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].

2008 年にサトシ･ナカモトを名乗る人物がブロックチェーンの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記録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 [2]．なぜなら新しいブロックの生成に時間がかかり，常に新しいブロックが増え続けるからだ．ブロックのデータは過去のブロックと関連しており，改ざんが困難だ．仮にあるコンピューター上にあるブロックを改ざんしても，他のコンピューターにブロックが正しい記録を保有している．多数決で正しい記録かどうかを判断するため，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だ [3]．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，集計して個別にガチャ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確率かどうかをプロトタイプに実装する．

3. 手法

以下の手法を用いて開発する．

1. Lauri Hartikka 氏の考案した NaiveChain を利用する．学習用目的で作成され，ブロックチェーンを動かすための基本的な機能を実装されている．
2. 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．「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を利用できる．

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．

5. 進捗状況

Bitcoin Core でテストネットワークを構築し，アカウント間で Bitcoin を送金できた．メッセージをハッシュ化し送信して複数のブロックを経てメッセージを受け渡しする事ができた．

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，複数台で同一アプリケーションを起動させデータを共有する．

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] アンドレアス・M. アントノプロス. ビットコインとブロックチェーン: 暗号通貨を支える技術. エヌティティ, 2016.

[3] 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.