社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

ステークの偏在化を考慮したPoS型ブロックチェーンにおけるSybil攻撃検知手法

屋敷　圭太†　　上山　憲昭††

† 立命館大学 大学院 情報理工学研究科
〒567-8570 大阪府茨木市岩倉町 2-150
† 立命館大学 情報理工学部
〒567–8570 大阪府茨木市岩倉町 2-150
E-mail: †is0583ff@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

あらまし　ブロックチェーンでは，新規ブロックを生成する際にネットワークの参加者全員でブロックを共有するための合意形成が行われる．代表的な合意形成としてはノードの計算能力に基づく競争型合意である PoW (proof of work) が挙げられる．合意形成の中でも PoS (proof of stake) は，新規ブロックを追加する権利を得るバリデータ (ノード) が，保有する資産量 (ステーク) に基づいて選出される．このコンセンサスアルゴリズムの特性として，ブロック生成者は PoW のように計算能力に依存するのではなく，ステーク量が多いほど選出される確率が高くなり，ブロック生成により獲得するインセンティブが多くなるという仕組みを取っている．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，かつブロック生成のインセンティブが少ないため，特定のバリデータにステーク量が集中する．このような状況は，ネットワークの分散性や公平性を損なうだけでなく，セキュリティリスクを高める可能性がある．そこで本稿では，バリデータ間でステークの集中を解消するインセンティブ手法を提案する．一方で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．

キーワード　Blockchain，Proof of Stake，クラスタリング

Sybil Attack Detection Method in PoS Blockchains Considering Stake Centralization

Keita YASHIKI† and Noriaki KAMIYAMA††

† Graduate School of Information Science and Engineering, Ritsumeikan University
2–150, Iwakura-cho, Ibaraki, Osaka 567–8570
† College of Information Science and Engineering, Ritsumeikan University
2-150, Iwakura-cho, Ibaraki, Osaka 567–8570, Japan
E-mail: †is0583ff@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

Abstract　In a blockchain, consensus building is performed among all network participants to share new blocks upon their generation. A representative example of this is Proof of Work (PoW), a competitive consensus mechanism based on the computing power of nodes. In contrast, Proof of Stake (PoS) selects validators (nodes) that earn the right to add new blocks based on the amount of assets they hold, known as their stake. A defining characteristic of this consensus algorithm is that block producers do not rely on computational power as they do in PoW; instead, the higher a participant's stake, the higher their probability of being selected and the greater the incentives they earn. While this PoS mechanism favors validators with large stakes, it creates a disadvantageous environment for new participants with smaller stakes. As a result, new validators have fewer opportunities to be selected for block generation compared to those with high stakes. Because they also receive fewer incentives, stake becomes concentrated among specific validators. This situation not only undermines the decentralization and fairness of the network but also potentially increases security risks. To address this, this paper proposes an incentive-based method to resolve the concentration of stake among validators. However, attempting to decentralize stake can make the network vulnerable to Sybil attacks, where an attacker injects multiple fake validators to illegitimately generate blocks. Therefore, this paper also proposes a method to detect Sybil attackers exhibiting specific characteristics through clustering based on validator feature sets.

Key words　Blockchain, Proof of Stake, Clustering.

1. 研究の背景

ブロックチェーンは，分散ネットワーク上でデータの不変性と透明性を確保しつつ，取引履歴を共有・管理する分散型台帳技術である [1]．本技術の最大の特徴は，中央集権的な管理者を介さず，複数のノードが合意形成アルゴリズムを通じて台帳の同一性を維持する点にある．当初はビットコインに代表される暗号資産の基盤技術として注目されたが，現在ではその高い信頼性を活かし，サプライチェーン，IoT，医療データ管理，ネットワークセキュリティといった多岐にわたる領域への応用が進められている．

ブロックチェーンネットワークにおけるデータの正当性を担保するためには，合意形成アルゴリズムが不可欠である．これは，分散環境下にある各ノードが，次に台帳へ追加すべきブロックについて一貫した合意を得るためのプロセスを指す．代表的な手法として，計算資源の投入量を競う Proof of Work (PoW)，資産の保有量に基づき決定権を割り当てる Proof of Stake (PoS)，およびノードの一部に障害や不正があっても合意を維持できる Practical Byzantine Fault Tolerance (PBFT) などが挙げられる [1] [2]. これらのアルゴリズムは，耐障害性，スケーラビリティ，リソース消費などの面で異なる特性を有しており，用途に応じた選定がなされる．特に PoS ベースの手法では，各ノードのステーク (保有資産量) が合意形成に与える影響力を左右するため，セキュリティや分散性の観点から固有の課題が指摘されている．

PoS は，各バリデータがネットワーク内にロックしたステーク量に応じて，ブロックの生成や検証権限を付与するアルゴリズムである．PoW と比較して膨大な計算資源を必要としないため，環境負荷が低いという利点がある．例えば Ethereum 2.0 では，32 ETH を預託することでバリデータとしての資格を得ることができ，ネットワークの維持に寄与する [5]．しかし，PoS の仕組み上，ブロック生成の選出確率や投票権の強さがステーク量に比例するため，報酬が大口の資産保有者に偏りやすい性質を持つ．これにより，多くの報酬を得たバリデータがさらに影響力を強めるという富の集中に伴う正のフィードバックが生じ，結果として中央集権化を招く懸念がある [4]．

本稿では，特定のバリデータへのステーク集中に伴う中央集権化を抑止し，新規参入者が従来よりも優位に活動可能なインセンティブ設計を提案する．従来の PoS では，保有ステーク量に比例してブロックの提案機会や報酬が増大するため，資本力のあるノードに権限が集中する課題があった．これに対し本提案では，インセンティブ算出式を再定義することで，小規模なステークを保持するバリデータが獲得できる報酬を相対的に向上させる．これにより，報酬の偏りを是正し，ネットワークの自律的な分散化を促進する．一方で，ステークの分散化を推進することで，多数の偽装ノードを投入してネットワークを操作する Sybil 攻撃への耐性を低下させる懸念が生じる．この課題に対し本稿では，バリデータの投票行動における偏りや，過去のブロック生成履歴を特徴量としたクラスタリング手法を導入し，悪意のあるバリデータを識別・検知する手法を提案する．

2. Ethereum

2.1 スロットとエポック

Ethereum は，PoS 型ブロックチェーンとして，Gasper と呼ばれる合意プロトコルを採用している [3]．Gasper は，Casper FFG (Friendly Finality Gadget) による最終確定機構と，LMD GHOST (Latest Message Driven Greediest Heaviest Observed SubTree) によるフォーク選択規則を組み合わせたプロトコルである．Gasper では，時間の概念をスロット (Slot) およびエポック (Epoch) という 2 つの階層的な単位で定義している．スロットは，ブロック生成が行われる最小の時間単位であり，Ethereum では 1 スロットが 12 秒間に設定されている．各スロットの開始時には，全バリデータの中から 1 名のブロック提案者が擬似乱数的に選出され，新しいブロックの作成およびネットワークへの公開権限が与えられる．なお，選出されたバリデータの通信障害やオフライン状態などの要因により，スロット内でブロックが生成されない場合も存在する．

エポックは，32 スロット (約 6.4 分) をひとまとめにした単位である．エポックは，ネットワークのファイナリティ (最終確定性) を判断するための重要な区切りとして機能する．具体的には，各エポックの境界にチェックポイントが設定され，バリデータによる投票 (Attestation) を集計することで，台帳の正当性が検証・確定される．各バリデータはエポックの開始時に，そのエポック内の特定のスロットを担当する委員会 (Committee) へと割り振られる．各スロットには，1 名のブロック提案者と，複数の検証者 (Attester) で構成される委員会が配置される．1 スロットあたりに編成される委員会の数はネットワーク全体のアクティブバリデータ数に応じて動的に変化し，最大で 64 委員会まで拡張される．プロトコル上の設計により，有効な全バリデータは，1 エポックの間に必ず 1 回，指定されたスロットでの検証作業を行うよう割り当てられる．このため，1 エポック全体で検証に参加するバリデータの総数は，その時点でのネットワークにおけるアクティブバリデータ総数と等しくなる．

2.2 ブロック投票

Ethereum の PoS では，一定量の暗号資産を預託したノードがバリデータとして合意形成プロセスに参加する．時間はスロットおよびエポックの単位で管理され，各バリデータはエポックごとにブロック提案とブロック投票 (Attestation) という 2 つの重要な役割を担う．選出された提案者は，フォーク選択規則である LMD GHOST に基づき，最も正当とされる親ブロックの先端に新たなブロックを生成・接続する．委員会に属する各バリデータは，自身の観測した最新の状態に基づき，正当なチェーンの先端を支持する投票を行う．本プロトコルの特徴は，この投票が単なるフォーク選択 (LMD GHOST) だけでなく，チェックポイント間の合意形成 (Casper FFG) としての役割も同時に果たす点にある．これにより，フォークの解消と最終確定のプロセスが並行して進行する．

エポックの境界に位置するブロックに対し，全ステーク量の 2/3 以上の投票が集まった状態を正当化 (Justification) と呼ぶ．正当化は，そのブロックが正当な履歴の候補としてネットワーク内で概ね合意されたことを意味する．2/3 以上のステークによる支持が必要であるため，競合する異なるブロックを同時に正当化させるには，バリデータによる大規模かつ共謀的な不正 (スラッシングの対象) が不可欠となる．正当化されたブロックは，次段階である最終確定に移行するための必須条件となる．なお，投票数が 2/3 に満たない場合，そのブロックは正当化されず，最終確定へのプロセスも停止する．これは，不完全な合意状態での確定を回避し，一貫性を保護する安全性を優先した設計を反映したものである．

Gasper FFG においては，ある正当化されたブロックに対し，後続のエポックでさらに 2/3 以上の支持 (Super Majority Link の形成) が得られた際に，そのブロックは最終確定 (Finalization) される．最終確定されたブロックはプロトコルが正常

に機能している限り，将来にわたって覆されることがない．また，確定済みの履歴を改ざんしたり，異なるブロックを二重に確定させたりするには，全ステークの 1/3 以上がスラッシングを伴う不正行為をする必要があり，攻撃コストが極めて高く設定されている．2/3 以上の投票が得られないブロックは，最終確定には至らず，確率的な正当性を持つ候補ブロックとして扱われるに留まる．

2.3 フォーク

ブロックチェーンにおけるフォークとは，同一の親ブロックから複数の異なる子ブロックが生成され，ブロックチェーンが分岐される現象を指す．フォーク発生確率は以下の通りである．

$$F(t) = 1 - e^{-t_{prop}/t_B} \tag{1}$$

ここで t_{prop} はブロック伝搬時間，t_B はブロック生成間隔を表している．ブロック伝搬時間は生成されたブロックがネットワーク内のすべてのノードに伝搬するまでに要する時間であり，ブロック生成間隔は新しいブロックが生成される間隔を指している．Ethereum の PoS 設計における最大の特徴は，フォーク選択と最終確定という 2 つの異なる役割を分離・統合している点にある．フォーク選択規則には LMD GHOST (Latest Message Driven Greediest Heaviest Observed SubTree) が採用されている．これは，ネットワーク内で一時的にフォークが生じた際，各バリデータの最新の投票に基づき，最も多くの重みが蓄積されたチェーンを正当と見なす規則である．ここで各ブロックの累積重みは，そのブロックおよびその子孫ブロックを支持して投票したバリデータの合計ステーク量として算出される．図 1 に示すように，LMD GHOST では，以下の手順で正当チェーンを決定する．

（1） ジェネシスブロックから開始
（2） 子ブロックが複数存在する場合各子ブロックのサブツリーの重みを比較する
（3） 最も重みの大きい子ブロックを選択し，そこから再帰的に同様の処理を行う
（4） 最終的に到達したブロックをチェーンの先頭とする

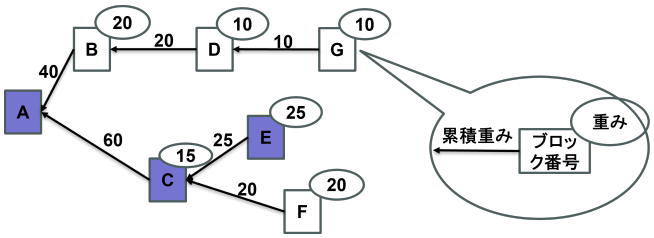

図 1　正当チェーンの決定方法

LMD GHOST は現時点で最も支持されているチェーンを特定するが，これのみでは過去のブロックが後に覆る可能性を完全に排除できない．そこで Ethereum では，Casper FFG を導入することで，履歴の不可逆的な確定を実現している．

Casper FFG では，エポックの境界にあるブロック (チェックポイント) に対し，全ステークの 2/3 以上の投票が集まった際に正当化が行われる．さらに，正当化されたブロックが次のエポックにおいて再び 2/3 以上の支持を得ることで最終確定に至る．この二段階のプロセスにより，ネットワークの安全性と履歴の不変性が保証される．

3. 関連研究

3.1 ステークの集中

PoS では，ブロック提案やブロック投票に対する報酬が，原則としてステーク量に比例して分配される．新規ブロックの生成の際，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．

$$I_i = s_i \tag{2}$$

ここで s_i はバリデータ i が保持するステークを意味する．PoS プロトコルではブロック生成機会および投票の重みがいずれも s_i に比例して決定される．この設計は，ステーク保有量に比例して期待報酬が増大する構造を内包している．獲得された報酬がステークへ再投資されることで，当該バリデータの次期報酬獲得確率はさらに上昇し，長期的には初期段階で多額の資産を保有する者が支配的な地位を維持・強化する正のフィードバックが形成される．ステークの偏りは経済的格差に留まらず，合意形成プロセスの分散性にも直接的な悪影響を及ぼす．高ステーク保有者は，少数であってもフォーク選択規則や最終確定プロセスにおいて決定的な影響力を行使できる．これにより，特定のバリデータの意向がネットワーク全体の合意結果を左右するリスクが高まる．一方で，ステーク量の少ないバリデータは投票の寄与度が限定的であり，ブロック提案の機会も稀少である．報酬の蓄積速度が遅いため，相対的な影響力が向上しにくく，ネットワーク内での地位が固定化されやすい．このようなステーク格差の拡大は，Nakamoto 係数の低下を招き，ブロックチェーンの根幹である分散性を損なう懸念がある．したがって，ステーク量以外の指標を組み込んだインセンティブ設計や，小規模バリデータの参画を促すメカニズムの構築が重要な研究課題となっている．

少数のバリデータによる意思決定の支配を抑制するため，ステーク量を非線形に変換して報酬や重みを算出する手法が提案されている．他研究では，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 Square Root Stake Weight (SRSW) [6] および Logarithmic Stake Weight (LSW) [8] を提案している．[6] では，バリデータの保有するステーク量を非線形に再調整し，ステークの分配を是正することにより，少数のバリデータがネットワークの意思決定を支配する状況を抑制している．[8] では，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．LSW モデルでは，次式でインセンティブを付与する．

$$I_i = \log s_i \tag{3}$$

3.2 Sybil 攻撃

Sybil 攻撃とは，分散システムにおいて単一の攻撃主体が大量の偽装ノード (Sybil ノード) を作成し，それらが独立した複数の参加者であるかのように振る舞う攻撃手法である [9]．本攻撃の主なプロセスは，ネットワーク内の情報流通の支配にある．攻撃者は特定の領域に多数の Sybil ノードを配置し，外部からは個別の参加者に見えるようこれらを集中的に制御する．誠実なノードがこれらの Sybil ノードによって周囲を包囲された場合，正常な情報の伝達が阻害される．攻撃者は正当なブロックやトランザクションの転送を意図的に放棄することや他ノードの接続先を攻撃者のノードのみにすることでネットワークの状態を誤認させるなどの操作をする．誠実なノードの通信相手が

攻撃者の支配下にあるノードのみに限定されると，当該ノードは真の合意形成プロセスから孤立し，攻撃者が捏造した情報を正当なものとして受容するリスクが生じる．

Sybil 攻撃は，その動機に基づいて 2 タイプに分類される [11]．複数の偽装ノードを運用することで，ネットワークから得られる報酬の不正な増大を主目的とする利得最大化型 (Utility-maximizing) と，投票権やブロック提案機会を掌握するため，より多くの委任 (Delegation) を獲得し，ガバナンスへの支配力を高めることを目的とする．影響力最大化型 (Influence-maximizing) の 2 つが存在する．PoS において，中央集権化を抑制するために個々のバリデータのステークが与える影響力を弱める設計を導入すると，新たな脆弱性が生じる．ステークの影響力が均等化されることで，攻撃者が自身の保持するステークを細分化し，多数のバリデータを生成して攻撃を行う Sybil 攻撃の実行コストが低下するためである．このステーク集中と Sybil 攻撃のトレードオフに対し，先行研究が存在し，Binfeng らの手法 [7] では報酬分配メカニズムおよびステークの委任構造を再設計する手法を提案している．Bappy らの手法 [12] ではマルチエージェント強化学習（MRL）を応用したコンセンサスアルゴリズム MRL-PoS+ を提案している．

4. 提 案 方 式

4.1 概　　要

本節では，提案する PoS コンセンサスアルゴリズムの詳細について述べる．本提案方式は，従来の PoS システムと比較して，インセンティブ設計と投票重み付けの変更，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 3 つの主要な特徴を有する．以下にそれぞれの詳細を述べる．

4.2 インセンティブ及び投票重みの算出式

本方式では，バリデータの報酬計算およびネットワークへの影響力を決定するブロック投票の重みについて，新たな算出式を導入する．インセンティブの計算式は以下である．

$$I_i = \frac{\gamma_i^{\alpha}}{\sqrt{\delta}} \times C \tag{4}$$

ここで，γ_i は対象バリデータ i のステーク量，δ は全バリデータの総ステーク量，C は定数項を表す．インセンティブ式における重みは (α) は，以下の式によって決定する．

$$\alpha = \frac{1}{1 + \beta \times \frac{\gamma_i}{\delta}} \tag{5}$$

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 (γ_i/δ) に応じて動的に投票の重み付け係数 α が変動する仕組みとなっている．

4.3 クラスタリングを用いた Sybil 攻撃者の検知

本提案方式の 3 つ目の特徴は，Sybil 攻撃者を動的に検知・排除する手法である．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．

（1） 特徴量の定義と投票の偏り

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，ネットワーク内で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．

（2） 攻撃者の検知ロジック

正常なバリデータと Sybil 攻撃者では，ブロック投票の行動原理が以下のように異なると想定される．

・正常なバリデータ: ブロック生成者のステーク量や過去のブロック生成履歴といったプロトコル上の正当性に基づき投票先を選択するため，特定の生成者に固執することなく分散的な投票行動を取る．

・Sybil 攻撃者: 複数の偽バリデータを用い，自身 (攻撃者のメインノード) が生成したブロックに投票を集中させることで正当化を試みる．その結果，特定の生成者に対する投票の偏りが顕著に表れる．

本手法では，これらの特徴量を基にバリデータをクラスタリングし，生成されたクラスタの中からステーク量が低く，かつ投票の偏りが最も強いクラスタを抽出することで，Sybil 攻撃者を検知する．

5. 性 能 評 価

5.1 評 価 条 件

提案方式を計算機シミュレーションにより評価する．また，提案方式における評価条件を以下に示す．バリデータ数は 128 とし，1 ラウンドごとのブロック生成数 3,200 で，合計で 1,000 ラウンド行う．また，インセンティブ式における C を 0.02 とし，β を 0.9 とする．

5.2 新規参入者ステーク

図 2 に，ネットワーク全体のバリデータのうち新規参入者が 10% を占める環境を想定し，新規参入者が 3,200 個のブロック生成によって得られるステーク量 (ETH) の推移を従来手法，提案手法，LSW のそれぞれで示す．

提案手法は従来手法及び LSW と比較して，最も顕著なステーク量の増加を示している．一方，従来手法と LSW の推移はほぼ同等であり．提案手法との間に大きな差が生じる結果となった．これらの推移の差は，各手法におけるインセンティブ設計の違いに起因している．従来手法はインセンティブ式が保有ステーク量に比例して報酬が増加する設計となっている．このため，初期ステーク量が少ない新規バリデータにとっては獲得できる報酬が限定的となり，結果として図 2 に示すような緩やかな増加にとどまっている．提案手法では，保有ステーク量が低いバリデータほど，より高いインセンティブを獲得できる設計を採用しているため，ステーク量が大きく増加している．

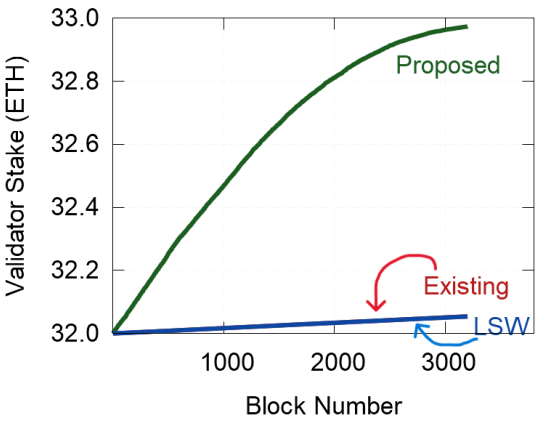

図 2　新規参入者のステーク量の時間変化

5.3 Nakamoto 係数

本評価では，システムの分散性を定量化する指標として

Nakamoto 係数 (Nakamoto Coeffcient) を用いる．Nakamoto 係数とは，システムに対して妨害や不正操作を企てる攻撃者が存在すると仮定した際，その攻撃を成立させるために必要な最少のノード数を算出したものである [13]．この値が大きいほどシステムの制御を奪うために多くのノードを占有する必要があることを意味し，分散性が高いと評価される．本評価では Nakamoto Coefficient for Liveness (N_L) と Nakamoto Coefficient for Safety (N_S) から分散性を評価する．N_L はシステムを阻害，ブロック生成を停止・妨害させるために必要な最小のノード数を示す指標である [14] [16]．この値が低いほど少数のノード離脱や共謀によってネットワークが停滞するリスクが高いことを示唆し，全バリデータのステーク合計の 1/3 以上を占めるために必要な最小の集合 L の要素数として，次式で定義される．

$$N_L = \min\{|L| \mid L \subseteq N, \sum_{i \in L} w_i \geq \frac{1}{3} \sum_{i=1}^{m} w_i\} \qquad (6)$$

ただし w_i はバリデータの保有ステークを示す．

N_S はシステムの安全性を脅かし，ブロックの改ざんや二重支払いなどを可能にするために必要な最小のノード数を示す指標である．これは，コンセンサスアルゴリズムにおける信頼の境界を定量化したものであり，全バリデータのステーク合計の 2/3 以上を占めるために必要な最小の集合 S の要素数として次式で定義される [15] [14]．

$$N_S = \min\{|S| \mid S \subseteq N, \sum_{i \in S} w_i \geq \frac{2}{3} \sum_{i=1}^{m} w_i\} \qquad (7)$$

システムの分散性を評価するため，Nakamoto coefficient を指標として用い，従来手法，提案手法，および LSW の 3 手法を比較した．評価結果を図 3 に示す．Nakamoto coefficient の値は，LSW，提案手法，従来手法の順に高く，LSW が最も優れた分散性を示している．従来手法は他手法に比べ最も低い係数となった．これは，ネットワークを操作するために必要なノード数が少なく，少数のノードによって攻撃が成立し得ることを示している．その要因として，従来手法は一部のステークを多く保有するバリデータに報酬が集中する設計であるため，ステーク量の偏りが拡大し，結果として中央集権的な構造になることが考えられる．提案手法は従来手法と比較して係数が向上している．これは，本提案における保有ステーク量が低いバリデータに対してより高いインセンティブを付与しているからである．この手法によりノード間のステーク格差が縮小し，ネットワーク全体の分散性が向上したと考えられる．LSW はインセンティブ式に非線形な重みづけを採用しており，これがステークの分散を促進している．その結果，攻撃に必要な最小ノード数が最大化され，Nakamoto coefficient が増加したと考えられる．

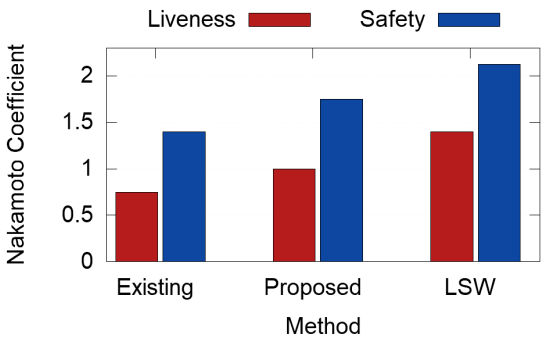

図 3　nakamoto 係数の方式間の比較

5.4　フォーク発生確率

図 4 に，攻撃者割合が 5%，10%，20% においての従来手法，提案手法，LSW の有効フォーク発生確率の比較結果を示す．いずれの攻撃者割合においても，提案手法は従来手法および LSW と比較して，フォーク発生確率が最も低い結果となった．一方，従来手法と LSW の間には有意な差は見られず，ほぼ同様の発生確率を占めている．提案手法では，後述するブロック提案バリデータの選出確率において，新規参入者が選出される確率を適切に抑制する設計を導入している．これにより，攻撃者がフォークを発生させる機会自体が低下し，ネットワーク全体の安全性が高められている．

従来手法と LSW においては，ブロック提案者の選出アルゴリズムにおいて新規参入者と既存ノードの間で選出確率に大きな差が生じない設計になっている．そのため，提案手法のようなフォーク抑制効果が働かず，結果として両手法は同程度の高いフォーク発生率にとどまっていると考えられる．

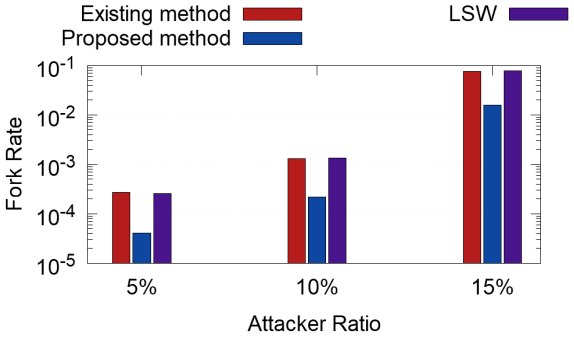

図 4　フォーク発生確率 (攻撃者割合 5%, 10%, 15%)

5.5　新規参入者選出確率

図 5 に示す通り，提案手法は従来手法及び LSW と比較して，新規参入者の選出確率が極めて低く抑制されている．一方，従来手法と LSW の間には有意な差は見られない．

従来手法と LSW のグラフがほぼ一致しているのは，両手法において新規参入者のブロック提案バリデータ選出確率を決定する数式が共通しているためである．提案手法は，前述の通りステーク量の低いバリデータに対して高いインセンティブを付与し，ネットワークの分権化を促進する．しかし，その一方で保有ステーク量が低いバリデータほど，ブロック提案者としての選出確率を低減させるという選出抑制アルゴリズムを導入している．この設計により，新規参入バリデータがステークを蓄積するまでの期間は，ブロック提案の機会を制限している．

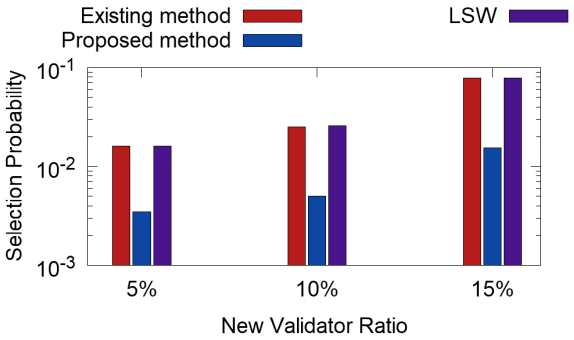

図 5　新規参入者選出確率 (新規参入者割合 5%, 10%, 15%)

5.6 攻撃者検知率

ネットワーク内の攻撃者割合を 10% に固定した条件下において，新規バリデータの割合によるシナリオ別に提案手法を用いた際の攻撃者検知率を図 6 に示す．本実験では，新規参入バリデータの割合が異なる 3 つのシナリオ (シナリオ A: 17%，シナリオ B: 41%，シナリオ C: 69%) において，提案手法の有効性を検証した．シナリオ A およびシナリオ C では 100% の検知率となっており，シナリオ B における検知率は約 80% となっており，約 20% の正常バリデータが攻撃者クラスタとして誤分類される結果となった．シナリオ A では，新規バリデータが多く存在するため，正常なバリデータの投票先が分散しやすい状況にある．この環境下では，攻撃者の特徴である特定のブロックへの集中的な投票行動が相対的に顕著となり，攻撃者の特徴を明確に抽出できたことが検知率の向上に寄与したと考えられる．

またシナリオ C においても，新規バリデータの割合が非常に高く，フォーク発生時に新規バリデータが生成したブロックが選択されやすい環境にある．これにより正常バリデータの投票先がさらに分散する傾向が強まり，攻撃者の投票集中がより際立つ結果となった．一方，シナリオ B で約 20% の誤検知が発生した要因は，ネットワーク内のバリデータの構成バランスに起因する．本シナリオでは，ブロック生成率の低い新規バリデータと，信頼性が高く投票が集中しやすい高ステークバリデータがそれぞれ一定数混在している．この状況下では，一部の正常な新規バリデータの投票挙動が，攻撃者グループの挙動と類似しているため，クラスタリングの過程で攻撃者側に分類されたものと考えられる．

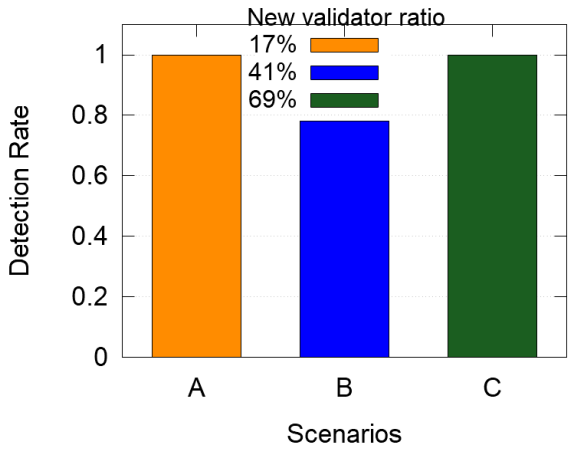

図 6　攻撃者検知率 (攻撃者割合 10%)

6. ま と め

本論文では，PoS 型ブロックチェーンにおいて，ステークの中央集権化が発生する課題に対し，新規参入バリデータがステークを獲得しやすいインセンティブ式とブロック投票の際の投票の重み式と，ブロック投票においてクラスタリングを行うことによって Sybil 攻撃者を検知する手法を提案した．数値評価において，新規参入者のステーク推移は，提案手法は従来手法と LSW に比べてステーク量が最も増加した一方，従来手法と LSW はほぼ同等のステーク量推移であった．nakamoto 係数による safety と liveness の評価では，LSW の値が最も高くブロック生成を停止、改ざんするために必要な最小ノード数が多く，分散性が最も高い．提案手法は分散性が，従来手法よりも高く LSW よりは低い．攻撃者検知率においては，高ステークバリデータが多く存在する正常バリデータの投票先が分散しやすい状況においては攻撃者のブロック投票行動が他バリデータの投票行動と明確に分けられ，攻撃者検知率が上昇する．新規参入者が多いような状況においては，フォーク発生時に生成されるブロックが新規バリデータのものであることが多くなるため，正常バリデータの投票先が分散し，攻撃者の投票行動が他に比べて別の行動として抽出され，検知率が上昇する．今後は検知率の低い攻撃者割合，シナリオを基に Sybil 攻撃の攻撃実行率を評価する予定である．

謝辞　本研究は 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．

文　献

[1] S. Nakamoto , ”Bitcoin: A Peer-to-Peer Electronic Cash System ,” https://bitcoin.org/bitcoin.pdf , 2008.
[2] Diogo Avelãs, Hasan Heydari, Eduardo Alchieri, Tobias Distler, and Alysson Bessani. Probabilistic Byzantine Fault Tolerance (Extended Version) . , arXiv preprint arXiv:2405.04606v3 [cs.DC] , 2024.
[3] V. Buterin, et al., Combining GHOST and Casper, arXiv:2003.03052 [cs.CR], May 2020
[4] G. Fanti, L. Kogan, S. Oh, K. Ruan, P. Viswanath, and G. Wang, “Com pounding of wealth in proof-of-stake cryptocurrencies,” in Financial Cryptography and Data Security: 23rd International Conference, FC 2019, Frigate Bay, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23, pp. 42–61, Springer, 2019.
[5] J. Traglia, “Beacon chain,” 2023. Accessed on 2024-04-27.
[6] S. Motepalli, et al., How Does Stake Distribution Influence Consensus? Analyzing Blockchain Decentralization, 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), May 2024.
[7] B. Song, et al., Decentralized Reward Allocation Mechanism with Sybil Resilience: The Case of Stake Pools, 2025 IEEE/ACM International Symposium on Quality of Service (IWQoS), 2025.
[8] S. Motepalli, et al., Decentralization in PoS Blockchain Consensus: Quantification and Advancement, IEEE Transactions on Network and Service Management (arXiv:2504.14351), Apr. 2025.
[9] J. R. Douceur, ”The Sybil Attack,” in Proc. of the International Workshop on Peer-to-Peer Systems (IPTPS), 2002.
[10] V. Buterin, et al., Combining GHOST and Casper, arXiv:2003.03052 [cs.CR], May 2020
[11] M. Platt and P. McBurney, “Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance,” Algorithms, vol. 16, no. 1, p. 34, 2023.
[12] F. H. Bappy, et al., ”Securing Proof of Stake Blockchains: Leveraging Multi-Agent Reinforcement Learning for Detecting and Mitigating Malicious Nodes,” in Proc. of IEEE Global Communications Conference (Globecom), 2024.
[13] Q. Lin, C. Li, X. Zhao, and X. Chen, ‘‘Measuring decentralization in Bitcoin and Ethereum using multiple metrics and granularities,’’ in Proc. IEEE 37th Int. Conf. Data Eng. Workshops (ICDEW), Apr. 2021, pp. 80–87.
[14] Balaji S. Srinivasan and Leland Lee. Quantifying decentralization. https://news.earn.com/quantifying-decentralization-e39db233c28e. Accessed: 2023-11-05.
[15] Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In Annual international conference on the theory and applications of cryptographic techniques, pages 643 673. Springer, 2017.
[16] Gengrui Zhang, Fei Pan, Michael Dang’ana, Yunhao Mao, Shashank Motepalli, Shiquan Zhang, and Hans-Arno Jacobsen. Reaching consen sus in the byzantine empire: A comprehensive review of bft consensus algorithms. arXiv preprint arXiv:2204.03181, 2022.