2R-06

ブロックチェーンシステムにおける 非中央集権性を充足する合意形成メカニズム

安達光太郎† 松原繁夫‡
京都大学大学院情報学研究科

1. はじめに

ブロックチェーンでは合意形成メカニズムを用いて非中央集権的にブロック形成に関する意思決定がなされる．Proof of Stake (PoS)は合意形成メカニズムの一つであり，通貨保有量に応じてユーザにブロック形成の意思決定過程に参加する権利を与える．PoSはEthereumが移行を検討するなど，注目が高まっている．

PoSはProof of Workに比べて電力消費の抑制といった点で優れるものの，一部のユーザに権限が集中する問題が指摘されている．中央集権化への対策として，ランダム選出の導入などが提案されているが，ブロック妥当性確認に関して精度低下を招く恐れがある．

この問題を解決するため，本研究では，非中央集権性を充足する合意形成メカニズムの提案を行う．まず，PoS を委員会構成問題としてモデル化する．本研究の特長は，ユーザの戦略的行動を検討する点である．ユーザの戦略的行動に頑健なチーム形成法を，数学的に，および，シミュレーションを用いて分析し，得られた知見を紹介する．

本研究では，合意形成メカニズムの以下の要素を検討の対象と議論を進める．

・ブロック妥当性確認（ブロックやトランザクションが正当なものか確認）
・ブロック確定処理（ブロックの正当性確定）
・インセンティブメカニズム（ネットワーク参加者に正当な行動を促す）

2．モデル

本稿では，Ethereum2.0 PoSプロトコルに基づいて対象のモデル化を行う．ブロック確定処理の流れは以下のようになる．

1. 検証者(Validator)の集団から n 人の委員(Committee)を選出
2. 選出された検証者は提案されたブロックを検証
3. ブロックをチェーンにつなげるか，検証者による投票を実施
4. 検証作業に対する報酬がもらえる．

この処理が繰り返し行われる．

ブロック検証精度の定式化は従来研究[1]に従う．検証者iは，確率p_iで正しい決定をできるとし，この値は過去の履歴から計算できるとする．このとき，委員会の検証精度は多数決で正しい決定を行う確率として定義される．例えば，p_1, p_2, p_3の 3 名の検証者から成る委員会の検証精度は$p_1p_2 + p_2p_3 + p_1p_3 - 2p_1p_2p_3$となる．委員会は委員会の検証精度に一致した利得を得，個人は委員数で等分した利得を得る．

委員会構成の評価として，効用と非中央集権度を定義する．効用は利得の総和とし，非中央集権度は個人の利得の分散とする．効用は大きい方が，分散は小さい方がよい．

つぎに戦略的行動について考える．検証者は自己の利得が増加するのであれば，故意に誤った投票をすると考える．個人の利得の大小が各人の真の検証精度の大小と同じ順序にならなければ，検証者の戦略的行動が現れ，メカニズムは頑健でなくなる．

3. 委員会構成に関する分析

通常のPoSでは保有通過量による重み付けランダム選択により委員会を構成する．この方法では非中央集権度を小さくできないため，その改善を考える．まずは簡単な場合として，以下を仮定し、委員会構成を考える．

・6 人の検証者 $\mathrm{a,b,c,d,e,f}$ が存在
・各検証者の検証精度を同記号$\mathrm{a,b,c,d,e,f}$で表す
・$0.5 <$ 検証精度 < 1.0
・$a \geq b \geq c \geq d \geq e \geq f$
・検証者から委員会に 3 名が選択され，多数決で意思決定を行う
・委員会には各検証者が同回数選択される

各検証者は同回数選択されるので，この問題は 6 人を 3:3 に分割する問題と考えられる．委員会構成として$\{(a,b,c),(d,e,f)\}$，$\{(a,b,d),(c,e,f)\}$などが挙げられる．前者は，a,b,cとd,e,fでそれぞれ委員会を構成することを意味する．

A consensus mechanism satisfying decentralization in blockchain systems
† Kotaro Adachi, Kyoto University
‡ Shigeo Matsubara, Kyoto University

3.1. 小規模な委員会構成の場合の分析

委員会構成について以下の命題が成り立つ．

命題：各検証者を 1 回ずつ選択する場合，戦略的操作に頑健な委員会構成は，能力別に分類した$\{(a,b,c),(d,e,f)\}$のみである．

紙幅の制限から証明は省略する．

また，各検証者を 2 回ずつ選択する場合，委員会としての検証精度（効用）と分散には，負の相関関係が存在することをシミュレーションにより確認した．相関係数は，個人の検証精度が一様分布に従う場合，-0.7108，正規分布 $N(0.8, 0.01)$に従う場合，-0.7863 であった．

3.2. 大規模な委員会構成の場合の分析

つぎに，より規模を拡大して，各検証者を 10 回ずつ選択する場合を調べる．

・6 人の検証者から 3 人を委員に選出することを 10 回繰り返す
・委員には各参加者が同回数選択される

以上の過程のもと，6 人の検証者の検証精度を$\{0.99, 0.9, 0.8, 0.7, 0.6, 0.51\}$として，様々な委員会構成に関して効用と分散を計算した結果を Figure 1 に図示する．縦軸は個人利得の分散（非中央集権度）を，横軸は効用を示す．プロットされた各点は，委員会構成の一つに対応する．赤は戦略的操作に脆弱であることを，黒は頑健であることを示す．

図を見ることで，検証者の選択回数を増やした場合でも，同様に分散と効用には負の相関があることがわかる．また，最適な委員会構成はいくつかに絞られること，戦略的操作に頑健な構成は脆弱な場合に比べて効用と非中央集権性が低下することがわかる．

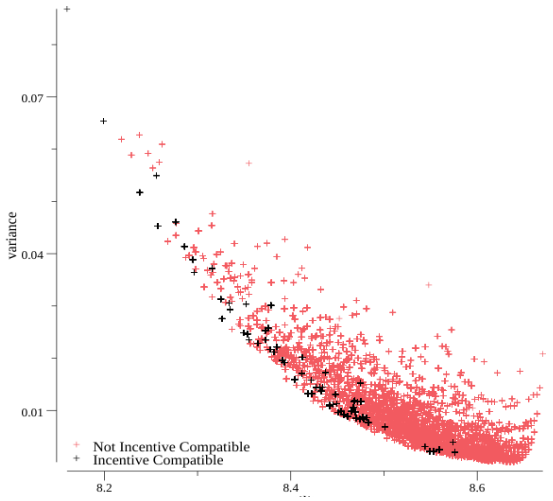

Figure 2　効用と分散の関係

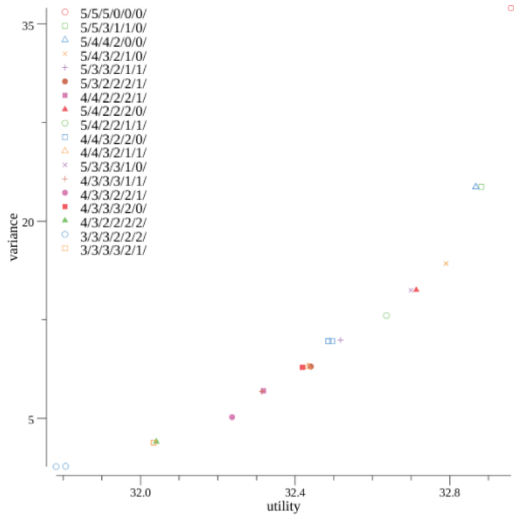

Figure 1　選出回数が異なる場合の効用と分散

これまでの分析では，検証者が同回数選出されることを仮定していたが，つぎに，異なる回数選出される場合を調べる．Figure 2は，検証精度$\{0.9, 0.85, 0.8, 0.8, 0.75, 0.7\}$を持つ6人の検証者から3人を委員に選出することを5回繰り返す場合に関する分析結果である．縦軸は個人利得の分散，横軸は効用を示している．図中の各点は異なる委員会構成を表し，例えば5/5/5/0/0/0は，0.9, 0.85, 0.8, 0.8, 0.75, 0.7を持つ検証者が各々5, 5, 5, 0, 0, 0回選択される場合を表し，戦略的頑健性を満たす構成の中で最適なものを示している．

効用の観点では5/5/5/0/0/0が最も優れている．非中央集権性の観点では3/3/3/2/2/2が最も優れている．効用と非中央集権性の間にはトレードオフの関係があることがわかる．現実のPoSでどれほどの非中央集権性が求められるかによって，各検証者の選択回数を調整する必要がある．

4. むすび

本研究では，PoS プロトコルを対象に，ブロックの検証精度と非中央集権性の両立を目的として，委員会構成法について分析を行った．

謝辞：本研究は JSPS 科研費 JP17H00759, JP19H04170 の助成を受けた．

参考文献

[1] S.Leonardos, D. Reijsbergen and G. Piliouras, "Weighted Voting on the Blockchain: Improving Consensus in Proof of Stake Protocols," 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 2019, pp. 376-384.