Web3 の実装と NFT メダル交換アプリへの応用

Implementation of web3 and application to NFT medal exchange application

トラストビルディング
石坂亮 1)，奥田航太 1)，黒澤航 1)，安野裕貴 1)
細野繁

1) 東京工科大学　コンピュータサイエンス学部　コンピュータサイエンス学科
サービスシステムデザイン研究室

キーワード：web3，ブロックチェーン，スマートコントラクト，認可，ゼロ知識証明

1． はじめに

現代の主流なインターネットである Web2.0 では、中央集権型と呼ばれる特定のサーバーにデータが集中することである情報集約化という問題点が指摘されている。この問題を解決するために新たな概念である Web3 が注目されている。トラストビルディングチームでは、この Web3 を大きなテーマとして持ち、各メンバーの研究分野を組合せ、一つのプロジェクトとして活動している。

2．スマートコントラクト

スマートコントラクトとは、ブロックチェーン上で契約を自動的に実行する仕組みのことである。従来の紙媒体による契約には、契約内容の認識齟齬，契約の不履行，手続きの煩雑さといった問題点がある。これらの課題を情報技術で解決しようという考え方がスマートコントラクトである。

ブロックチェーンは、従来の中央集権型システムとは異なり、複数のシステムがそれぞれ情報を保有し、常に同期が取られる「分散型台帳」という仕組みで管理されている。そのため誰でもブロックチェーンにアクセスすることができ、またデータの改ざんに強いというメリットがある。

本研究は、スマートコントラクトを活用した DApps と呼ばれる分散型アプリケーションの開発を容易に行えるようなフレームワークを開発することが目的である。

3． 認可

Web3 を実現するために、分散型アイデンティティによって認証を実現しているが、この認証方法に対応した認可方法は実現されていない。本研究はその認可方法の実現を目指す。

分散型アイデンティティとは、ブロックチェーンを用いた認証方法であり、ユーザ自身のアイデンティティはユーザ自身で管理･生成･削除は出来るべきという考え方である自己主権アイデンティティを実現するために利用されている技術である。

サービス提供サーバーから独立した認可部分に機能を移すことで分散型アイデンティティに対応した認可の実現に近づくと考える。本研究では Open Policy Agent(OPA)を用いて認可を行う。

OPA とは、ポリシーエンジン(PE)を提供する OSS である。その特徴として、汎用的である点が挙げられる。PE には、事前に決めたポリシーが必要であり、OPA ではポリシーをコードとして記述する Policy as code が用いられている。

4．ゼロ知識証明

ゼロ知識証明とは、ある知識を持っていることを、その知識に関する何の情報も明らかにすることなく証明する手法である。

プライバシー強化技術のひとつであるゼロ知識証明は、活用例としてブロックチェーンとの連携があげられる。ブロックチェーンのデータを公開する仕組みは、機密情報まで共有されてしまうといった問題がある。そこでゼロ知識証明を活用することで、パブリック型ブロックチェーンの利点を生かしつつ、情報が公開されてしまうという欠点を回避することができる。

本研究は、ゼロ知識証明とブロックチェーンを連携し、パブリック型ブロックチェーンの利点を引き出せる仕組みをアプリケーションに取り入れることを目標としている。

5. Non-Fungible Token (NFT)

現在のイラストなどのデジタルコンテンツはコピーが簡易的である。これはコンテンツの利用が簡易化された半面、コンテンツの所有者の特定が不可能になり、誰でもなりすましができてしまう。今後のデジタル社会には新たな信頼の拠り所を明らかにする仕組みが必要である。この課題に対して NFT を活用するアプリケーションについて提案を行う。NFT とは非代替性トークンと呼ばれ、従来のデジタルコンテンツに付随して、所有者が明記された証明書として発行される。一度発行された NFT と同じ内容の NFT が発行されることはなく、従来のデジタルコンテンツの所有者を明らかにすることができる。

6. 現在までの活動内容

トラストビルディングチームでは、実際にサービスを開発、評価する事で研究を行う。現在までに多摩リズムプロジェクト実行委員会が開催しているタマリズムコンテストにアイデアを提案し、実際に開発を進めてきた。

7. 開発サービスの概要

開発するサービスは主に、ユーザが地域に関する写真を投稿する機能、ユーザに対してサービス内で利用するメダルを発行する機能、発行したメダルを他のユーザと交換できる機能の 3 つに分けられる。写真投稿機能では集客目的の他に、サービスを利用する地域に関する投稿内容に限定することで地域内の活性化を促すことを想定している。また、メダル発行機能は、写真 1 投稿に対して 1 回メダルを発行できる。発行したメダルはユーザ同士が交換することができ、ユーザの繋がりをもとにした効率的な宣伝が可能であると考えた。

本サービスで写真投稿、ユーザ同士のメダル交換を利用することで、既存の SNS よりも効率的に従来の顧客と新たな顧客との接点を作ることができる。これにより集客力の向上を見込める。

次に実装方法について説明する。ブロックチェーンに NFT を発行・管理する機能をスマートコントラクトで実行している。NFT の交換を行う際に、交換したい NFT と自身の NFT の交換の可否や、NFT の持ち主が一致しているかどうかの認可を行う。その後、交換された NFT の記録は、スマートコントラクトによりブロックチェーンへ保存される。ゼロ知識証明により、NFT の本人確認の際に、個人情報を明かさずにユーザの証明を可能にしている。

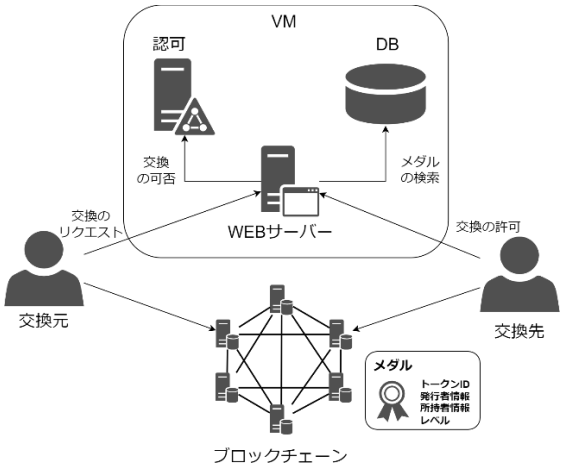

図 1　サービスの構成図

8. まとめ

トラストビルディングチームでは Web3 を大きなテーマとして持ち、実際に各研究分野を組み合わせたサービスの開発、評価を行っている。同時にタマリズムプロジェクトを通して、多摩地域の活性化につながるサービスを提案し、地域にある課題の解決を目指している。