Discussion Paper Series A No.748

Ethereum Proof of Stake は持続可能か
― スマートコントラクト基盤間競争の観点から考える―

斉藤賢爾（早稲田大学）
副島豊（SBI 金融経済研究所）
杉浦俊彦（SBI 金融経済研究所(現格付投資情報センター)）
北村行伸（立正大学, 一橋大学）
岩村充（早稲田大学）

September 2023

Institute of Economic Research
Hitotsubashi University
Kunitachi, Tokyo, 186-8603 Japan

Ethereum Proof of Stake は持続可能か — スマートコントラクト基盤間競争の観点から考える —

斉藤 賢爾 [*] , 副島 豊 [†] , 杉浦 俊彦 [‡] , 北村 行伸 [§] , 岩村 充 [¶]

2023 年 9 月 7 日

概 要

Ethereum は The Merge アップデート以降、Proof of Stake に移行したことで消費電力がより小さく、また、より安全になったと喧伝されている。しかし、 仮にそうだとして、 その状態は持続できるのだろうか。

この論文では、Ethereum のネイティブ通貨である Ether (ETH) の価格が他のスマートコントラクト基盤との競争の影響を受けうることに注目し、Proof of Stake の設計がもたらすとされる 安全性と持続可能性について 疑問を投げかける。

Keywords: Proof of Stake, Blockchain, Cryptocurrency, Smart Contract, Competition、ブロックチェーン、仮想通貨、暗号資産、スマートコントラクト

JEL classification: B31, E42, E51

[*]早稲田大学 大学院経営管理研究科 教授
[†]SBI 金融経済研究所 研究主幹
[‡]SBI 金融経済研究所 研究主幹 (現 格付投資情報センター 執行役員)
[§]立正大学 データサイエンス学部 教授, 一橋大学 経済研究所 非常勤研究員
[¶]早稲田大学 名誉教授

Is Ethereum Proof of Stake Sustainable?

— Considering from the Perspective of Competition Among Smart Contract Platforms —

Kenji Saito*, Yutaka Soejima†, Toshihiko Sugiura‡,
Yukinobu Kitamura§, Mitsuru Iwamura¶

September 7, 2023

Abstract

Since the Merge update upon which Ethereum transitioned to Proof of Stake, it has been touted that it resulted in lower power consumption and increased security. However, even if that is the case, can this state be sustained?

In this paper, we focus on the potential impact of competition with other smart contract platforms on the price of Ethereum's native currency, Ether (ETH), thereby raising questions about the safety and sustainability purportedly brought about by the design of Proof of Stake.

Keywords: Proof of Stake, Blockchain, Cryptocurrency, Smart Contract, Competition

JEL classification: B31, E42, E51

*Professor, Graduate School of Business and Finance, Waseda University

†Principal research fellow, SBI Financial and Economic Research Institute

‡Principal research fellow, SBI Financial and Economic Research Institute (currently, Executive Officer, Rating and Investment Information, Inc.)

§Professor, Faculty of Data Science, Rissho University; Associated Research Scholar, Institute of Economic Research, Hitotsubashi University

¶Emeritus Professor, Waseda University

1　イントロダクション

1.1　動機

Bitcoin[21] は、従来の中央銀行による決済システムと異なり、参加者間の競争・協調にもとづく自律分散システムによる貨幣の創造と送金を成立させた。また、そのための道具である「ブロックチェーン」を設計・実装した初の試みとなった。

Ethereum[2] は後発のブロックチェーンとして設計され、(第 2.1節で詳しく述べるように条件付きではあるものの) 任意の状態の変化を表すプログラムコードを保存し、呼び出して実行する機能を実現した。これにより、送金、すなわち残高の変化のみならず、例えばトークンを移転することで表される何らかの権利の移譲を行うことなども可能にした。

両者は Proof of Work (PoW) として知られている不正防止策を応用し、累積した PoW のコストが最も重い履歴が最も正しい履歴であるという「ナカモト・コンセンサス[1]」を編み出し、またそれを拡張する[2]ことによって、ある高い水準で不正を防止し続けることにこれまでのところ成功している。

しかしながら、PoW ではマイナー間の計算競争を支えるために大量の電力が消費されるようになり、その量は中規模先進国の総電力消費量にも匹敵するようになっている。これは昨今の環境問題に鑑みて、大きな問題であるとの指摘がなされてきた（エネルギー消費の問題)。また、両ブロックチェーンは一定時間内で処理できるトランザクション[3]の数が極めて限定的であり (スケーラビリティの問題)、実行にも時間がかかりすぎるとの批判があった。

2022 年 9 月、Ethereum はエネルギー消費やスケーラビリティ等の課題を抱えていた PoW を捨て、Proof of Stake (PoS) と呼ばれる別の手法に移行した (この移行は「The Merge」と呼ばれる)。著者らは、移行を済ませた Ethereum が、これまでと同等な水準で持続的に不正を防止し続けられるかどうかに興味がある。

1.2　目的

この論文の目的は次の 3 点にまとめられる。

[1] この名称は、Bitcoin のアルゴリズムを開発した仮名の開発者であるサトシ・ナカモトに由来する。

[2] 第 2.3節にて後述する GHOST (Greedy Heaviest Observed Sub-Tree)。

[3] 権利の移譲とそれに伴う支払い等、分割できないひとまとまりの処理。

1. Ethereum の持続性の議論に、そのネイティブトークン[4]である Ether (ETH) の市場価格の水準およびスマートコントラクト実行基盤間の競争という視点を持ち込む。

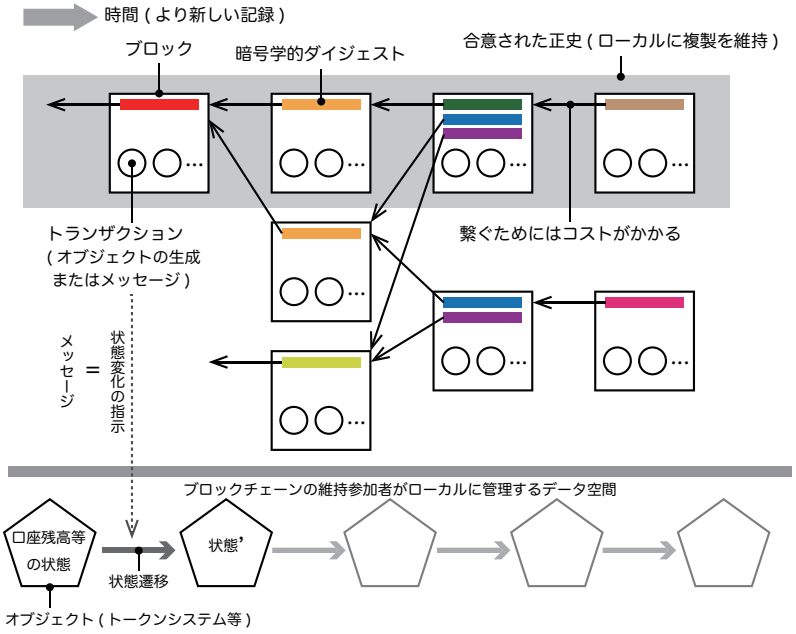
2. Ethereum における PoS (以降、Ethereum PoS) をモデル化し、価格や基盤間競争を論じうる土台を作る。

3. モデルを用いた議論により、Ethereum PoS が持続できない場合について検討する。

2 背景

2.1 ブロックチェーン

ブロックチェーン [21] は、一般に図 1 で示すように設計されている。



- ただし、Bitcoin や The Merge 後の Ethereum の各ブロックは、自己の手前のブロックを指す暗号学的ダイジェストをただひとつだけ持つ。

図 1: 抽象化されたブロックチェーン

初期から Ethereum の技術仕様を定めている文書 [27] によれば、ブロックチェーンは、トランザクションにもとづいた状態の移り変わりを管理す

[4]ブロックチェーンの維持活動の報酬として生成されるトークン。

るシステム (状態マシン) だと表現されている。すなわち、あるアドレスで示される口座の残高といった、検索キーと値の組 (変数[5]) の集合を「状態」として維持し、トランザクションを適用することで、その状態を変化させていくシステムである。

ただし、その状態マシンはブロックチェーンの維持参加者らが手許で管理するデータベース (ローカルに管理するデータ空間) で動作し、ブロックチェーンのデータ構造自体は、トランザクションを記帳した言わば台帳である。

スマートコントラクト　こうした台帳を作る動機は、もともとは自分が所持する貨幣を自由に使うことを誰にも止めさせないために、送金の事実を事実上変更不可能なかたちで記録するためだったと考えられる。

だが、そうした台帳にプログラムコードとそれが扱うデータ (定数や変数)、実行ログ、および実行による変数の変化を記録することで、送金に限らず、状態マシン一般について、(ブロックチェーンに書き込まれている範囲では) 真正に動作していることを万人が確認可能になった。これがスマートコントラクト [2] であり、Ethereum で初めて本格的に導入された。

スマートコントラクトのプログラムコードとその初期データをブロックチェーンに書き込む行為は、展開するという意味で「デプロイ」(deploy) と呼ばれる。

ブロックチェーンにおける状態マシンの複製　ブロックはトランザクション (を記述したデータ) の集まりである。トランザクションは、ブロックチェーンの維持参加者らがローカルに管理するデータ空間に状態マシンを構成するオブジェクト (スマートコントラクト) を投入したり、投入済みのオブジェクトにパラメータを含む実行の指示 (メッセージ) を送ったり、あるいはネイティブトークンを送金したりすることで状態の変化を引き起こす。

ブロックチェーンでは、参加者は自発的に検証者 (バリデータ) になり、それぞれのバリデータが任意に選択したトランザクションの正当性[6]を検証し、検証済みの複数のトランザクションのデータを集めて記録することでブロックが作成される[7]。

ブロックチェーンの実行とは、そのプロセスが何人にも止められないように、自律的に参加する各々のローカルなデータ空間に、状態マシンを完

[5]検索キーに対して得られる値が常に同じで変化しない場合は特に「定数」と呼ぶ。

[6]例えばトークンを二重使用していないか等、過去の履歴に照らして矛盾が無いかどうかや、トークンの現在の所持者が正当な署名を付けて移転を指示しているか等、権限をもつ利用者によりトランザクションが投入されているかどうか。

[7] どのバリデータがブロックを作成できるかについては、本節 (PoW の場合) や次節 (PoS の場合) の中で後述する。

全に複製する過程である。

状態マシンの複製は、分散システムの分野では、同じ機能をもつサーバを複数個動かすこと (冗長化) により、一部のサーバの停止や異常動作に耐えてシステムを継続できること (耐障害性) の実現を目的として、1980年代には確立していた手法である [25]。

状態マシンが複製されるには、複製を行う参加者の間で次の条件が満たされている必要がある。

1. 等しい初期状態が共有される。
2. トランザクションが等しい順序で共有される。
3. 状態に対して非決定的[8]な作用を及ぼすトランザクションは適用されない。

そのため、最初のブロック (いわゆるジェネシス・ブロック) が共有されること (上記 1) に加え、ブロックチェーンの維持参加者ら全員が、トランザクションの列を同じ並びで観測する (上記 2) 必要がある。その実現のため、ブロックの暗号学的ダイジェスト[9]が、直後に続くブロックに格納される。ブロック A のダイジェストをブロック B が格納するのであれば、ブロック A はブロック B に先行している必然性があるので、この構造により時系列が論理的に表現される。図 1でブロック間を繋ぐ矢印が時間の進行とは逆向きになっているのは、それぞれのブロックに格納されているダイジェストは、手前のブロックを一意に指し示している[10]からである。

ただし、一般に分散システムでは、参加者がいつでも正常に動作しているとは限らないし、ネットワークを通した伝送の遅延もあって、トランザクションの順序が異なって観測されることがある。上記 2の条件を満たすためには、トランザクションの順序を一意に決めるような、参加者間のコンセンサスの仕組みが必要となる。

ブロックチェーンにおいても、参加者の悪意や伝送の遅延等の理由で同時に異なるブロックが作られ、ブロックの列が分岐 (フォーク) すること

[8]同じインプットに対して必ず同じアウトプットを返す処理を「決定的」と呼び、必ずしも同じアウトプットにならない場合を「非決定的」と呼ぶ。 状態マシンの複製では非決定的な状態の変化は記述できないため、トランザクションの中で並列処理を行ったり、乱数を生成したりはできない。

[9]暗号学的ハッシュ関数を適用して得られた出力値。暗号学的ハッシュ関数は、任意の入力を 256 ビット等の決まったビット長の数値に変換して出力するが、入力が等しければ必ず等しい出力が得られるものの、入力が少しでも異なればまったく別の出力が得られ、どのような出力になるかは実際に計算するまで分からない。また、出力の値はそのビット長 (例えば 256 ビット) で表現可能な数の空間に一様に分布し、異なる入力から同じ出力が得られること (衝突) が起きる可能性は極めて小さい。

[10]ダイジェストの衝突の可能性は極めて小さく、また、仮に衝突が起き、過去のブロックと同じダイジェストが得られた場合は その新たなブロックは無効にできるので、ダイジェストによりブロックをユニークに識別できる。

がある (図 1にも分岐した複数の履歴が描かれており、バリデータが検証しながらそれらを形成しているのだから、それぞれの履歴の中には矛盾が無い)。そのため、上記 2の条件を満たすべく、ブロックの列が分岐した場合にどの列が正統[11]であるかに合意する参加者間の仕組みが必要となる。

ブロックチェーンでは、ブロックの作成にコストがかかるようにして、コストをかけて作成したブロックが連なることによりそのコストが蓄積されるようにしている。すなわち、現在までに蓄積されたコストを改めて負担することによってしか過去のブロックを改ざんできないという仕組みであり、こうした仕組みによって耐改ざん性を高めようとしている。この時、分岐した複数のブロック列の中でも、蓄積されたコストが最も大きいブロック列を最も正統な履歴と定義することにより、改ざんの困難さと履歴の一意性を同時に実現できる。これが「ナカモト・コンセンサス」である。

Proof of Work と Proof of Stake　ブロックの作成のコストは、ブロックを作成できる条件だと言い換えられる。

ブロック内に、それを作成するバリデータが任意に決められる番号 (Nonce: Number used Once) を置き、作成されたブロックの暗号学的ダイジェストが、典型的には手前のブロックから引き継がれ、参加者全員により同じアルゴリズムによって上下する「ターゲット」の値以下でなければならないという条件を設ける方式を Proof of Work (PoW; 作業証明) と呼ぶ。

PoW におけるバリデータ (マイナー) は、この条件を満たすダイジェストが得られるまで、Nonce を変化させながら暗号学的ハッシュ関数の計算を何度も繰り返すという作業を強いられる。この作業を行ったという証明 (ブロックのダイジェストがターゲット以下であること) を以て後述する「報酬」を得る行為は「マイニング」と呼ばれる。

PoW では、主として上述の計算作業に伴うコスト、換言すれば、コンピュータで計算処理を行うために必要な電力コストが、ブロック作成に必要なコストになっており、ブロックが次々と作成され、繋げられていくことで、計算作業に必要なコスト（電力コスト）が蓄積し、耐改ざん性を高める仕組みになっている。ただ、この方法には、不特定多数のマイナーが大量の計算を行うために電力消費量が膨大になるといった課題がある と指摘されている。しかし、グリーンエネルギーの重要性が高まるなか、生産調整が困難で蓄電対応もコストを要する同エネルギーの普及推進をいかに行うかが社会課題となっている。再生可能エネルギーの余剰電力が発生するタイミングでマイニングを行う「グリーンマイニング」は、補助金な

[11] ここでの「正統」は、予め定められた何らかの正統性に皆が追従するのではなく、延伸すべき列だと相当数の参加者が認めたものを正統と見なすという意味である。

どに頼らずグリーンエネルギーの採算性を高め、グリーンエコノミーへの移行を促進する手段として注目されている [15] 。

こうした間接的な方法によらず、アルゴリズムの変更によってこれらの課題を解決するとされるのが、Proof of Stake (PoS) である。第 2.3節にて後述する通り、これは、暗号資産をデポジットすることでブロックやその列に投票する権利を得て、得票により正統な履歴を決定していく方法である。

報酬　正統なブロック列 (すなわち合意された正史) の維持 (記録とその保全) に関わる参加者らは、その作業の報酬として、当該ブロックチェーンがプロトコルに基づいて無から生成するネイティブトークンを受け取る。

2.2　Proof of Work の経済

参加者が、トークンで払い出される報酬による利益を求めてブロック列の維持に参加するのだとしたら、次の理由により維持のコストとトークンの市場価値は長期的には均衡する。

前節で述べた通り、PoW の場合、維持のコストは主に電力である。トークンの価格が高く、トークンで払い出される報酬の期待値が電力コストを上回る場合、マイニングに新たな参入が起き、参加者全体で見た計算力が増大することで、ブロックの適切なダイジェストを引き当てる頻度が高くなる。すなわち、ブロック作成の間隔が短くなる。ブロック作成の間隔が短くなると、プロトコルに沿って (Bitcoin の場合であれば平均 10 分間に 1 回というブロック作成の間隔を維持すべく)、ターゲットがより小さく調整される。するとマイナーが 1 単位のトークンを得るために必要な電力コストは増大し、報酬に接近する。逆にトークンの価格が低く、報酬の期待値が電力コストを下回る場合、マイニングからの撤退が起き (少なくともハードウェアの電源が切られ)、参加者全体で見た計算力が減少することでブロック作成の間隔が長くなる。ブロック作成の間隔が長くなると、プロトコルに沿ってターゲットがより大きく調整される。その結果、マイナーが 1 単位のトークンを得るために必要な電力コストは減少し、やはり報酬に接近する。

著者らは、[17][24] にてこのことを詳細に論じ、価格が不安定になりがちな PoW にもとづく cryptocurrency にて価格を安定化させる設計上の工夫を提案した。本論文は、同様の経済学的な考え方を Ethereum PoS に適用し、分析を試みるものである。

2.3 Ethereum における Proof of Stake

Ethereum は、当初は PoW を採用していたが、2022 年 9 月 15 日に完了した The Merge アップデート以降、PoS に移行した [11][8]。以下では、次章以降の議論を理解するための前提として、Ethereum における PoS の仕組みを説明する。

デポジット　バリデータとしてブロックチェーンの維持に参加するユーザは、Ethereum のネイティブトークンである Ether (ETH) を予め預託 (デポジット) する必要がある (無論、参加者はバリデータにならないことを選択し、手数料を支払ってトランザクション実行の恩恵を受ける利用者として Ethereum に参加してもよい) 。参加に必要なデポジット額は 1 バリデータ当たり 32 ETH である。参加に伴う報酬はデポジット額に加算され、ペナルティ (後述) はデポジット額から差し引かれるため、参加資格を得た後のデポジット額は増減する。ただし、報酬額を算定する場合等に有効なデポジット額 (effective balance; 実効残高)[20] は最大でも 32ETH を上回ることはない。また、デポジット額が 16ETH を下回ると自動的にバリデータの地位を喪失する。

スロットとエポック　Ethereum における時間は 12 秒間隔の「スロット」と 32 スロットからなる「エポック」で区切られる。

各スロットでは、ランダムに選ばれた 1 バリデータが 高々ひとつのブロックを作成し (選ばれたバリデータがオフラインだった等の理由でブロックが作成されない場合もある) 、それを全体に対して提案する。そして、ランダムに選ばれたバリデータによる委員会[12]が、提案されたブロックの正当性を証言 (attest) する。証言は署名されるが、同じ内容の証言は BLS 署名 [1] を用いて集約される。

各エポックの最初のブロックは「チェックポイント」と呼ばれる。 すべてのバリデータはふたつの連続するチェックポイント c からなる組 $\langle c_{e-1}, c_e \rangle$ (ただし e は最新のエポック番号) に対してその正当性を証言する。組に含まれるうち古い方を「ソース・チェックポイント」、新しい方を「ターゲット・チェックポイント」と呼ぶ。 全バリデータの ETH によるデポジット額の合計の $\frac{2}{3}$ 以上に相当する証言を集めた組について、

[12] ブロックへの証言を担当する委員会には「ビーコン（beacon）委員会」(The Merge に先立ち、PoS の機構を担う「ビーコンチェーン」を PoW チェーンから独立して運用していたことからこの名がある) と「同期 (sync) 委員会」の 2 種類がある。ビーコン委員会はエポック毎にシャッフルされ、すべてのバリデータがどれかのスロットの委員会に割り当てられる。同期委員会はランダムに選ばれた 512 バリデータから成り、256 エポック毎に選出される。後者はブロックチェーンの維持活動に参加しないクライアント (軽量クライアント) によるブロックの検証を容易にするために導入された。

1. c_{e-1} (ソース・チェックポイント) は「確定 (finalize)」され、

2. c_e (ターゲット・チェックポイント) は「正当化 (justify)」される。

c_{e-1} は $\langle c_{e-2}, c_{e-1}\rangle$ に対して証言が集められた際に正当化されていた[13]ことになるので、チェックポイントは「正当化」→「確定」と段階的に認定されていくことになる。 あるチェックポイントの直前に生成されたブロックが正当化されるには、典型的に 1 スロット分の時間しかかからないが、チェックポイントの直後に生成されたブロックが正当化されるためには、約 1 エポック分の時間を要する。確定のためには加えて 1 エポック分の時間が必要となる。このことから、ブロックに格納されたトランザクションは、証言が順調に進むのであれば最長でも 13 分弱 (2 エポック分の時間) で確定されることになる。

しかし、証言が十分に集まらなかった場合、正当化や確定は起こらない。 連続して 5 エポック以上、確定に失敗した場合、すなわちデポジット総額に対して $\frac{2}{3}$ 未満の証言しか集められない状況が続いた場合は、マジョリティとなる参加者らとは異なる証言をした (あるいは証言を行わなかった) バリデータらのデポジットから没収するペナルティがある。この没収は、いずれマジョリティがデポジット総額の $\frac{2}{3}$ 以上となり、確定が行われるようになることを促進する。

フォークの選択　この機構においても、分散システムの常として遅延や障害、そこからの回復や、あるいは攻撃などを要因とする行き違いが起き、ブロックの列すなわちチェーンが分岐しうる。その場合、 正当化されたチェックポイント以降の分岐毎のブロックへの証言の実効残高換算での合計 (重み) を比較し、 最も大きいものを採用する LMD-GHOST[14][6] アルゴリズムによって正統な分岐を決定する。 チェックポイントの正当化を含むこの部分が、Ethereum PoS における狭義のコンセンサス・アルゴリズムである[15]。

RANDAO　脚注 8にも示した通り、非決定的な処理があると状態マシンを複製できないため、ブロックチェーンの実行においては通常の方式で乱数を得ることはできず、何らかの決定的かつ予測不能な方法を用いて、全員が一致する乱数列を得なければならない。そこで、ブロックの提案

[13]最新の組に対する証言時において、最新の正当化されたチェックポイントだったことを示すが、これが「ソース・チェックポイント」の定義である。

[14]LMD-GHOST は Last-Message Driven, Greedy Heaviest Observed SubTree の略。GHOST は Ethereum で採用された、拡張されたナカモト・コンセンサスである。

[15]分散システムにおけるコンセンサスは、 並行して実行されるすべての正常なプロセスにおいて同じ変数 の値が一致することを示す [18]。ブロックチェーンの場合は、ブロック番号が変数名であり、ブロックのダイジェストがその値だと言える。

者や、ビーコン委員会・同期委員会のメンバーの選出等、ランダムな選択を行う必要がある際は RANDAO (Random DAO) と呼ばれる乱数を用いる。これは巷にあふれる、スマートコントラクトにより実現されるものとは異なる概念的な DAO (Decentralized Autonomous Organization; 分散型自律組織)[3] であり、Ethereum の状態の一部として保存されている 256 ビットの値である。この値はブロックが提案される度に次のようにシャッフルされる: ブロックの提案者は、エポック番号にもとづくデータに対する検証可能な BLS 署名を施す。その署名の 256 ビットダイジェストと既存の RANDAO 値の排他的論理和をとったものが新たな RANDAO 値となる。

Gas 使用料　スマートコントラクトの実行に要する計算資源量 (計算ステップ数やストレージの使用量) は gas という単位で測られる [10]。gas はまた、ブロック内の全トランザクションの実行に要する gas を総計することで、そのブロックの規模を表す数値としても用いられる。トランザクションを投入するユーザは、1 gas 当たりに手数料として支払う ETH を指定する (典型的には Gwei[16]の単位で測られる程度となる)。これを gas 価格 (gas price) と呼ぶ。Gas 価格に、実際に消費された gas を掛けた額が gas 使用料 (gas fee) となる。

2021 年の London アップデート以降、gas 使用料は「基本料金 (base fee)」と「優先料金 (priority fee)」に分けられることになった。基本料金の単価 (1 gas 当たりの価格) は直前までのブロックの混み具合に応じてプロトコルにより決定される。ブロックの最大サイズは 3,000 万 gas であり、ブロックを作成するバリデータは、この最大サイズの半分である 1,500 万 gas を目安としてブロックにトランザクションを組み込む。実際に作成されたブロックのサイズが目安より大きければ、続く次のブロックでの基本料金は最大で 12.5% 引き上げられ、反対にブロックサイズが目安より小さければ、続く次のブロックでの基本料金は引き下げられる。一方、優先料金の単価は、トランザクションの処理をどれだけ優先してほしいかというニーズに基づいて、トランザクションの投入者が任意に設定する。

Gas 使用料の大半を占める基本料金は消却 (burn) され、ETH の流通から取り除かれる。優先料金は、当該ブロックを提案したバリデータの収入となる (The Merge 以前はブロックを生成したマイナーの収入となった)。

こうした設計は次の理由に拠るとされる [5]。

- 基本料金をプロトコルに基づいて自動的に求めることができ、料金を予測可能にできる。

[16]Ether の最小単位である wei は 10^{-18} ETH であり、 Gwei は 10^{-9} ETH。

- 基本料金を消却し、バリデータに渡さないことにより、次を実現できる。
  - トランザクションの実行には ETH でしか料金を支払えないことを強制し、Ethereum における ETH の経済的価値を確立させる。
  - Gas 使用料を巡るバリデータによる戦略的な行動[17]を抑制する。
  - インフレーションに対して対抗する[18]。

報酬とペナルティ　上記のバリデータとしての仕事に参加することで報酬が得られ、仕事を怠ることでペナルティがある [12][13]。どちらもデポジットに対してエポック毎に適用される。

各バリデータが得られる報酬は、各々のデポジットの実効残高に比例し、全バリデータによるデポジット総額の平方根に反比例する (後に第 3.3節にて詳細を説明する)。実効残高は ETH 単位に丸められた整数値であり、最大値は 32 ETH である。

報酬は以下の仕事の対価として支払われる。

- ソースチェックポイントにタイムリーに証言する。
- ターゲットチェックポイントにタイムリーに証言する。
- 最新のブロックにタイムリーに証言する (ビーコン委員会に参加) 。
- 同期委員会に参加する。
- ブロックを提案する。

証言がスロット単位で観測して遅いタイミングで行われるほど報酬は小さくなる。 また、十分な証言が得られないことでチェックポイントの正当化や確定が行われず、マイノリティ側のバリデータに対してペナルティが適用される間、マジョリティ側に対しても証言に対する報酬は支払われない (検閲やサービス否定 (DoS) 攻撃により他のバリデータを陥れる行為を抑制するため)。

ブロックの提案者は、ブロックに含まれる正当な証言の数に比例した追加の報酬を受け取る。また、他のバリデータによる不正行為の証拠をブロックに組み込むことでも報酬を大きくできる。

[17]例えば、使用料の一部をユーザにキックバックしたり、ダミーのトランザクションを自ら投入したりすることで、使用料を不当に引き上げること。

[18]Ethereum に限らず、いわゆるクリプト界隈では貨幣の希少性とインフレの関係に対するナイーブな理解が受け容れられている。

一方、ペナルティは以下の場合に課され、当該参加者のデポジットから没収される (ペナルティの基本額は、正しく参加した場合に得られたであろう報酬と等しい)。

- 同期委員会に選ばれた際に応答しない場合。
- チェックポイントの組に対して証言しない場合。

デポジット総額の $\frac{2}{3}$ 以上に当たるバリデータが正常に動作している場合、マイノリティ側に課せられるペナルティは大きくない。マジョリティが $\frac{2}{3}$ に満たない場合 (確定が行われない場合)、ペナルティは大きくなる。

また、次の行為が観察される場合、バリデータは追放される (slashed)。すなわち、デポジット額の $\frac{1}{32}$ が没収され、36 日の猶予期間を経て、当該参加者はバリデータの資格を自動的に喪失する。

- 同一スロットにて複数の異なるブロックを提案する。
- 履歴の改変を試みる。
- 二重投票する。

スラッシングを受けるバリデータが複数いる場合、個々のバリデータのデポジットから没収される額は大きくなる (共謀への対策)。

以上から総合して、バリデータとして Ethereum に参加すると年率で 2 ～ 20% の ETH での報酬が得られるという [13]。典型的には 5% 未満程度となる。

退出　次の方法でバリデータのリストから取り除かれる。

- ペナルティによりデポジットが基準値 (16ETH) を下回った場合やスラッシングによりバリデータの資格を喪失する。
- 署名を要する退出メッセージにて表明することで自ら退出する。

一定期間中に退出できるバリデータの数は制限される (参入できるバリデータの数も制限される)。一度退出したバリデータは復帰できない。

3　Ethereum PoS の持続性に対する懸念

3.1　The Merge 以前

過去の Ethereum は PoW にもとづいていたため、基本的には ETH の市場価値と使用する電力コストの間に著者らが [17][24] で指摘したような均衡の関係があったと考えられる。

加えて、Ethereum はスマートコントラクトの実行基盤であるので、[26] が指摘しているような参加インセンティブのミスマッチの構造があった。すなわち、ブロックチェーンの維持に関わるマイナーたちにとっては ETH の獲得とその価格の上昇がインセンティブである一方、アプリケーションの開発者やユーザにとってはスマートコントラクトの実行に伴う利益が参加のインセンティブである。アプリケーションの開発者やユーザにスマートコントラクトをデプロイし実行したいという欲求がある限り、彼ら・彼女らは gas 使用料を支払うべく ETH を買い支えると考えられるが、他方で gas 価格や ETH の価格の上昇はユーザの参加インセンティブを減じる方向に作用する。

このインセンティブのミスマッチにより、ETH の価格が暴落する場合に、アプリケーションとは無関係の理由で Ethereum のブロックチェーンが停止する恐れがあった[19]。

ただし、PoW の場合、ETH の価格は電力コストを言わばアンカーとして、実体経済と関係づけられていた。ハードウェアの購入・売却や電源の投入・遮断を通して、ETH の価格と連動するマイナーの急激な参入・退出は抑制されていたと考えられる。Ethereum における PoW は GPU の利用が主流であり、ハードウェアが汎用的で、昨今の機械学習の応用機運の高まりから需要も高く、売却は容易だとしてもである (このことは旧マイナーらが、自らの退出を促すとも言えた The Merge を現実的選択と見なせた一因でもあっただろう)。

3.2 The Merge 以降

The Merge によって導入された PoS のもとで、Ethereum のバリデータが負担する 主たるコストは、ブロックの作成等、ブロックチェーンの維持に要する計算資源量が大幅に減少したことから電力コストではなくなる一方、バリデータとしての資格要件としてデポジットを求められる ETH の機会費用になると考えられる。具体的な機会費用としては、ETH を任意のタイミングで売却することで得る売却損益や、ETH を他のブロックチェーン基盤や DeFi 等に預託したり貸し付けたりすることでより高いリターン率で ETH その他のトークンを報酬として受ける機会などが考えら

[19]対して Bitcoin ブロックチェーンの場合は、基盤上に展開されているアプリケーションは基本的にネイティブトークンである BTC の転送のみである。当初言われていたように、BTC の転送機能が主に資金決済手段として用いられ、かつトランザクション手数料がユーザにとって看過できない水準にあるとすれば、上述の Ethereum PoW と同様にマイナーとユーザの間で参加インセンティブのミスマッチが生じうる。しかし実際には、BTC を「資産 (投資対象)」とみなし、その価格上昇を期待して BTC の移転機能を利用しているユーザによる取引量が大半なため、現在の Bitcoin ブロックチェーンでは、アプリケーションのユーザと基盤維持参加者 (マイナー) の参加インセンティブは合致していると言える。

れる。もっとも、ETH の価格上昇が期待できる限り、売却機会の逸失コストは小さく、またバリデータとしての参加報酬として得る ETH の価値も上昇することが期待できるため、バリデータの期待損益、すなわち参加インセンティブは ETH の価格動向そのものに依拠することとなる。

バリデータの参加インセンティブがネイティブトークンの価格動向に紐づくこと自体は PoW と変わらないが、バリデータが負担するコストのなか でトークンの価格形成のアンカーとなり得るもの の価値 (トークンの価格を実体経済における価値と結び付けるもので、PoW の電力コストに相当するもの) が、PoS では 大幅に下がっている点が大きな違いである。一方、アプリケーションの開発者やユーザにとってはスマートコントラクトの実行に伴う利益が参加のインセンティブであり、スマートコントラクトの実行に必要な gas 使用料がディスインセンティブになる。このことは、PoW であれ PoS であれ変わらない。

つまり、Ethereum PoS では、バリデータの参加インセンティブの構成要素の中に、実体経済との紐付けになるアンカーが失われた状況にあって、アプリケーションの開発者やユーザの参加インセンティブの構成要素である「スマートコントラクトの実行による利益」が、gas 使用料と (長期的に) 均衡することを通じて ETH の価格を実体経済につなぎ止めるアンカーになると考えられる。

従って、Ethereum PoS における ETH の均衡価格を考えるにあたっては、スマートコントラクトの開発者やユーザの Ethereum への参加インセンティブ、すなわち彼ら・彼女らが Ethereum に参入し、また退出する条件を考える必要がある。

Ethereum がスマートコントラクトの実行基盤として独占的な立場にあれば、gas 使用料の高騰によって開発者やユーザが基盤の利用を諦めるほかない状況に陥る可能性があるし、現に 2021 年以降でしばしば価格が高騰した局面ではそうした実例も少なからず聞かれた。しかし、スマートコントラクトの実行基盤はもはや Ethereum のみではなく、ユーザは複数の実行基盤の間で gas 使用料の水準や基盤としての利便性・安定性等を比較検討し、利用するブロックチェーンを選択することが可能になっており、このことは、NFT[9] のマーケット [22] 等においてすでに始まっている。スマートコントラクトの実行基盤もまた、競争に晒されているのであり、Ethereum がその敗者とならないとも限らない。

3.3 Ethereum PoS のモデル化

ここで、「ユーザへの効用と費用」、「gas のマーケット」、「バリデータの収入と費用」「ETH 総量の変化」について簡単な数学的表現によりモデル化し、複数の実行基盤の間の競争の作用について論じる。

ユーザへの効用と費用　トランザクション x が実行されることによる、x の投入者であるユーザ $x.u$ にとっての効用を $\mathcal{U}_x^{x.u}$ とし、法定通貨により測られるものとする。また、x を特に Ethereum で実行することの $x.u$ にとっての効用は $\mathcal{U}_{x_E}^{x.u}$ で表せ、同様に法定通貨で測れるものとする。

トランザクション x の gas を $x.g$ とする。ブロック番号 (高さ) h のブロック、すなわちトランザクションの集合 X_h における基本料金の単価 f_h は、[5] にもとづいてブロックの最大サイズ G から得られる目安 $\frac{1}{2}G$ と実際に作成されたブロックの gas の比によって料金の引き上げ (または引き下げ) 比を求める関数 F_Δ を用いて

$$f_h = \begin{cases} 1\,\text{Gwei} & h = h_0 \\ F_\Delta\left(\sum_{x \in X_{h-1}} x.g, G\right) f_{h-1} & h > h_0 \end{cases}$$

で表される (ただし h_0 は London ハードフォーク時点のブロック高)。x の投入者であるユーザ $x.u$ がブロック番号 h の時点で支払うつもりの優先料金の単価を $p_h^{x.u}$ とし、ETH と法定通貨 (ここでは仮に USD) の比価 (USD/ETH) を θ とすれば、x の gas 使用料は

$$(f_h + p_h^{x.u})\, x.g\, \theta$$

で表せる[20]。

ここから、ユーザ $x.u$ が Ethereum のブロック高 h に相当するスロットに向けて x を投入するための合理的条件は次の式で表せる。

$$\mathcal{U}_{x_E}^{x.u} - (f_h + p_h^{x.u})\, x.g\, \theta \geq 0 \tag{1}$$

すなわち、ユーザ $x.u$ にとって、効用 $\mathcal{U}_{x_E}^{x.u}$ が大きければ大きいほど、また gas 使用料 $(f_h + p_h^{x.u})\, x.g\, \theta$ が小さければ小さいほど、Ethereum に参加して x を実行するインセンティブは強まる。

効用 $\mathcal{U}_{x_E}^{x.u}$ を大きくするには、例えば、Ethereum でより高度なスマートコントラクトが実行できるような機能を提供すること等が考えられる。間接的な効果、外部経済効果を持つものとしては、例えば、多数かつ多様なアプリケーションが展開され、ユーザがそれらを選択的に利用して常に高品質のサービスを安く享受することができたり、様々なアプリケーションを組み合わせて使うことでより高度なサービスが享受できたりすること

[20] ちなみに、f_h の説明変数である $\sum_{x \in X_{h-1}} x.g$ と $\frac{1}{2}G$ の比はトランザクション処理の需要と供給が緩和または逼迫している状況を表すもので、優先料金の単価 $p_h^{x.u}$ にも影響を及ぼし得る。これは、プロトコルで予め定式化された (自動的に決定される) 基本料金の単価の変動だけでは需給調整が十分に行えない場合に、ユーザの裁量に基づいて設定される優先料金の単価を、補完的な需給調整機能として活用することを企図したものと解することができる。

が考えられる。また、作成コストのかかるブロックを連ねて耐改ざん性を高めてきた実績は、実行基盤としての安定的な稼働に対する信頼感を高めていると考えられる。

一方、gas 使用料 $(f_h + p_h^{x.u})\, x.g\, \theta$ を小さくするには、x にとって $x.g$ は固定であるので、1) gas 価格 $(f_h + p_h^{x.u})$、2) ETH と法定通貨 (USD) の比価（USD/ETH) θ が、それぞれ小さくできればよい。

このうち、1) については、ブロックの最大サイズ G を大きくすることで gas 価格を小さくできる[前述の脚注20]。Ethereum が今後導入する予定のシャーディング (水平分散)[21]は、ひとつにはこうした効果を狙っているのだろう。ただ、需要[22]に対して十分に大きなサイズにしなければ、処理能力の閾値を超過して gas 価格が急騰する事態を十分には抑止できない点には留意が必要である。

Gas のマーケット　これまでの議論はスマートコントラクトの実行基盤として Ethereum のみが存在すると仮定したものである。しかし、前述のとおり、スマートコントラクトの実行基盤はもはや Ethereum のみではないため、アプリケーションの開発者やユーザが Ethereum 以外の実行基盤も選択できる状況を考える必要がある。

競合するスマートコントラクト実行基盤 (議論のため、そのすべての仮想マシンにおいて x に相当する処理は実行可能で、所要の gas である $x.g$ のコストも各々のネイティブトークンと法定通貨建てで計量可能だとする) の集合を L とし、$l \in L$ であるような l について、その gas 価格を f^l (基盤によって基本/優先料金の区別がない可能性もあるので単純化のため区別しない)、ネイティブトークンと法定通貨との比価を θ^l とし、$x.u$ が l にて x を実行することの効用を $\mathcal{U}_{x_l}^{x.u}$ と表すとすれば、$x.u$ が Ethereum を使い続ける合理的条件は、式 (1) と次の式 (2) が同時に成立する論理積で表せる。

$$\forall l \in L\colon \quad \mathcal{U}_{x_E}^{x.u} - (f_h + p_h^{x.u})\, x.g\, \theta \quad \geq \quad \mathcal{U}_{x_l}^{x.u} - f^l x.g\, \theta^l - \mathcal{EC}_{x_{E/l}}^{x.u} \qquad (2)$$

ここで $\mathcal{EC}_{x_{E/l}}^{x.u}$ は、前述したような Ethereum の利用に伴う (正の) 外部経済効果で、ユーザが Ethereum から競合する他の実行基盤 l に移ろうとする場合に、個々のトランザクションの処理に要する gas 使用料とは別に生じるコスト (または失う効用) である (Ethereum へのロックイン

[21]全バリデータがブロック内のすべてのトランザクションを検証するのではなく、各バリデータがブロック内の分割された管理区分 (シャード) を均等に担当する方式。ただし、バリデータの処理が負荷分散されることにより G が m 倍になるだけであり、少なくとも過去の設計では $m = 64$ とされる。

[22]経済的事象では珍しくないが、一時的で急激な需要の増減に対処する必要もあり得る。

効果)。競合する実行基盤の方が Ethereum よりも大きい正の外部経済効果を持つ場合には、$\mathcal{EC}^{x.u}_{x_{E/l}}$ は負の値をとることも考えられる。

上述の通り、ここでは議論の単純化のために Ethereum と競合する他の実行基盤でトランザクション x を同様に処理できる (全く同じサービスを提供できる) と仮定しているため、$\mathcal{U}^{x.u}_{x_E}$ と $\mathcal{U}^{x.u}_{x_l}$ は等しくなる。さらに単純化のために、Ethereum の外部経済効果 $\mathcal{EC}^{x.u}_{x_{E/l}}$ を 0 と仮定する (その妥当性は第 4.3節で議論する) と、式 (2) はそれぞれの基盤における gas 使用料 (を法定通貨建てに換算したもの)、すなわち Ethereum での gas 使用料である $(f_h + p^{x.u}_h)\, x.g\, \theta$ と競合基盤での gas 使用料である $f^l x.g\, \theta^l$ の大小関係に依拠する条件式となる。x が同じ計算である以上、$x.g$ は基盤に関わらず同じであるので、式 (2) は $(f_h + p^{x.u}_h)\, \theta$ と $f^l\, \theta^l$ の大小関係、すなわちそれぞれの実行基盤における gas 価格 $(f_h + p^{x.u}_h)$ と f^l の大小関係およびネイティブトークンの法定通貨比 θ と θ^l の大小関係に帰着することになる。

この競争は本来的な意味で gas のマーケットを形成する。すなわち、真正性が検証できる「コードの実行量 + データの保存量」を表す gas を商品として、その供給能力と価格にて Ethereum (レイヤー 1 および 2)[23] を含む複数のスマートコントラクト実行基盤が競争するマーケットである。

スマートコントラクトの実行基盤のなかで Ethereum の利用者が圧倒的に多い現在の市場では往々にして $\theta^l < \theta$ であることから、仮に Ethereum の gas 価格 $(f_h + p^{x.u}_h)$ と競合する他の実行基盤の gas 価格 f^l が同水準だとしても、法定通貨建てでみた gas 使用料は競合する実行基盤の方が低くなる。その結果、NFT マーケット等ですでに Polygon[23] などの実行基盤を利用する例が見られているように、Ethereum 以外の基盤が好まれるようになり、$x.u$ が保持していた ETH が売られるなら θ は減少し、均衡 ($\theta^l = \theta$、ひいては $(f_h + p^{x.u}_h)\, x.g\, \theta = f^l x.g\, \theta^l$) に向かうこととなる。

もっとも、gas 価格の高騰やトランザクションの処理遅延の問題に対して Ethereum が無策というわけではなく、前述したシャーディングによりブロックの最大サイズの拡張と同様の効果を持つ処理能力の引き上げを図ったり、レイヤー 2 の技術である ZK-rollup[14] 等の導入を図ろうとしたりしている。

Rollup はトランザクションをオフラインで実行する仕組みであり、ZK はゼロ知識 (Zero Knowledge) を表す。ZK-rollup は、トランザクションをレイヤー 2 で (レイヤー 1 から見ると「オフラインで」) 実行したうえで、そのトランザクションの中身を明かさずに、それが正しく実行されたことをレイヤー 1 で検証できるような仕組みである。多数のトランザク

[23] 第 1 階層であるレイヤー 1 は本稿で説明するような Ethereum の基盤そのものを指し、第 2 階層であるレイヤー 2 は、トランザクションをブロックチェーンから見てオフラインで実行し、その証拠をレイヤー 1 で検証可能にする技術の総称である。

ションをバッチで実行し検証可能にできるため、スケーラビリティの課題を解決できるとして期待されている。トランザクションを全てレイヤー 1 で処理する従来の方法に比べて、ZK-rollup の仕組みの下ではレイヤー 1 での処理量が 例えば 0.3% 程度まで減少する [19] ため、仮にレイヤー 2 のサービスがレイヤー 1 に対して支払うべき gas 価格や ETH の法定通貨建て価格が従来と同じであったとしても、レイヤー 2 のサービスにユーザが例えば USD 建てで支払う料金は、従来の $\frac{1}{300}$ 程度まで減少する。この結果、スマートコントラクトを実行したいユーザが保持すべき ETH の量は少なくなるので、このこと自体は ETH の法定通貨建て価格の下落圧力になりうるが、1 トランザクション当たりの料金の低下がより多くの需要を喚起し、レイヤー 2 まで含めた Ethereum 環境が増加した需要に対処できる処理能力を持つのであれば、競合する他の実行基盤に対する優位を確保しつつ、ETH の法定通貨建て価格を (相応の水準で) 維持することが可能となるかもしれない。

以上から、The Merge 後の Ethereum がシャーディングとレイヤー 2 によるスケーリングを狙うのは、自己の存在意義を維持するための戦略として意味があると言える。

バリデータ収入と費用　あるエポック e において、n 個のバリデータが稼働しているとする。i 番目のバリデータの実効残高を b_e^i とし、その振る舞いに応じた [12] にもとづく報酬・ペナルティの係数を次の 2 種類用意する。

- n に依らず、バリデータ i の行動のみによって定まる係数 r_e^i
- n に応じてスロット毎に確率的に機会が発生する、ブロック提案や同期（sync）委員会参加の有無によって定まる係数 w_e^i

e の s 番目のスロット、すなわち高さ $h = F_B(e, s)$ (ただし F_B はエポックとスロットからブロック番号を求める関数であり、不在を表す $\perp$ を返しうる) のブロック X_h (トランザクションの集合) における優先料金の総和を

$$P_{e,s} = \begin{cases} 0 \text{ wei} & h = \perp \\ \sum_{x \in X_h} p_h^{x.u}\, x.g & h \neq \perp \end{cases}$$

と表すとすれば、e におけるバリデータ i の収入の期待値は

$$\left(\frac{r_e^i\, b_e^i}{\sqrt{\sum_{j=1}^n b_e^j}} + \frac{1}{n} \sum_{s=1}^{32} \left(P_{e,s} + \frac{n w_e^i\, b_e^i}{\sqrt{\sum_{j=1}^n b_e^j}} \right) \right) \theta$$

で近似的に表せる。

ここで、単純化のために全バリデータの実効残高が常に 32 ETH である、すなわち全バリデータが業務を常に完璧にこなすと仮定する。この場合にバリデータの行動のみによって定まる報酬の係数を R、n に応じてスロット毎に確率的に機会が発生する行為による報酬の係数を W、スロット当たりの平均優先料金を P とすれば、あるエポックにおける 1 バリデータ当たりの収入の期待値は以下のようになる。

$$\frac{4R\sqrt{2n} + 32(P + 4W\sqrt{2n})}{n}\theta$$

コンピュータによる検証作業に要する電気代およびデポジットによる機会費用を含む、バリデータ i が新たな 1 エポックに滞在するための費用を α^i とし、それが法定通貨により測られるとすれば、i がそのエポックにバリデータとして留まる (あるいは新たに参入する) ための合理的条件は次の式で表せる。

$$\frac{4R\sqrt{2n} + 32(P + 4W\sqrt{2n})}{n}\theta \ \geq \alpha^i \tag{3}$$

α^i で支配的なのは 32 ETH のデポジットによる機会費用だと考えられるが、それは特に θ が減少していく局面で退出の動機 (損失を最小化したい) になりうる。左辺は n に反比例するので他のバリデータの退出は歓迎され (cf. discouragement attacks (落胆攻撃)[4])、参入のインセンティブは n が大きくなるにつれて小さくなる。退出は歓迎されるといっても、θ が減少する局面では、残るバリデータにとって滞在のインセンティブが大きくなるとは限らない。このことから、ブロックチェーンの事実上の停止を狙った外からの落胆攻撃、すなわちバリデータの利益を損なわせることによりその退出を促す攻撃の余地がある。

ETH 総量の変化　以上の表記にもとづけば、エポック e では基本料金の総和分の ETH である、

$$\sum_{s=1}^{32} f_h \sum_{x \in X_h} x.g$$

(ただし単純化のため $h = F_B(e, s)$ であるすべての h について $h \neq \perp$ とする) が消滅する。

あるエポックにおいて全バリデータが取得しうる収入の合計は、1 バリデータ当たりの収入の期待値を n 倍したものである。そのうち P に関わる量は、トランザクションを投入するユーザから既存の ETH をブロックを提案したバリデータに移転するものなので省くとすれば、エポック e に

おける ETH 総量の増量 (または減量) Δ_e は

$$\Delta_e = 4\sqrt{2n}(R + 32W) - \sum_{s=1}^{32} f_h \sum_{x \in X_h} x.g \tag{4}$$

となる。

Ethereum コミュニティ (あるいはいわゆるクリプト界隈全般) では、貨幣の希少性とインフレの関係に対するナイーブな理解が広く受け容れられているため、Δ_e が正である場合、ETH の保持者はその価値が希釈されたと考えうる。

右辺の第 1 項は $\sqrt{n}$ の形になっており、n の増加に対して増加率を逓減しながら ETH 総量を増加させる方向に作用するため、コミュニティは n の過剰な増加を歓迎しない。また、n が過剰に減少することは θ の減少と関連づけられるのでやはり歓迎しない。

gas の基本料金（右辺の第 2 項）の増加は、ETH の消却の増加ひいては ETH 総量の減少に繋がり得るためコミュニティは歓迎する。しかし、基本料金の増加が基本料金の単価の上昇によるものである場合[24]には、それはブロックが混雑し、$x.u$ の利益が損なわれることを意味する (インセンティブのミスマッチ)。

レイヤー 2 の利用は $x.u$ の利益を増加させる。しかし、gas 価格の低下に見合う利用の十分な増加を伴わなければ θ が減少する可能性があるほか、ブロックの混雑緩和により、基本料金の単価が低下し、基本料金を原資とした ETH の消却の減少ひいては ETH 総量の増加に繋がり得るとすれば、コミュニティは ETH の価値が希釈されたと考えて歓迎しない (インセンティブのミスマッチ)。

3.4 Ethereum PoS の停止の可能性

第 3.2節で論じ、第 3.3節のモデル化で確認したように、Ethereum PoS にもバリデータとユーザの間のインセンティブのミスマッチの構造は引き継がれている。Ethereum PoS においても、ブロックチェーンの維持に関わるバリデータたちにとっては ETH の獲得とその価格の上昇がインセンティブである。一方、ユーザにとってはトランザクションの実行に必要な gas 使用料を ETH で支払わなければならない以上、ETH の価格上昇は Ethereum に参加するインセンティブを減退させる。そして、Ethereum のほかにも実行基盤が登場している現状にあっては、ユーザが競合する他

[24] f_h は $\sum_{x \in X_{h-1}} x.g$ による正のフィードバックを受けるのだから、G が大きくならない限りはそのような場合だと言える。

の実行基盤に乗り換えることが現実の選択肢として存在する。すなわち、Ethereum PoS においても、バリデータとユーザ間のインセンティブのミスマッチが引き続き存在していることや、Ethereum がほぼ唯一の実行基盤であった状況からより競争的な状況に環境が変化していることを勘案すれば、PoS への移行により Ethereum がより安定的あるいは安全になったとは必ずしも言えないと考えられる。

さらに、Ethereum PoW において、ETH の価格の低下や暴落が Ethereum への信用の喪失やブロックチェーンの停止を引き起こすリスクがあったことが、PoS への移行によって変わったのかどうかということである。前述のとおり、Ethereum PoS においても、ブロックチェーンの維持に関わるバリデータたちにとっては ETH の獲得とその価格の上昇がインセンティブである。したがって、価格が上昇すれば参入が起き、下降すれば退出が起きる。ただ、Ethereum PoS では、得られる報酬の期待値がデポジット総額の平方根に反比例すること、また、一定期間中に参入・退出できるバリデータの数を制限することをもって、急激な参入・退出を抑制しようとしていると考えられる。

また、PoW においては、ETH の価格が下降する局面ではマイニングのハードウェアの電源を切ってコストを抑制する判断ができた。しかし、PoS においてはオフラインになることのペナルティがあるため、電源を切ることによる退出に逆にコストが発生する。このことにより、Ethereum PoS は PoW よりも退出を抑止する機構として優れているというのが、設計者を含む Ethereum コミュニティの見方だろう。

しかし、このような退出抑止策が講じられているにも拘らず、例えば、PoS のバリデータの権利を他者に売って退出するという「抜け道」も考えられる。買い手さへ見つけられれば、秘密鍵を売るだけで権利譲渡、すなわち撤退することができてしまう。このような売買は、単にバリデータの主体をすげ替えるだけであるので、Ethereum に閉じて考えるのであれば、ETH の価格や信用に影響しないように見える。しかし、Ethereum の価値を棄損したい勢力があるならば話は別である。バリデータの権利を買い取った上で、敢えてバリデータの責務を果たさない (バリデータ用のコンピュータ端末をオフラインにしてしまう) ことで、最悪の場合、Ethereum を停止に追い込むことができる。

ひとたび ETH の価格が暴落すれば、バリデータがオフラインになる (責務を果たさない) ことに対するペナルティのコストも小さくなるので、一般のバリデータが単純に電源を切って退出する選択も現実的となる。スラッシングによる退出と異なり、ETH の価格下降によるバリデータのオフライン化は、マジョリティとマイノリティ、どちらのバリデータに対しても等しく起きうるので、デポジット総額の $\frac{1}{3}$ を超えるバリデータがオフ

ラインとなる可能性が高まり、確定が起きづらくなる。Ethereum は基盤としての信用を損ない、そのことは ETH の価格の更なる下降を引き起こしうる (負のスパイラルが起きうる)。

これらのことから、Ethereum PoS においても ETH の価格下降や暴落は Ethereum への信用の喪失やブロックチェーンの停止を引き起こしうるし、それが起きることを抑制する機構が PoW に比較して強いとは一概に言えない。

4 議論

4.1 ETH 総量の安定と通貨的価値の安定について

Ethereum PoS について気がかりなのは、式 (4) に関する議論でも簡単に述べたが、トランザクション実行の基本料金を消却するといった点において、ETH の供給の量的安定が通貨価値の安定につながるという誤解がルールの中に入り込んでいるように思われるところである。しかし、暗号資産における単純な共有量の固定は、その市場価格の安定どころか不安定をもたらすはずだと私たちはすでに指摘していたが [16]、その懸念は、bitcoin を含む多くの暗号資産のその後の極めて不安定な値動きによって現実のものとなっている。

もっとも、ETH は bitcoin とは違う。bitcoin は、投機の対象として使う以外は、決済手段としてしか使い道がなく、したがって bitcoin の市場価格が刻一刻と把握できれば、その価値に安定性がなくても決済用の通貨として最低限の raison d'être はあると言えるのに対し、Ethereum は、いわゆるスマートコントラクトという名で契約の執行基盤としての役割をも果たすべくデザインされているので、そこで契約の表示と履行の単位すなわち価値尺度となる ETH に とって、その通貨的価値における安定性（予見可能性）の重要さは bitcoin よりもはるかに大きいもののはずである。bitcoin の場合は、通貨的価値の不安定性（予見困難性）そのものが投機対象としての魅力の一部になっている面すらあると言えるが、ETH においては、その通貨的価値形成における不安定は、現在の世界で多くの契約の表示と執行を担っているドルやユーロあるいは円などの法貨に比して、契約の価値尺度としての raison d'être において決定的な劣後要因の一つとなっていると私たちは考えている。現在までの ETH への需要には、Ethereum 上のスマートコントラクトの決済手段および価値尺度としての需要ばかりでなく、その投機的な値動きを狙った需要も少なからず含まれているように思われるが、もし PoS に移行した Ethereum が、その raison d'être の軸足を、PoW が作り出す投機性からスマートコントラクトの基盤性へと移そうと志向しているのならば、ETH の供給の量的安定

が通貨価値の安定につながるというかかる誤解は、Ethereum の今後の発展を阻害する要因になり得るのではないだろうか。

そして ETH については、価値の拠り所をスマートコントラクトの執行基盤としてのサービスの効用に素直に求めた方が、通貨としての価値の安定に結びつくばかりでなく、スマートコントラクト執行基盤としての効率性にも寄与するのではないだろうか。

4.2 独占と競争

筆者らが懸念するのは、今回の PoS への移行を企画・実行するに際して、Ethereum が、これまでのところ、いわゆるスマートコントラクトの標準的な執行基盤として、ほぼ独占的ともいえる地位をすでに獲得していること、しかし競合する他の実行基盤が登場してきたことによって、そうした地位を脅かしうる競争的な環境にシフトする可能性が否定できなくなってきていることをどれほど深く認識していたのだろうかという点である。

今回の PoS において ETH をデポジットすることがバリデータとして参加することの条件になっているのは、暗号資産としての ETH を保有していることは ETH の価値を保つことの自然なインセンティブとなるはずだという発想によるものであろう。筆者らはそうした認識自体に異を唱えるつもりはない。だが、注意すべきは暗号資産としての ETH を現に保有している主体であっても、彼らの ETH 建て契約者としての状況によっては、ETH の価値を維持するどころか、その価値を崩壊させることにインセンティブを持ちうるということである。

どんなときに、そんなことが起こるのだろうか。答は簡単である。バリデータたちが ETH 建ての契約における債権者ではなく債務者だったら、ETH の実質価値の低下は彼らの利益になってしまうからである。だから、もしバリデータの大半が、ETH 建ての債務を保有する一方、1) 他の通貨建て債権や株式や不動産などの実質資産を保有するというバランスシートを有しているならば、あるいは、2) 競合する他の実行基盤により深くコミットしているような主体であるならば、そうしたバリデータのグループは、全体として ETH の価値を維持するのではなく棄損することに、より大きなインセンティブを持つことになりかねない。(前者の場合も、競合する他の実行基盤があって、かつ当該基盤への乗り換えが容易にできるのであれば、Ethereum を停止に追い込んだとしても、ユーザからさほど批判されることはないかもしれない。) ちなみに、他者から 32ETH を借り入れて ETH のバリデータになれば、上述のようなポジションは容易に作ることができる。

とはいえ、そうしたETH価値棄損インセンティブがバリデータのグループの行動にあからさまに現れるとは限らない。バリデータによるETH価値棄損行動は、棄損行動をとる者にとって短期的には利益にはなっても、より長期的には彼らの利益にならない可能性もあるからだ。だが、不幸な偶然あるいは悪意によりバリデータの大半がETH建て過剰債務者に占められるという事態を、今回のPoSルールが排除できていないのは、いわゆるスマートコントラクト執行基盤としてETH建ての債権債務取引の発展を支えようという現在のEthereumの方向性と根本的に矛盾するのではないかと筆者たちは懸念するものである。

もちろん、バリデータにおける意図的な価値棄損問題は、PoWでも起こりうる。ただ、bitcoinをはじめとする多くの暗号資産は、現状ではあまりにも価値変動が激しく、結果として投機の対象にはなっても、貨幣論でいう価値尺度として契約関係を支える役割を果たせていなかったことが、その背景にあったことを私たちは見過ごすべきでないだろう。BTCにおいて議論され続けてきた いわゆる51%攻撃が現実には これまで起こらなかった理由の一つは、PoWにもとづく暗号資産であるBTCにおけるターゲット調整アルゴリズムの不備がもたらした価格不安定という「欠陥」が作り出した一種の幸運であるにすぎないのだ [17]。

では、通貨の価値管理者における自通貨価値棄損インセンティブを断つ方法はあるのだろうか。

その第一の方法は、通貨の価値管理者として振る舞う者についての適格基準を厳しくして、何らかの「公」の管理下に置くことである。法定通貨の世界において「中央銀行の独立性」が求められるのは、中央銀行の設置者である政府は、多くの場合、法定通貨建ての債務の巨額保有者であり、少なくとも短期的には自国通貨価値棄損すなわちインフレ誘導へのインセンティブを持ちがちだという認識がその根底にあると考えられる。

そして第二の方法は通貨価値管理者における「競争」である。あのフリードリヒ・A・ハイエクが展開した競争的貨幣発行論は、どの通貨を使うかという「選択」を法によって強制するのではなく各人の自由に委ねれば、少なくとも長期的には通貨価値維持のインセンティブが棄損のインセンティブに優越するだろうというものだったが、彼の議論の正しさは固定相場制崩壊後の中央銀行間の貨幣価値維持競争がもたらした世界的なインフレ終息というかたちで、少なくとも間接的には試されたと筆者たちは考えている。その経験に学べば、さまざまなスマートコントラクト執行基盤の制度間競争こそが望ましい未来なのではないだろうか。

4.3　スマートコントラクト実行基盤の乗り換えは現実的か

コンピュータソフトウェアが持つネットワーク外部性は、自由な競争が

行われる上での障壁となる。 第 3.3節の中で、Ethereum の外部経済効果 $\mathcal{EC}^{x.u}_{x_{E/l}}$ を 0 と仮定して議論を進めたことは妥当だったのだろうか。 特に、代替性をもつファンジブルトークン同士をあるレートに基づいて交換するといったスマートコントラクト (e.g. DEX: Decentralized Exchange) に対しては、ネットワーク外部性が大きく作用すると考えられる。しかし、本論文でもたびたび指摘しているように、代替性を持たない NFT 等に関してはその限りではない。

過去のものとは独立して新規にスマートコントラクトをデプロイする場合、乗り換えは問題にならない。スマートコントラクトをアップグレードする場合も、Ethereum では一度デプロイしたものは (無効化は可能でも) 変更できないので、新規にデプロイし直すことが行われている。この場合も乗り換えは問題になりにくい。

新コントラクトが旧コントラクトからデータを引き継ぐ場合はより困難になるが、手法は例えば [26] にて提案されている。また、Ethereum レイヤー 1 の場合、すべてのトランザクションは記録されているのだから、最新の状態をオフラインで再現することは難しくない (正しく再現できているかどうかも第三者が検証できる)。それを移行先の基盤に移植しなければならないが、Ethereum からの移行を商機ととらえる基盤があるのなら、そのことを低コストで行うための機構を用意するだろう。乗り換えをサービス化する業者も現れるかもしれない。

4.4 乗り換えの要因

Gas 使用料の高低だけが乗り換えの要因ではなく、Ethereum が安定性に欠くと観測されれば乗り換えは起きうる。例として、第 3.4節に示したように、競合他者による攻撃を受けることで安定性が損なわれることがありうる。

また、デポジット総額の $\frac{1}{3}$ 超の ETH を長期的に制御下に置く (確定が起きないように証言するあるいは証言を怠ると退出させられるので、継続的にデポジットしていく必要がある) コストに比較して、より大きな価値が Ethereum のスマートコントラクト上に載っているとすれば、第 4.2節でもすでに議論しているように、それを無効にすることで利益を得たり負債を解消できる主体には、チェックポイントの確定を食い止め続けるような攻撃をすることで Ethereum を停止させることに合理的な動機が生じうる。

5 結論

この論文では、Ethereum の持続性の議論に ETH の価格水準およびスマートコントラクト実行基盤間の競争という視点を持ち込み、ETH の価格が下落するような局面では Ethereum PoS が持続できない場合があることを描き出した。

Ethereum PoS に対する様々な攻撃の可能性を論じた論考に [7] がある。そこでは、PoS の安全性は善意の参加者がデポジット額ベースでマジョリティであることに依存しているので、その条件が崩れた場合には技術的には攻撃を防ぐことはできず、最終的には善意のコミュニティの力により悪意の参加者を排除する必要があると述べられている。しかし、この論考には ETH の価格水準への言及がない。ETH が下落する状況下で、善意のコミュニティの力は期待できるだろうか。

基盤が信頼を損ない、アプリケーションが実行できなくなるような事態を引き起こす要因にインセンティブのミスマッチがある。アプリケーションを開発し動かすユーザにとってのインセンティブと、基盤を維持する者らにとってのインセンティブとが整合するような、新たなスマートコントラクト基盤の設計が待たれる。

この論文で行った問題提起が、広く適用され始めている Proof of Stake の設計の見直しや、新たなスマートコントラクト基盤の設計に繋がるとしたら幸いである。

謝辞

この研究は、科研費 基盤研究 (A) 「ブロックチェーンを持続可能にする数理的・実験的研究」により支援されています。(This work was supported by JSPS KAKENHI Grant Number JP21H04872.)

参考文献

[1] Dan Boneh, Ben Lynn, and Hovav Shacham. Short Signatures from the Weil Pairing. Journal of Cryptology, 17(4):297–319, 2004.

[2] Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform, 2013. https://ethereum.org/en/whitepaper/.

[3] Vitalik Buterin. DAOs, DACs, DAs and More: An Incomplete Terminology Guide, 2014.

https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/.

[4] Vitalik Buterin. Discouragement Attacks, 2018. https://github.com/ethereum/research/blob/master/papers/discouragement/discouragement.pdf.

[5] Vitalik Buterin, Eric Conner, Rick Dudley, Matthew Slipper, Ian Norden, and Abdelhamid Bakhta. Fee market change for ETH 1.0 chain, 2019. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1559.md.

[6] Vitalik Buterin, Diego Hernandez, Thor Kamphefner, Khiem Pham, Zhi Qiao, Danny Ryan, Juhyeok Sin, Ying Wang, and Yan X Zhang. Combining GHOST and Casper, 2020. https://arxiv.org/abs/2003.03052.

[7] Joseph Cook. Ethereum PoS Attack and Defense, 2022. https://mirror.xyz/jmcook.eth/YqHargbVWVNRQqQpVpzrqEQ8IqwNUJDIpwRP7SS5FXs.

[8] Ben Edgington. Upgrading Ethereum Edition 0.3: Capella [WIP], 2023. https://eth2book.info/capella/.

[9] William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs. Non-Fungible Token Standard, 2018. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md.

[10] ethereum.org. GAS AND FEES, 2022. https://ethereum.org/ja/developers/docs/gas/.

[11] ethereum.org. PROOF-OF-STAKE (POS), 2022. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[12] ethereum.org. PROOF-OF-STAKE REWARDS AND PENALTIES, 2022. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/rewards-and-penalties/.

[13] ethereum.org. Validator FAQs, 2022. https://launchpad.ethereum.org/en/faq.

[14] ethereum.org. ZERO-KNOWLEDGE ROLLUPS, 2023. https://ethereum.org/ja/developers/docs/scaling/zk-rollups/.

[15] Juan Ignacio Ibañez and Alexander Freier. Bitcoin's Carbon Footprint Revisited: Proof of Work Mining for Renewable Energy Expansion, 2023. https://arxiv.org/abs/2304.04578.

[16] Mitsuru Iwamura, Yukinobu Kitamura, Tsutomu Matsumoto, and Kenji Saito. Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money. Discussion Paper Series A No.617, Institute of Economic Research, Hitotsubashi University, 2014. (Earlier version of [17]).

[17] Mitsuru Iwamura, Yukinobu Kitamura, Tsutomu Matsumoto, and Kenji Saito. Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money. Hitotsubashi Journal of Economics, 60(1), June 2019.

[18] Leslie Lamport. The Part-time Parliament. ACM Transactions on Computer Systems (TOCS), 16(2):133–169, May 1998.

[19] Loopring Project Ltd. Loopring – zkRollup Layer2 for Trading and Payment, as of 2023. https://loopring.org/.

[20] Jim McDonald. Understanding Validator Effective Balance, 2019. https://www.attestant.io/posts/understanding-validator-effective-balance/.

[21] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. http://bitcoin.org/bitcoin.pdf.

[22] Ozone Networks, Inc. OpenSea, the largest NFT marketplace, as of 2023. https://opensea.io/.

[23] Polygon Labs UI (Cayman) Ltd. Blockchains for mass adoption, as of 2023. https://www.polygon.technology/.

[24] Kenji Saito and Mitsuru Iwamura. How to make a digital currency on a blockchain stable. Future Generation Computer Systems, 100:58–69, 2019.

[25] Fred B. Schneider. Implementing Fault-Tolerant Services Using the State Machine Approach: A Tutorial. ACM Computing Surveys, 22(4):299–319, 1990.

[26] Kazuyuki Shudo, Reiki Kanda, and Kenji Saito. Towards Application Portability on Blockchains. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), pages 51–55, 2018.

[27] Gavin Wood. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER, 2015. https://ethereum.github.io/yellowpaper/paper.pdf.