PoS 型ブロックチェーンにおける公平分配によるステーク分散の設計と評価

Design and Evaluation of Stake Decentralization Through Fair Distribution in PoS Blockchains

屋敷 圭太 [1]　　上山 憲昭 [2]
Keita Yashiki　　Noriaki Kamiyama
立命館大学　情報理工学研究科 情報理工学専攻 [1]
College of information Science and Engineering, Ritsumeikan University
立命館大学 情報理工学部 [2]
College of Information Science and Engineering, Ritsumeikan University

1. はじめに

ブロックチェーンでは，新規ブロックを追加する際にブロックをネットワークの参加者全員で共有するための合意形成が行われる．合意形成の中でも PoS (proof of stake) は，新規ブロックを生成する権利を得るバリデータが，保有するトークンの量 (ステーク) に基づいて選出され，ブロックの生成に伴い，以下の式に従ってバリデータ i に対するインセンティブ I_i を付与する [1].

$$I_i = s_i$$

ここで，s_i はバリデータ i のステーク量を表す．PoS のこの仕組みは，ステーク量の多いバリデータにとっては有利に働く一方で，新たにネットワークに参加したステーク量の少ないバリデータにとっては不利な状況を生み出す．この結果，新規バリデータはブロック生成に選出される機会が，ステーク量の多いバリデータに比べ減少し，それに伴い，ブロック生成のインセンティブを得る機会が少ないため，ネットワークの参加意欲を減少させる要因となり得る．そこで本稿では，バリデータ間でステーク量に偏りが生じにくくなるような新しいインセンティブ計算式を提案し，ステークの集中を解消する．ステークの分散化を図ると，複数の偽バリデータをネットワーク投入し，不正にブロック生成を行う sybil 攻撃に対し脆弱になる可能性がある．そこで本稿では，バリデータの特徴量を用いたクラスタリングによって，特定の特徴を示す sybil 攻撃者を検知する手法を提案する．

2. 関連研究

PoS 型ブロックチェーンにおいて，ネットワークの分散性およびインセンティブ設計に関する研究として，既存バリデータのステーク分布がコンセンサス形成に与える影響を分析した研究が存在する．[2] では，バリデータのステーク量とブロック生成機会の偏在性に着目し，PoS 環境下でのステーク集中がもたらすコンセンサス形成への影響について評価している．また [3] では，少数の高ステークバリデータが合意形成に対して過度な影響力をもつ問題に対して，非線形なステーク重み付け方式である Logarithmic Stake Weight (LSW) を提案している．LSW モデルでは，次式でインセンティブを付与する．

$$I_s = \log s_i$$

このモデルは，ステーク量に対して対数的なインセンティブを付与することで，過大なステークを持つバリデータの支配力を抑制し，報酬の成長速度を緩やかにする．

3. 提案方式

本稿の提案方式は，従来の PoS システムと比較して，インセンティブ設計およびクラスタリングを用いた sybil 攻撃者検知メカニズムの導入という特徴を有する．バリデータ v に対するインセンティブ I_v の計算式は以下である．

$$I_v = \frac{{S_v}^{\alpha_v}}{\sqrt{S_t}} \times C$$

ここで，S_v は対象バリデータのステーク量，S_t は全バリデータの総ステーク量，C は定数項を表す．インセンティブ式の重み α_v は，次式によって決定される．

$$\alpha_v = \frac{1}{1 + \beta \cdot \frac{S_v}{S_t}}$$

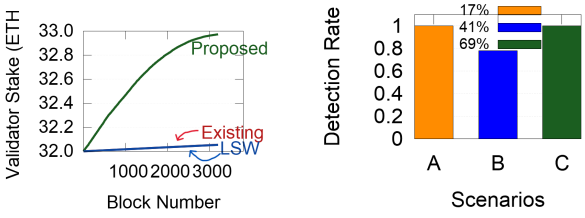
ここで β は重みの調整係数である．この式により，バリデータのステーク占有率 (S_v/S_t) に応じて動的に投票の重み付け係数 α_v が変動する仕組みとなっている．sybil 攻撃者を動的に検知・排除する手法において，本手法では，バリデータの特徴量を用いたクラスタリングを行い，特定の挙動を示すクラスタを攻撃者として識別する．クラスタリングに用いる特徴量 (ラベル) には，バリデータの過去のブロック生成数およびフォーク発生時における投票の偏りの 2 点を設定する．ここで投票の偏りとは，ブロックチェーンのフォークが発生し，その正当化のために投票が行われる際，投票を行うバリデータとその投票先ブロックを生成したバリデータとの関係性における偏重度合いと定義する．

4. 性能評価

提案方式を計算機シミュレーションにより，従来の PoS や LSW と比較し評価する．全バリデータ数 128，生成ブロック数 3,200 ブロック，新規バリデータの初期ステーク 32ETH で新規バリデータのステーク量推移と攻撃者検知率の評価を行った．

図 1(a) に従来の PoS，LSW，提案方式の初期ステーク量が 32ETH である新規バリデータのステーク量推移について各々示す．従来方式と LSW は新規参入者のステーク量推移にほとんど差がない．LSW は高ステークバリデータに与えるインセンティブを下げ，ステーク量に伴うブロック生成の影響率を下げることで分散性を上げている．提案方式では保有ステークが低いほどバリデータに与えるインセンティブが高いため，他の手法に比べてステーク量が増加している．

図 1(b) に攻撃者割合を 10%に，新規参入者割合を 17% (シナリオ A)，41% (シナリオ B)，69% (シナリオ C) に設定した場合の攻撃者検知率を示す．いずれのシナリオにおいても検知率が 80%以上となっている．シナリオ B においては，ブロック生成率の低い新規バリデータにより，投票行動のサンプル数が不足し，統計的に攻撃者の挙動と区別が困難になったと考えられる．



(a) Stake of New Validators　　(b) Attacker Detection

図 1: 新規参入者のステーク推移・攻撃者検知率

4. まとめ 本稿では proof of stake のブロックチェーンにおいて、バリデータがブロックを生成した時に手に入るインセンティブの計算式を変更することで、新規バリデータが参入しやすくなり新規ブロック検証の信頼度が向上する手法を提案した。今後は提案手法を適用による sybil 攻撃耐性の低下を考慮し、提案手法の改良を行い、攻撃耐性の評価を分析する予定である。

謝辞 本研究成果は JSPS 科研費 25K03113，23K28078 の助成を受けたものである．ここに記して謝意を表す．

参考文献

[1] V. Buterin, et al., Combining GHOST and Casper, arXiv preprint arXiv:2003.03052 2020.

[2] S. Motepalli, et al., How Does Stake Distribution Influence Consensus? Analyzing Blockchain Decentralization, IEEE ICBC 2024.

[3] S. Motepalli and H. Jacobsen, Decentralization in PoS Blockchain Consensus: Quantification and Advancement, arXiv preprint arXiv:2504.14351v1 2025.