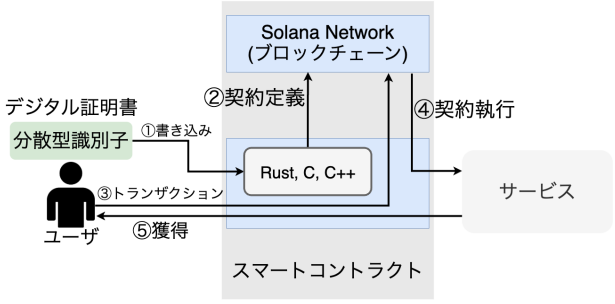

図3　デジタル証明書でのコントラクト

8　評価

実際に公的証明書の定義と同じデジタル証明書の発行と検証を行った．スマートコントラクトにおいても，分散型識別子を契約定義として書き込むことができる.

9　考察

9.1　デジタル証明書の検証

従来の公的証明書に記載されていた個人情報をデジタル証明書としてデジタル化することで，自己主権型アイデンティティの概念のもとユーザの意図しない個人情報の開示をコントロールできるようになり，悪用のリスクを回避できる.

9.2　デジタル証明書とスマートコントラクト

デジタル証明書とスマートコントラクトと組み合わせることで，スマートコントラクトの契約に関与するユーザの個人情報を保護することが可能である．また，検証済み証明書の分散識別子をコントラクトに書き込むことで，ユーザは公的に証明されているとしてサービスと契約することが可能であり，ユーザはサービスを信頼し，サービスはユーザを信頼することが可能である.

9.3　スマートコントラクトにおけるユーザとサービス間の信頼

従来のスマートコントラクトでは，ウォレット ID 同士の取引であり，サービスはユーザが誰であるか不明瞭な点があった．本研究のデジタル証明書とスマートコントラクトの組み合わせによって，ユーザは公的に発行された証明書を用いてサービス及びコントラクトを実行しているとしてサービスはユーザ信頼することができる.

10　結論

本研究によって，デジタル証明書を起点とした自己主権型アイデンティティに基づくアプリケーションの開発方法に見通しを立てられた.

参考文献

[1] Christopher Allen, The Path to Self-Sovereign Identity, http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html,(Accessed on 01/02/2023).
[2] Ethereum, DecentralizedIdentity, https://ethereum.org/en/decentralized-identity/,(Accessed on 01/02/2023).
[3] World Wide Web Consortium, Verifiable Credentials Data Model v1.1, https://www.w3.org/TR/did-core/,(Accessed on 01/02/2023).
[4] Vitalik Buterin,Ethereum A Next-Generation Smart Contract and Decentralized Application Platform, 2014.