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

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．本研究ではブロックチェーンの特徴である，データの改ざんが困難であるという点に重点を置いて研究を進める．

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．データの改ざんが困難である理由は 2 つある．1 つは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り，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である．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．

2. 目的

サイコロを振った結果をブロックに書き込み，複数のノード間で結果を共有できるシステムを作成する事が目的である．サイコロを振った結果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，乱数データをを CSV ファイルに保存するプログラムを作成した．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

改ざんできない記録をブロックチェーン上に公開する事はユーザにとってサービスを提供している会社を信頼できる 1 つの判断材料になる．実際の有料アイテム抽選装置の結果を不正のないようブロックチェーンに追加する為には，抽選結果をコンピューターが自動的に判断してユーザーが意図的に誤った結果をブロックチェーンに書き込ませない為のシステムが必要である．

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.