ブロックチェーンによるゲーム内乱数の信憑性確認法の提案

プロジェクトマネジメントコース　矢吹研究室　1442020　大木崇雅

1. 背景

ビットコインを始めとする仮想通貨の存在が広く知られるようになってから，ブロックチェーン技術にも注目が集まっている．ブロックチェーンとは分散型のコンピューターネットワークであり，データベースを中央に置かずに分散して取引記録を管理している [1].

ブロックチェーンは 2008 年にサトシ・ナカモトを名乗る人物が基本理論を提唱した．記録データを「ブロック」と呼ぶ小分けしたデータに加工し，順番に関連付けして鎖 (チェーン) のように連なる構造を取る．ブロックが連なる同一の記録データを複数のコンピューターが管理・保存するというもので，コンピューター同士がブロックを比べてデータを更新する．

ブロックチェーンにはデータの改ざんが困難という特性がある．理由は 2 つある．1 つは仮にあるコンピューター上に存在するブロックを改ざんしても，他のコンピューター上に正しい記録を持ったブロックがある場合，前後のブロックと内容が異なる場合，多数決で不正に書き換えられたデータを排除するからだ．全体の 50 %以上のコンピューター上の記録を書き換えないと改ざんできない仕組みである [2]．もう 1 つの理由は常に新しいブロックが増え続けるからだ．新たなブロックが生成される速度を上回る速度でブロックを書き換える計算能力を持ったコンピューターが必要があり事実上不可能なためだ．

ブロックチェーンの応用分野は金融サービス業に限らず，「改ざんできないデータを共有する」メリットがある業務は対象になり得る．利用者がそれぞれ同じデータを保有することで，単一のシステムや管理組織に依存しない新たなシステム基盤技術とみなす．私はソーシャルゲームに備わっている有料アイテム抽選装置であるガチャの確率についてブロックチェーンの改ざんできないという特徴に焦点を当て研究を進める．

2. 目的

サイコロを振った結果をブロックに書き込み，集計して個別にサイコロを振った結果のデータを取り出せるアプリケーションのプロトタイプを実装する．最終的には課金によって入手できるガチャの確率と，サービスを提供している会社が公に発表している確率が同じかどうか検証するシステムを実装する．

3. 手法

ブロックチェーン上のプログラム開発に対応している HyperledgerFabric を用いる．HyperledgerFabric とは「ブロックチェーン技術推進コミュニティー」のオープンソースであり許可制ネットワーク対応のプラットフォームである．

4. 想定される成果物

サイコロを振った結果をブロックに書き込み，複数の端末機器の間で結果を共有できるアプリケーションを作成する事を目標に研究を進める．

5. 進捗状況

Bitcoin Core という仮想通貨のアプリケーションでローカル PC 上にテストネットワークを構築し，複数のアカウント間でビットコインを送金できた．

6. 今後の計画

ブロックチェーンを用いたアプリケーションのプロトタイプを作成し，複数の PC 上にあるそれぞれ異なるアカウント間で同一アプリケーションを起動させてデータをブロックに書き込む事を目標とする．

参考文献

[1] 広田望. ブロックチェーン (Blockchain). 日本経済新聞社, 2016.

[2] 丸山和子, 愛敬真生. 文系でもわかるブロックチェーン. 日経 BP 社, 2017.