Proof-of-Stake 型ブロック・チェーンにおける投票プロファイルを用いたインセンティブ・メカニズム
Incentive Mechanism Based on Voting Profile for Proof-of-Stake Blockchains

笠原正治(Shoji KASAHARA, Ph. D.)
奈良先端科学技術大学院大学　先端科学技術研究科
情報科学領域　教授
(Division of Information Science, Graduate School of Science and Technology, Nara Institute of Science and Technology, Professor, Dr. Eng.)
電子情報通信学会、日本オペレーションズ・リサーチ学会、
情報処理学会、IEEE, INFORMS
受賞：電気通信普及財団 第 22 回電気通信普及財団賞（テレコムシステム技術賞）(2006 年度) KDDI 財団 2010 年度 KDDI 財団優秀研究賞（2010 年度）電子情報通信学会フェロー（2018 年度）日本オペレーションズ・リサーチ学会フェロー（2020 年度）
研究専門分野：待ち行列理論とその応用、性能評価モデリング、情報ネットワーク

あらまし

ブロック・チェーンのスケーラビリティ問題を解決するアプローチとして、新規ブロックの合意形成を複数ノードの投票によって行う Proof-of-Stake (PoS) の導入が検討されている。Proof-of-Stake (PoS) では、バリデータと呼ばれる管理ノードによる投票により、新規ブロックの正当性を判断する。一般に投票に基づく合意形成では、悪意のあるバリデータの割合が増加すると、合意形成が不適切に行われる危険性が増大する。そのため、PoS では正しいコンセンサスに貢献したバリデータに報酬を与え、そうでないバリデータに罰則を与えることで、バリデータに対して正しい投票を動機づけている。本稿では、バリデータの投票行為を評価する指標として、投票実績に基づく信頼度を導入し、信頼度に基づいて報酬もしくは罰則を与えることで、バリデータが保有する保証金 (Stake) の量を変動させる方式を提案する。計算機シミュレーションにより、バリデータ信頼度の推定精度、及びバリデータが保有する平均 Stake 量について評価を行う。数値例より、バリデータが正しく投票する確率が動的に変化する状況下で提案手法はバリデータの信頼度を高精度に推定できること、及び信頼度の高いバリデータに対して多くの報酬を与えることができることが確認された。

1．序論

ブロック・チェーンはインターネット上で流通する仮想通貨を支える分散台帳技術である。ブロック・チェーンでは取引情報を記録した台帳データが、peer-to-peer ネットワーク技術によって複数のノード上で分散管理されている。台帳が分散管理されていることから、電子マネーにおける中央サーバのような管理主体を必要としない。ブロック・チェーンでは取引情報であるトランザクションをブロックという単位に格納し、過去の全取引情報が記録された台帳データベースに新規ブロックをチェーン状に結合する。このとき、複数のノードが新規ブロックの正当性について検証を行い、ブロック・チェーンへの追加の可否について合意形成を行う。この新規ブロックの承認に関する一連の手続きはコンセンサス・アルゴリズムによって実現されている。

ブロック・チェーンの代表的なコンセンサス・アルゴリズムの一つに、Bitcoin [1]で採用されている Proof-of-Work (PoW) がある。PoW では、ブロックはハッシュ計算に基づくパズル的問題解決を行うことで承認手続きが行われる。パズル的問題解決に必要な計算処理が莫大なため、高い処理能力を有するノードがブロック生成を行う権利を獲得する確率が高くなるという特徴がある。Bitcoin や Ethereum [2] といった仮想通貨ではマイニングに勝利したノードに対し、報酬を与えることで、ブロック・チェーンの管理に貢献する動機付けを与えている。しかしながら、マイニングには膨大な計算量が必要であり、ブロック承認のために大量の電力が消費されることが欠点として知られている。

PoW の欠点を改良するためのコンセンサス・アルゴリズムとして、計算能力をそれほど必要としない Proof-of-Stake (PoS) が提案されている。PoS では、PoW における計算力を Stake と呼ばれる仮想通貨で支払われる保証金で代替する。PoW では高い計算能力を持つノードがブロックを生成する権利を獲得するが、

PoS では参加ノードは保有する Stake の量に応じてブロックを生成する権利を獲得する。

一般的な PoS におけるブロック承認は以下の通りである。参加ノードは Stake の量に応じて新規ブロックの正当性を検証する役割を担うバリデータと呼ばれる特別なノードに選出される。選出されたバリデータは生成されたブロックに不正がないかどうかを検証し、その正当性について投票を行う。生成されたブロックの正当性について一定数以上の投票が集まれば、ブロックは正当であると合意が形成され、生成ブロックはブロック・チェーンに結合される。反対に、規定の投票数に満たなければ正当性が認められないために当該ブロックは却下・廃棄される。

PoS では、バリデータが生成ブロックの正当性を正確に検証して正しく投票することが重要である。バリデータが正しい投票をしない場合、ブロックの正当性について正しく合意がなされない状況が考えられる。そこで、システムが正しい投票を行うバリデータに報酬を与え、逆に正しく投票しないバリデータには罰則を課すことで、バリデータに正しい投票を動機づける方式が検討されている。バリデータの投票結果に応じて賞罰を取り入れた仮想通貨として Cosmos [3] や Polkadot [4]、 Ethereum2.0 [5] が挙げられる。しかしながら、具体的なアルゴリズムや実装方法については未公開のため、不明な点が多い。

本研究では、正しい投票を行う動機付けをバリデータに対して行うための報酬・罰則付与型 PoS コンセンサス・アルゴリズムについて基本的検討を行う。バリデータに対する報酬・罰則の算出のため、バリデータの投票に対する信頼度の指標を導入する。提案方式では、バリデータの過去の投票履歴を基に信頼度を算出し、新規ブロックの正当性検証時に行った投票内容と投票結果が一致したかどうかに応じて信頼度で割り引いた報酬・罰則を与える。提案方式を評価するための計算機シミュレーションでは、報酬として新規に分配されるトークンのインフレ率を考慮したシナリオの下で、バリデータの投票結果に応じてどのように Stake 量が変化していくのかを定量的に分析する。

本稿の構成は以下の通りである。2 章ではブロック・チェーンのコンセンサス・アルゴリズムに関する関連研究を示す。3 章では報酬・罰則付与型 PoS 用コンセンサスアルゴリズムの詳細を述べる。4 章では提案手法の数値実験結果を示し、5 章でまとめと今後の課題を示す。なお、本稿の内容は研究成果[6]に依っている。

２．研究の背景

Bitcoin では、ネットワークに参加するノードに対して、ブロックの生成を動機づけ、かつノード間でブロックの正当性について合意をとるアルゴリズムとして PoW を採用している。Bitcoin では、参加ノードはマイニングと呼ばれるハッシュ計算に基づく暗号学的パズルを解くことで新規ブロックをブロック・チェーンに接続し、報酬を受け取る。マイニングの難易度は新規ブロックの生成間隔が平均 10 分間になるように自動的に調整されている[7]。マイニングの勝利確率は参加ノードの計算パワーに依存しているため、マイニングに参加するノードは高い計算能力を有するハードウェアで構成されている。そのため、消費する電力が莫大であり、マイニングの電力消費が環境破壊に繋がっているという報告もある[8]。

消費する資源が少ない効率的なコンセンサス・アルゴリズムとして、PoS が提案されている。PPcoin [9] は PoS を初めて取り入れた例として知られている。PPcoin では、所有しているトークンの量とその所有期間の積に応じて、ブロックを生成する権利がノードに割り当てられる。これにより高い計算力が不要となり、消費する資源は PoW に比べて小さくなる。

Bitcoin や PPcoin では、最新ブロックの直後に複数のブロックが付け加わってチェーンが枝分かれするフォークと呼ばれる現象が発生する。Bitcoin や PPcoin ではフォークが発生した際、その後に付け加えられるブロック数が一番大きいチェーンを正当なチェーンとみなす。これを longest chain の法則という [1, 10]。これにより、最長のチェーンに含まれるブロックの正当性は、時間が経過するにしたがって確実なものになっていく。しかしながら、将来的に別の長いチェーンが生成される可能性があり、ブロックに含まれるトランザクションの決済完了点を保証することができないファイナリティの問題がある。

決済完了点を持たせた PoS の実装例の一つに

Tendermint [11] がある。Tendermint では、参加ノードはネットワークで利用される通貨であるトークンを保証金（Stake）として特定のアドレスに預け入れる。Stake はシステムによって管理され、ノードによる引き出しが制限される。Stake が預け入れられると、そのノードはバリデータ候補者リストに登録される。バリデータ選出時点が来ると、Stake 量の大きいノードから降順に、予めプロトコルで決められた数のバリデータが選出される。

選出されたバリデータは、ラウンドロビン方式で順番にブロックの生成を担う。ブロックの生成を担うノードはプロポーザと呼ばれる。プロポーザがブロックを生成すると、プロポーザ以外のバリデータが生成ブロックの正当性について検証を行う。選出された複数のバリデータは委員会を形成しており、各バリデータは自身が行った生成ブロックの正当性検証の結果を基に、そのブロックの正当性について投票を行う。生成されたブロックが正当であると判断したバリデータは承認票を投じ、逆に不当であると判断したバリデータは投票を行わない。投票の結果、ネットワークであらかじめ定められた閾値より大きい数の承認票が集まれば、そのブロックは正当であると委員会レベルで合意が形成される。合意に至ったブロックはブロック・チェーンに追加される。この投票による合意形成により、フォーク現象は発生しない。生成ブロックに対して委員会が合意を形成した時点を決済完了点とすることができる。

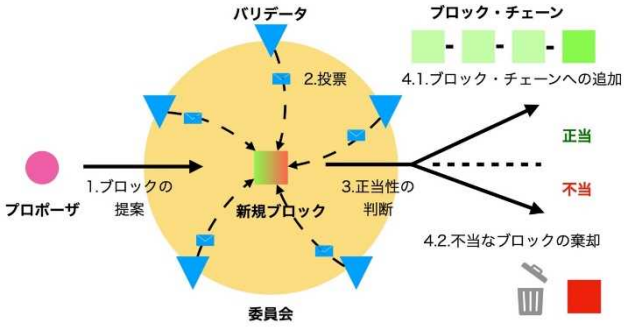

図 1　PoS におけるコンセンサス処理
(copyright©2020 IEICE)

委員会におけるブロックの適切な正当性判断は、バリデータの投票の正しさに依存する。正しい投票が行われない場合、委員会の合意形成が正しく行われない危険性が増大する。そこで、適切な正当性判断が行われるような投票手法が検討されている。Leonardos らは重み付き投票に基づく PoS 型合意形成法を提案している [12]。これはバリデータの投票結果からバリデータの信頼度を算出し、その信頼度に応じてバリデータの投票に重み付けをするものである。Cosmos、Polkadot、Ethereum 2.0 といった PoS 型コンセンサスアルゴリズムを採用しているブロック・チェーン技術では、ブロックの正当性を、承認または否認(無投票を含む)の二択の単純投票によって合意形成を行う。単純投票では投票者一人が重み 1 の票を投じる投票方法であるが、単純投票を拡張したものとして、各投票者の票の重みを変化させる重み付け投票がある。定数が定められた委員会における二択の重み付き投票に関する研究が文献 [13]で行われている。Leonardos らはこれらの結果を応用し、個々のバリデータの信頼度に応じた重みの算出方法、及び合意形成に必要な重み付き承認票の割合の算出方法を提案している。

文献[14]では、バリデータの信頼度を基に報酬を配布する方式を提案している。具体的には、プロトコルの遵守率に応じてノード毎のスコアを算出し、閾値を下回るノードの報酬を割り引く報酬配布を提案している。これにより、信頼度の高いノードほど多くの報酬を得ることができる。

Buterin らは、バリデータが正しく投票を行うインセンティブを与えることを目的に、正しくない投票を行ったバリデータの Stake を徴収する仕組みを提案している[15]。これは正しくない投票をするバリデータに対して罰則を課すことで、負のインセンティブを与えるものである。これによりバリデータは正しい投票をする動機づけがなされ、委員会が適切な正当性判断に至ることが期待される。

本研究では、バリデータの投票履歴を基に信頼度を算出し、信頼度を基に報酬を分配するとともに、誤った投票に対して Stake を減ずる罰則を課す方式について提案する。

3．研究方法・結果

前章で紹介したように、PoS は賞罰のメカニズムを導入してバリデータが正しい投票をすることを動機づけている。バリデータは正しい投票をすれば報酬を得ることができ、保有する Stake 量を増加させる。反対に、バリデータが誤った投票を行った場合、Stake の一部が没収され、バリデータの Stake 量が減少する。本節では、提案する報酬・罰則型 PoS アルゴリズムの詳細について述べる。初めに全体のメカニズムを紹介し、次にバリデータ信頼度の算出法について説明する。

３．１　報酬と罰則

ブロック・チェーンの維持管理を行うバリデータの集合を$N = \{1,2, \dots, V\}$とする。ブロックはタイムスロットt毎に生成され、バリデータはブロックが生成される毎にその正当性を検証し、投票を行う。タイムスロットt開始時点におけるバリデータ$i \in N$の Stake 量を$s_{i,t}$, tでの投票結果で与えられる報酬・罰則を$r_{i,t}$とする。このとき、タイムスロット$t+1$開始時点でのバリデータiの Stake 量$s_{i,t+1}$は次式で与えられる。

$$s_{i,t+1} = s_{i,t} + r_{i,t}$$

タイムスロットtにおけるバリデータiの投票結果を$x_{i,t} \in \{0,1\}$と定義する。0 はバリデータが誤った投票を行ったことを、1 は正しい投票を行ったことを表す。正しい投票とは、正当なブロックに対して「正当」と判定し、不当ブロックに対して「不当」と判定して投票を行うことを指す。反対に誤った投票とは、正当なブロックに対して「不当」、不当ブロックに対して「正当」と判定して投票することを意味する。不当ブロックに対して「正当」と投票することは、ブロック・チェーン全体の正当性の観点から極めて重大な誤りの投票行為であることに注意する。誤った投票は、意図して行われた場合と意図せず行われた場合の二種類が考えられるが（意図して行われるものは、正しいコンセンサスを失敗させるための攻撃として考えることができる。一方、意図せず行われるものは、ハードウェアの故障や、不安定なネットワークの影響によるものが考えられる。）、本稿ではこれを区別しない。
賞罰$r_{i,t}$は投票結果$x_{i,t}$を用いて次式で表すことができる。

$$r_{i,t} = \begin{cases} reward_{i,t}, \text{ if } x_{i,t} = 1, \\ penalty_{i,t}, \text{ otherwise.} \end{cases}$$

ここで$reward_{i,t}$はタイムスロットtにおけるバリデータiの報酬を、$penalty_{i,t}$はバリデータiの罰則を表す。報酬$reward_{i,t}$は次節で定義する信頼度$p_{i,t}$を用いて次式で算出する。

$$reward_{i,t} = p_{i,t} \cdot \beta$$

ここでβはプロトコルで定義されたタイムスロット毎の標準報酬額である。この標準報酬額βを基準に、信頼度$p_{i,t}$に応じて報酬$reward_{i,t}$が算出される。信頼度$p_{i,t}$が高いバリデータほど多くの報酬$reward_{i,t}$を得られる仕組みになっている。

罰則$penalty_{i,t}$はバリデータiの直前のタイムスロット$t-1$での Stake 量$s_{i,t-1}$を用いて次式で算出する。

$$penalty_{i,t} = -\gamma \cdot s_{i,t-1}, \quad 0 \le \gamma \le 1$$

ここでγは罰則の重みを表すパラメータであり、Stake 量 $s_{i,t-1}$を基準にどれだけの割合の Stake を没収するかを決定する。

３．２　バリデータの信頼度を考慮した報酬配布

本節では、バリデータの信頼度を用いた$reward_{i,t}$の算出方法を説明する。$p_{i,t} \in [0,1]$をタイムスロットtにおけるバリデータiの信頼度とする。信頼度$p_{i,t}$は投票結果$x_{i,t}$に応じて次式に従って更新される。

$$p_{i,t} = \delta \cdot p_{i,t-1} + (1-\delta) \cdot x_{i,t}, \quad 0 \le \delta \le 1$$

$p_{i,t}$は 1 に近いほど新規ブロックに対して正しい投票を過去に行ったことを表す。$p_{i,t}$ の式の右辺は指数荷重平均であり、重みパラメータδが小さいほど直前の投票結果を信頼度に反映させ、大きいδは平均的な投票結果を重視した信頼度を与える。

信頼度$p_{i,t}$の算出に指数加重平均を採用した理由は以下の通りである。

- バリデータの過去の投票実績を信頼度に反映させる必要がある。
- バリデータはハードウェアの故障やネットワーク障害などで誤った判定結果を投票する可能性がある。この場合、バリデータの計算環境が通常に戻って正しい投票を行う場合、その結果を速やかに追従させる必要がある。

４．数値例

４．１　シュミレーションモデル

ブロック生成間隔はd秒とし、これを 1 タイムスロットとする。シミュレーション時刻tは離散的に0,1,2,3,...,Tの値を取り、時刻Tでシミュレーションが終了する。タイムスロットtの開始時点において、新規ブロックが生成される。新規ブロックはタイムスロット毎に独立に確率 ξ で正当なものが提案される。各バリデータは新規ブロックの正当性について投票を行う。すべてのバリデータは確率ζで正しい投票を行う。すなわち、確率ζでバリデータは正当なブロックに対して「正当」、不正なブロックに対して「不正」と投票する。逆に確率$1-\zeta$で正当なブロックに対して「不正」、不正なブロックに対して「正当」と投票する。

時刻tでネットワーク上に存在するトークンの総額をS_tとすると、S_tは次式で表される。

$$S_t = \sum_{i=1}^{n} s_{i,t}$$

初期のトークン総額S_0をもとに、基準報酬額βを次式で算出する。

$$\beta = \frac{S_0 \cdot \epsilon}{T \cdot V}$$

ここで、ϵは全期間Tにおけるインフレーション率を示す。バリデータiの時刻$t+1$での Stake 量$s_{i,t+1}$は時刻tの賞罰$r_{i,t}$に応じて更新される。

性能評価量として、次式で与えられる時刻tでのバリデータの平均 Stake 量$s_{avg,t}$を考える。

$$s_{avg,t} = \frac{\sum_{i \in N} s_{i,t}}{V}$$

シミュレーションではブロック生成間隔を$d = 60$ [s] とし、2 週間のブロック生成過程を模擬する。これより最終時刻は $T = 20160$ となり、タイムスロットは $t \in \{0,1,\dots,20160\}$ の範囲となる。バリデータの総数は $V = 1000$ とする。すべてのバリデータに対して Stake の初期値を$s_{i,0} = 1000$、信頼度の初期値を$p_{i,0} = 0.5$ とする。このとき、$s_{i,avg} = 1000$、およびシミュレーション開始時点での Stake 量の総量は$S_0 = 10^6$となる。また、文献[16]を参考に 1 年あたりのインフレーション率を 0.15 とした。これよりシミュレーション期間 2 週間あたりのインフレ率は

$$\varepsilon = 0.15 \cdot \frac{14}{365} \approx 5.7534 \times 10^{-3}$$

で与えられる。

４．２　実験結果

４．２．１　信頼度推定重みパラメータの影響

最初に、バリデータの信頼度$p_{i,t}$の推定式における重みパラメータδが推定値に与える影響を調べる。ここでは簡単のため正当なブロックのみが生成される状況を考え、バリデータが正しい投票を行う確率ςを変化させて$p_{i,t}$の追従性を確認する。ςは、$1 \le t < 2500$のとき$\varsigma = 1$，$2500 \le t < 7500$のとき$\varsigma = 0.25$，$7500 \le t < 12000$のとき$\varsigma = 0.5$，$12000 \le t < 17000$のとき$\varsigma = 0.75$，$17000 \le t \le 20160$のとき$\varsigma = 1$，のシナリオで変化させる。

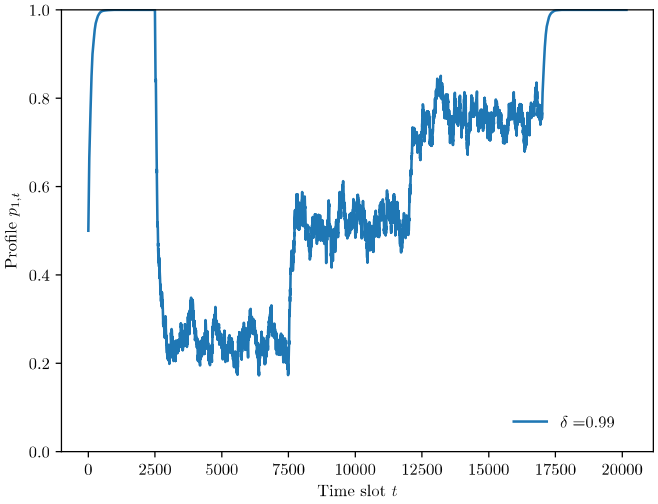

図 2：$p_{i,t}$の推定結果（$\delta = 0.99$）（copyright©2020 IEICE）

図 2 は一つのバリデータノードに対する$p_{i,t}$ の時間変化を表している。ここでは $\delta = 0.99$として$p_{i,t}$ を計算している。この図より、$p_{i,t}$は概ねςの変化に追従できていることが観察される。 以下では$\delta = 0.99$と設定したときのシミュレーション結果を示す。

４．２．２　正しい投票をする確率ςの影響

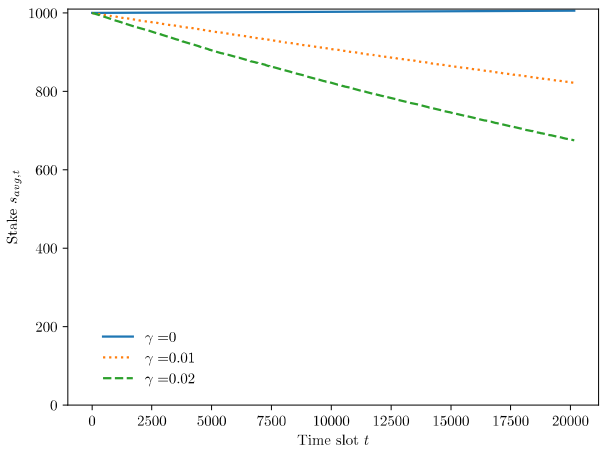

図 3 平均ステーク量$s_{avg,t}$の変化（$\gamma = 0.01$）

図 3 はタイムスロットtに対する 1000 台のバリデータの平均 Stake 量$s_{avg,t}$を示している。ここではςを全期間を通じて一定の $0.99, 0.999, 1$ とした場合の 3 種類の$s_{avg,t}$をプロットしている。ここでは罰則の重みを$\gamma = 0.01$としている。$\varsigma = 0.99$のとき、平均 Stake 量は単調かつ大幅に減少している傾向が観察される。$\varsigma = 0.999$でも単調減少ではあるが、減少量は$\varsigma = 0.99$と比べるとそれほど大きくない傾向を示している。$\varsigma = 1$, すなわち正確に投票を行う場合は平均 Stake 量は微小ながら増加する。

４．２．３　罰則の重みγの影響

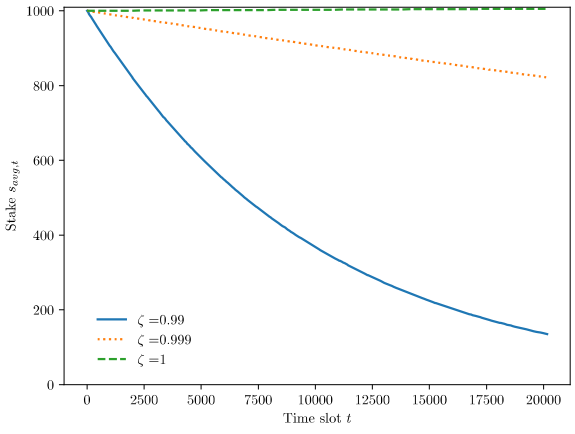

図 4：平均 Stake 量$s_{avg,t}$の変化（$\varsigma = 0.999$）

図 4 はタイムスロットtに対する 1000 台のバリデータの平均 Stake 量 $s_{avg,t}$の変化を表している。ここでは$\varsigma = 0.999$と固定したときの$s_{avg,t}$について、$\gamma = 0, 0.01, 0.002$ の 3 種類の場合をプロットしている。

図 4 より、$\gamma = 0.02$のときは平均 Stake 量は大きく減少し、$\gamma = 0.01$では緩やかな減少傾向が見られ、$\gamma = 0$のときは微小ながら増加していることが観察される。これより、罰則の重みγを大きくするほど、正しい投票をしないバリデータに対して厳しい罰を課すことがわかる。しかしながら、あまりにも厳しい罰則を課してしまうと、バリデータがシステムから離脱し、PoS による合意形成が機能しなくなる恐れがある。そのため、罰則の重みパラメータγについては慎重な設計が必要である。

まとめ

本報告書では、PoS における報酬・罰則付与型コンセンサス・アルゴリズムについて基本的な検討結果を紹介した。提案手法ではバリデータの信頼度を考慮したアルゴリズムを考え、正しい投票を行う動機づけを試みた。数値例より、提案手法はバリデータの信頼度を概ね正しく推定できることが示された。また、信頼度を導入することで、信頼度の高いバリデータは信頼度の低いバリデータよりも多くの報酬を獲得できることが示された。このことは、バリデータに対して正しい投票を動機づける可能性があることを示している。

ここでの提案手法では、信頼度の低下によって割り引いた報酬や、罰則によって取り去られた Stake の再利用については未検討である。今後の課題として、Stake の再利用を考慮したコンセンサス・アルゴリズムの検討、及びバリデータがより正確に投票を行うようなインセンティブを与えられるような報酬・罰則メカニズムの検討が挙げられる。

参考文献

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, 2008.
[2] V. Buterin, et al., “A Next-Generation Smart

Contract and Decentralized Application Platform," https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf}, 2014.

[3] K. Jae and B. Ethan, "Cosmos A Network of Distributed Ledgers," https://cosmos.network/cosmos-whitepaper.pdf}.

[4] G. Wood, "Polkadot: Vision for a Heterogeneous Multi-Chain Framework," https://www.win.tue.nl/~mholende/seminar/references/ethereum_polkadot.pdf,2016.

[5] GitHub, "Ethereum 2.0 Specifications," https://github.com/ethereum/eth2.0-specs.

[6] 松永赳尭, 張元玉, 笹部昌弘, 笠原正治, "Proof-of-Stake 型ブロック・チェーンの参加ノードへのインセンティブづ けに関する一検討," 電子情報通信学会技術研究報告 (NS2020-86), pp. 62-67, 2020.11.27.

[7] A.M. Antonopoulos, Mastering Bitcoin, O'Reilly, 2014.

[8] C. Mora, R.L. Rollins, K. Taladay, M.B. Kantar, M.K. Chock, M. Shimada, and E.C. Franklin, "Bitcoin Emissions Alone Could Push Global Warming above 2C," Nature Climate Change, vol.8, no.11, pp.931-933, 2018.

[9] S. King and S. Nadal, "Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," https://decred.org/research/king2012.pdf, 2012.

[10] StackExchange, "What Does the Term "Longest Chain" Mean?" https://bitcoin.stackexchange.com/questions/5540/ what-does-the-term-longest-chain-mean, 2012.

[11] J. Kwon, "Tendermint: Consensus without Mining," https://tendermint.com/static/docs/tendermint.pdf, 2014.

[12] S. Leonardos, D. Reijsbergen, and G. Piliouras, "Weighted Voting on the Blockchain: Improving Consensus in Proof of Stake Protocols," Proc. of IEEE ICBC 2019, pp.376-384 2019.

[13] R.C. Ben-Yashar and S.I. Nitzan, "The Optimal Decision Rule for Fixed-Size Committees in Dichotomous Choice Situations: The General Result," International Economic Review, vol.38, no.1, pp.175-186, 1997.

[14] A. Ouaguid, N. Abghour, and M. Ouzzif, "Towards a New Reward and Punishment Approach for Blockchain-Based System," Proc. of IEEE SysCoBIoTS 2019, pp. 1-7 2019.

[15] V. Buterin, "Slasher: A Punitive Proof-of-Stake Algorithm," https://blog.ethereum.org/2014/01/15/slasher-a-punitive-proof-of-stake-algorithm, 2014.

[16] GitHub, "Signal Non-Final Status of Base Reward and Desired Issuance Goal #971," https://github.com/ethereum/eth2.0-specs/pull/971.

この研究は、平成３０年度ＳＣＡＴ研究助成の対象として採用され、令和元年度～令和３年度に実施されたものです。