# 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. 序論

2017 年 11 月 15 日に株式会社 Akatsuki が提供しているソーシャルゲームで有料アイテム抽選装置の確率の不正が疑われ，会社の時価総額が暴落した事件があった．このような事件をデータの改ざんが困難であるブロックチェーン技術を用いて解決できるのではないかと考えた．ブロックチェーンとは分散型のコンピュータ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である．

データの改ざんが困難な理由は 2 つある．1 つはあるコンピュータ上に存在するブロックを不正に書き換えても，他のコンピュータ上の記録と異なるブロックを多数決で判断して排除する為だ．全体の 50 %以上のコンピュータ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がなければブロックを改ざんする事は不可能である．

ブロックチェーンの応用分野は仮想通貨などの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．本研究ではブロックチェーンの，データの改ざんが困難であるという特徴に重点を置いて研究を進める．

## 2. 目的

ソーシャルゲームの有料アイテム抽選装置での抽選結果をブロックに書き込んでユーザー間で共有・閲覧できるようにすることが本研究の目的である．今回は有料アイテム抽選装置をサイコロで代替し，サイコロの出目を複数のノード間で共有・閲覧可能な環境を再現する．サイコロの出目が記録されたそれぞれのブロックからデータを取り出し，集計して乱数に偏りがないか調査する．

## 3. 手法

疑似乱数列生成器の 1 つであるセルメンヌツイスタを用いてサイコロの疑似乱数を発生させ，乱数データを CSV ファイルに保存するプログラムを作成する．乱数データの入ったブロックを P2P ネットワークで共有できる naivechain のブロックチェーン上に追加する．

## 4. 結果

naivechain のプログラムを入れていないノードからでも，同一ネットワーク上で繋がっているノードであればデータを共有する事が可能になった．ホストノードの URL を指定することで，ブロックチェーン上の全ブロックの閲覧と，ホストノード上にあるブロックチェーンにブロックを作成して追加する事ができた．

## 5. 考察

データの改ざんが困難なブロックチェーン上で誰もが記録を閲覧できる本研究は，Akatsuki のようなソーシャルゲームサービスを提供している会社の意図的な不正と，ユーザー側の一方的な誤解を防ぐ証明として役立つのではないかと考えられる．

## 6. 結論

以上の結果から，ブロックチェーンに記録されたゲーム内乱数の信憑性は高いと言える．今後は抽選結果をコンピュータが自動的に判断してブロックチェーンに追加するシステムを実装することが今後の課題である．

## 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.