ブロックチェーンを適用する抽選システムの拡張に関する検討

Considerations for extending lottery systems to apply blockchain

吉川　健斗†　田谷　昭仁†　戸辺　義人†
Kento YOSHIKAWA†　Akihito TAYA†　Yoshito TOBE†
† 青山学院大学理工学部情報テクノロジー学科
† Department of Integrated Information Technology,　Aoyama Gakuin University

1. はじめに

近年，オンライン上での抽選において透明性を確保するための手法として，ブロックチェーンを利用した研究が広く行われている．本研究では，他利用者の抽選内容が確認できてしまうというブロックチェーンの特性より公平性の確保ができない，有限個のあたりかつリアルタイム抽選システムにおいて公平性を確保するための方法を検討する．

2. 関連研究

ブロックチェーンを利用した抽選システムの研究として[1]では透明性のある乱数生成の方法について述べている．また，[1]の乱数生成法を利用してスマートコントラクト上で景品の対応付けまで行うガチャシステムの提案を行っている研究がある[2]．本研究においても[1]，[2]で用いていた乱数生成法を利用する．

3. 提案手法

本研究において，抽選の公平性の確保のための方法として2つのシステムの提案を行う．1 つ目がコスト変動，確率変動型の抽選システムの VCVP(Variable Cost Variable Probability)．2つ目がコスト一定，確率一定型の抽選システム CCCP(Constant Cost Constant Probability)とする．

3.1 VCVP

本システムにおける既存手法との相違点は

1. ユーザが支払うコストの概念を追加し，金額のやり取りをスマートコントラクト内で行う，
2. ユーザが支払うコストを，引くタイミングの景品排出の期待値によって変動させる，

の2点である．

相違点 1 について，[2]では抽選に際してのユーザが支払うコストについて別アプリケーション内で決済を行うことを想定していた．しかし，その場合であるとブロックチェーンを利用する利点となる一貫したトラストレスな環境を維持できていないといえる．よって，決済を ether に変更することで，スマートコントラクト内で決済まで処理できるようにする．

3.2 CCCP

CCCP では VCVP とは異なった考え方でユーザの公平性の確保を行う．前述した VCVP の考え方では景品価値の期待値の変動によってコストを変動させていくという考え方であったが，CCCP では引くタイミングによっての景品価値の期待値を一定にすることでユーザの公平性の確保を行う．

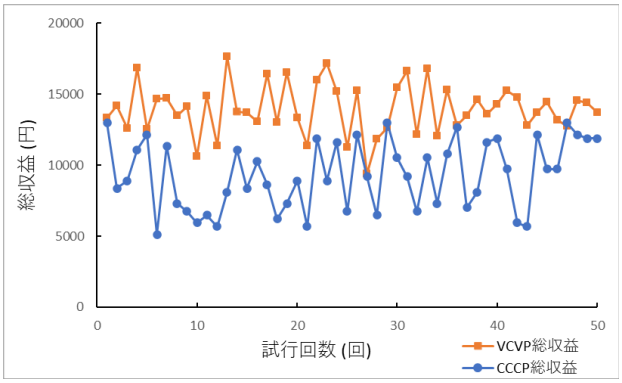

図 1 VCVP と CCCP システム 50 回分の試行

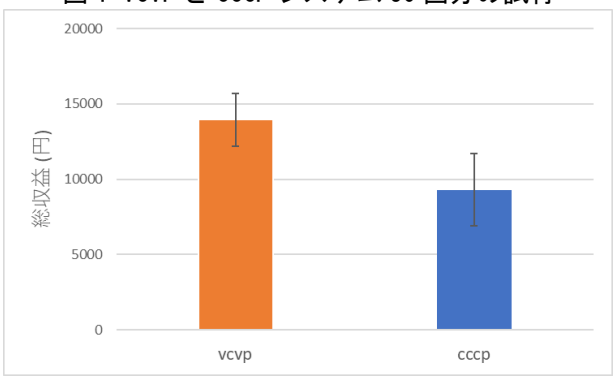

図 2　VCVP と CCCP の比較

4. 実験結果

VCVP，CCCP ともに抽選のどのタイミングにおいても当選期待値とコストが等しくなり，公平性を確保することができた．また，図 1 はシステムを 50 回分の試行においての運営の総収益を VCVP，CCCP で比較したものである．そして，図 2 は総収益の平均値，標準偏差を比較したものである．結果として総収益の観点では CCCP よりも VCVP の方が優れていることが示された．

5. むすび

ブロックチェーンを用いると他の人の抽選内容がトランザクションとしてチェーンに記録され確認できてしまうため、公平性の確保ができなかった．しかし，本研究により有限個の景品がある抽選方式についてブロックチェーンを用いて公平な抽選を行えるようになった．

参考文献

[1] 江原 友登，多田 充，”ブロックチェーンによる乱数生成の透明性確保，” Computer Security Symposium 2017，vol.2017，no.2，Oct.2017.

[2] 廣澤 龍典，上原 哲太郎，”ブロックチェーンを用いた 透明性のある抽選システムの提案と実装，”情報処理学会論文誌，Vol.61，no.12，pp. 1859-1870，Dec.2020.