暗号資産のトランザクション履歴を用いた合意アルゴリズム[*1]

古味佑樹，立川崇之
高知工業高等専門学校

概要

暗号資産におけるブロックチェーンのコンセンサスアルゴリズムでは，Proof of Work や Proof of Stake が用いられている．ところが現行のアルゴリズムでは莫大な電力消費や平等性などの問題が存在する．我々はトランザクション履歴を用いた，新たなコンセンサスアルゴリズムを考案した．過去の取引記録からランダムに承認の投票権を与えることで，平等性を確保する．また，発行量を調整する仕組みを取り込み，価値の安定性も測ることができると考えられる．

1 Introduction

Satoshi Nakamoto [1] により提案された P2P の電子マネーシステムは，様々な暗号資産のシステムに応用されている．オンライン決済における二重使用問題を，信用のおける第三者機関の認証を必要とせずに実現できるようにするため，ブロックチェーンの仕組みが提案された．ブロックチェーンはデータの破壊，改ざんが極めて困難であるため，取引の信用を維持できる

Bitcoin をはじめとする暗号資産でのブロックチェーンでは，継続的なプルーフ・オブ・ワーク (PoW) を実現するために，時系列準のハッシュチェーンによる共有台帳を保有する．改ざん防止と不可逆性の実現のためにハッシュチェーンの仕組みは非常に有用であるが，参加者は各々のノードで特定のハッシュ値が現れるまで演算を繰り返し，目的のハッシュを見つけたノードがチェーンに新しいブロックを追加することができる．ところでこのハッシュ値の計算は莫大な計算処理を必要とする．また，ハッシュ値の計算に対するインセンティブを与えることから，ハッシュ値の計算を目的とした大規模な計算資源が使用され，莫大な電力を消費していると問題視されている [2].

PoW に代わる方法として，プルーフ・オブ・ステーク (PoS) と名付けられた，新たなアルゴリズムが提唱されている．この仕組みでは例えば，ユーザが暗号資産のトークンをどれだけの時間保有したかという「コイン年齢」に基づいて，Stake としている [3]．Ethereum では，2022 年 9 月に PoW から PoS への移行を行い，エネルギー消費を約 99.95% 削減できるとしている [4]．しかしながら PoS では暗号資産の流通量が下がるという懸案がある．

本論文では，PoW のように莫大な計算資源を必要とせず，従来の PoS のように流通量を下げない，暗号資産に関する新たなコンセンサスアルゴリズムを提案する．本アルゴリズムはトランザクション履歴に基づいている．ユーザは過去に暗号資産を所有していたが，何らかの取引により手放しているとする．この取引行為を暗号資産の振興に寄与したとみなし，ユーザにブロックの署名者になる権利，すなわち新しいブロックを追加

[*1] 本論文は，
”Consensus Algorithm Using Transaction History for Cryptocurrency”
Yuuki Komi and Takayuki Tatekawa
高知高専学術紀要第 68 号, pp.29-35 (2023.3)
Cryptology ePrint Archive Paper 2023/373
の日本語訳である．

する権利を与える．別の言葉で言い換えると，PoW のハッシュ値の計算に代わり，取引を行うことでインセンティブとする．

暗号資産においては，ブロックを追加するユーザに対し，新しいブロックを追加する際のインセンティブの他に，取引手数料も与えられる．取引手数料を適切に調整することで，大量の自己取引を行ってもユーザが得をしないようにすることで，暗号資産の適切な運用が出来ると期待できる．

本論文は以下のように構成されている．2 章で新たなプロトコルを提案する．3 章では，新たなプロトコルによる発行量の調整について述べる．最後に 4 章で本研究を総括する．

2 新たなプロトコルの提案

2.1 トランザクション履歴

暗号資産であるコインを支払いに使うには, そのコインを誰かから受け取る必要がある．そしてそのトランザクションがチェーンに記録されることは, 誰かが誰かにコインを支払ったという証明になる．暗号資産のコインの価値は, その流動性に拠ってのみ成り立つと考えられるため，取引を行える集団を大きくすることが必須である．

トランザクション履歴とは, あるコインがどのような取引を経てきたかという記録である．ブロックチェーンでは取引情報をブロックに記録していく．その際にどのトランザクションからも参照されていない通貨を Unspent Transaction Output (UTXO) とみなす．新たなトランザクションが発生した時，取引に必要な UTXO を見つけて清算することで、トランザクションが成立する。

2.2 チェックポイント・システム

我々が提案するプロトコルでは,「取引を行ったこと」に対し，分岐しているブロックチェーンのツリーからただ一つのブロックチェーンを選ぶ権利を与える．取引に基づく権限の付与により，参加者による暗号資産の利用範囲の拡大が期待できる．本プロトコルは PoW とハイブリッドに使われる事を想定されたものである．PoW システムは以下の目的のため使用される．

- ブロックチェーンの不可逆性の保証
- 前のブロックの検証
- ブロックの生成に対する多少の経済的リスク負担

PoW はステーキングを用いた完全な PoS によるマイニングでの代替も可能である．

本プロトコルは, チェックポイント・システムによる一定期間ごとの投票と, 投票者の選出に楕円曲線上の離散対数問題を用いることで，シビル攻撃への耐性を持たせている．本プロトコルでは，Bitcoin で用いられている secp256k1 [5] の適用を想定している．

我々のプロトコルで用いているチェックポイントツリーは, Ethereum 財団によって提案された PoS 方式の一種である Casper FFG [6] で使われている方式である．チェックポイントツリーは，チェーンの正統性を考える上でブロックツリー全体を扱わないように効率化するものである．定期的な高さごとにチェックポイントを設け, フォークしたチェーンから唯一の正当なチェーンを決められるようにする．

図 1 で示すように，チェックポイントは, ブロックツリーの高さ（またはブロック番号）が 100 の倍数であるすべてのブロック，もしくは高さ 0 のジェネシスブロックである．ブロックの番号が 100k であるブロック

の「チェックポイントの高さ」は k である．チェックポイント c の高さ $h(c)$ は，親リンクに沿って c からルートまで延びるチェックポイントチェーンの要素数で与えられる．

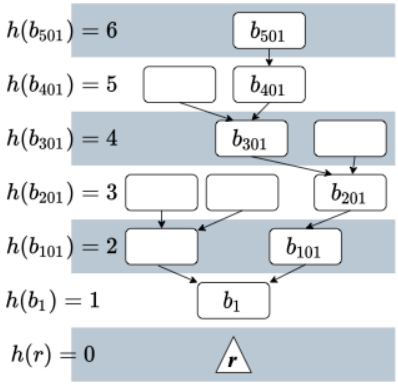

図 1　チェックポイント・ツリーと高さ

高さ n のチェックポイントにおけるブロックに合意がなされれば，その時点までの正統なチェーンが定まる．FFG は PoS のプロトコルであるため, Etherium の場合にはチェックポイント毎に 1 票への対価として 1ETH を課す，経済的リスクを負ったバリデーターによる投票が行われる．正当なバリデーターの 2/3 以上の投票が得られた場合に高さ n のチェックポイントは正当化される．そして，高さ $n+1$ のチェックポイントのブロックが正当化されることで，高さ n のブロックが確定する（図 2）．チェックポイント a からチェックポイント b にツリーが延びているとき，$a \rightarrow b$ と表す．

この仕組みは, 確定されたチェックポイントは覆されないという特性をもたせることで，過去になされた取引が否定されないことが重要である．

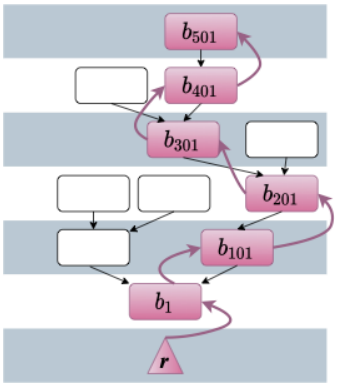

図 2　チェックポイントのブロック数とチェックポイントの高さ．下向きの矢印の間には，99 個のブロックが存在する．上向きの矢印は正当化される順序を表す．

2.3　検証者の選出

検証者の選出は, 表 1 に示す要素でなされる．

これらの要素は全てチェックポイント a から一意に計算することが可能である．トランザクション t ではまだ正当化されていない $a \rightarrow b$ 間のブロックが参照されるのを防ぐため, ブロックの添字に 100 が加算され

表 1　検証者の選出に用いられる要素

Notation	Description
hash(a)	チェックポイント a におけるブロック B_{n-100} のハッシュ値
P	hash(a) を秘密鍵 e でスカラー倍した公開鍵
S	P を 16 bit ごとに分割した値の集合
i	S に含まれる各要素
t	ブロック $B_{n-(i+100)}$ に記録されているトランザクション

ている．検証者の重複を防ぐため，i が重複した場合には，加算や論理演算で重複を回避する．検証者は t により決定される．

このようにして検証者を恣意的に選択できないようにする．チェックポイントでの投票で不正がなされた時, 該当する UTXO を使用不可能にする懲罰的な仕組みを導入するため，t における output が未使用である必要がある．

2.4　検証者の戦略

あるチェックポイントで選出された検証者達が，正当に検証を行うようにするために，検証を行うインセンティブを与えることを考える．そして検証者が不正を行わないようにする．検証者が正当な検証を行うことは，以下のルールで実現できる．ここではチェーンは $c \to c' \to c''$ と伸びていくこととする．

- 検証者は投票を示すメッセージに，投票権を得た UTXO が自身のものであることを証明しなければならない.
- 投票を示すメッセージに含まれた UTXO は使用済とされ，UTXO セットから取り除かれる．
- もしあるノードにおいて，不正を発見し, その不正があったブランチに投票が行われていた場合には，不正の発見者は投票されていた UTXO を受け取ることができる．不正の検証は，検証者以外でも行える．
- また不正を発見したものは、投票者の UTXO を input としてトランザクションを作成する権利を持つことになる．つまり，仕組み上は投票権を得た UTXO を input にしたトランザクションは誰でも発行可能である．その上で，不正の証明以外での使用をできない　ようにする．
- 前項の方法では投票者が損をすることになるため、c が確定してからいくつかのチェックポイントが確定するまでに、UTXO をそのまま自身に向けて input するようなトランザクションを発行できるようにする．
- 正しい投票を行った検証者は，報酬として c' から c'' までのブロックにおいて，トランザクション手数料の半額を得る特別な署名を行うことができる．
- 投票数が最も多いチェックポイントが正当化される．

もし検証者が不正を行うには，検証者を選択するトランザクション集合の中で，自身のトランザクションが最大数になる必要がある．

2.5 シビル攻撃への耐性

シビル攻撃とは，攻撃者が複数のノード，アカウント，計算機を使用して，ネットワークシステムを支配しようとする攻撃である．本提案のアルゴリズムはシビル攻撃に対して以下の方法で対処している．

まず，ブロックの生成には PoW を用いており，ブロックを作成すること自体が参加者にとって大きな負担になることを保証している．このために，大量のブロックを作成した攻撃を防止できる．次に，投票者の選出は参加者から操作不能な値で選ばれており，投票者は他者との利害関係を想定できない，このため，組織投票を防止できる．投票者に選ばれる可能性を上げるには，大量のトランザクションを発行する必要がある．ところが取引に手数料が必要となるため，大量のトランザクションの発行を行うと，大量の手数料を要求される．このため，作為的に投票者になるためのトランザクション発行を防止できる．

定量的にシビル攻撃が困難であることを説明する．あるトランザクションを行った者が検証者になる可能性を持つのは，そのトランザクションを含むブロックが確定してから，$2^{16}(= 65536)$ 個のブロックが採掘されるまでである．もし 1 つのブロックが採掘されるまでの平均目標時間が 15 秒であるとすると，トランザクションが行われたブロックにより検証者が確定するのは約 273 時間後である．その間に生じたチェックポイントが 655 回になり，起点と終点の 2 つのチェックポイントを除く 653 回で投票権が得られる可能性がある．もしシビル攻撃を行うには，トランザクションが行われてから検証者が確定するまでの約 273 時間の間に，攻撃者は過半数のトランザクションを発生させなければならない．以上の理由から，シビル攻撃は困難であるといえる．

3 発行量の調整

暗号資産を実取引に使用するためには．法定通貨との交換レートが安定していることが非常に重要である．暗号資産を法定通貨などに裏付けされることで，法定通貨との交換レートの変動が極めて小さくなるようにする，Stablecoin が考えられている．本提案では法定通貨などの裏付けなしに，法定通貨との交換レートの変動を抑えるための仕組みを考える．

PoW において取引の承認を行い，信任を行っているのは膨大な計算処理を行っている miner である．ところが暗号資産の価値が認められ，miner の数が増えても，miner が得られる暗号資産の量は減っていく．miner の数を維持するためには，暗号資産の単位当たりの価値を際限なく上昇させてしまう．さらに PoW ではコインを減らすことが出来ず，マネーサプライの調整に相当する行為がなされない．

経済学において取引と貨幣量の関係は，”Equation of exchange” と名付けられた以下の式で表される [7].

$$MV = PT\,, \tag{1}$$

ここで M は全貨幣量，V は貨幣の取引流通速度，P は物価，T は一定期間における財やサービスの取引量を表す．この方程式を含めた経済学の法則を， Bitcoin と米ドルとの交換レートに適用した先行研究がなされており，交換レートの変動が法則によく合うことが示されている [8].

さて，PoW における難易度は，ブロックを追加するための時間と，前のブロックでどれだけの計算量を必要としたかで決定される．もし前のブロックで大量の計算がなされたとすると，PoW の難易度は上昇する．

ところで暗号資産の正確な取引量を測定することには，一般に困難が生じる．取引記録の全てがブロックチェーンに記録されており誰でも閲覧可能だが，同一人物が複数のアカウントを所有し，自己取引を繰り返し

た場合には，実際の取引よりもはるかに多い取引がなされたようになってしまう．

もし取引に手数料がかかるようにすると，大量の自己取引を防ぐことができる．2.5 章で述べたように，トランザクションを発生されてから検証者が確定するまでに約 273 時間かかる．検証者確定に既に用いられた暗号資産のコインは「正しいコイン」といえる．「正しいコイン」を調べることで，検証がなされた取引数を表すことができる．

PoW の難易度を考えると，”Equation of Exchange” は，過去の流通速度 V_O，取引額 P_O，取引数 T_O に応じて以下のように修正されると考えられる．

$$MV_O = P_O T_O D\,. \tag{2}$$

D は現在の PoW の難易度を示す．ここで V_O については，ブロックチェーンによる取引記録を参照すれば決定できる．P_O, T_O については直前のブロックに記録しておけば，全てのブロックを参照する必要はない．ブロックチェーンにおいて変数の値が唯一に決定され，不正な値を検知する仕組みを実装する必要がある．

過去のブロックから暗号資産の全体量を求められる．

$$M = \frac{P_O T_O D}{V_0}\,. \tag{3}$$

この M をチェックポイントごとに求める．n 番目のブロックを追加する時に $M_n > M_{n-1}$ であれば差分は PoW の追加報酬となり，そうでなければ追加報酬は発生しない．また，多くのチェックポイントで連続して追加報酬が発生しなかった場合には，検証者に支払われる手数料の 1/2 を，誰も引き出せないアドレスに送信するトランザクションを発生させる．本プロトコルではマイナーと検証者が同一になる場合は非常に稀であるため，この処置によるマイナーの減少は考えにくいと期待される．

4 Summary

本論文では，PoW，PoS に代わる，暗号資産に関する新たなコンセンサスアルゴリズムを提案した．本提案のアルゴリズムでは膨大な計算処理を必要とせず，流通量の低下の問題もないと考えられ，さらに暗号資産の発行量の調整も見込めると期待される．

提案したアルゴリズムの仕組みを例示した際に用いたパラメータは仮の値であり，最適値とは限らない．適切にコンセンサスが得られ，暗号資産として大勢の匿名の利用者により，不正が行われることなく運用されるかどうかの検証がさらに必要である．

本論文では新たなアルゴリズムを提案しているだけであり，アルゴリズムに基づいたソフトウェアの開発，実装，テストは行っていない．他の暗号資産のアルゴリズムと同様，本アルゴリズムに基づくソフトウェア開発は年単位の時間と労力を要し，またテストは大勢の協力者を必要とすると考えられる．本アルゴリズムに基づくソフトウェア開発，テストは今後の課題とする．

不正を行わない方が参加者にとって得策かどうかについては，ゲーム理論による分析が必要である．先行研究として，PoW の代わりにディスクスペースを提供する暗号資産のアルゴリズムに対し，ゲーム理論を用いて安定性と合意形成がなされることが証明されている [9]．本アルゴリズムも同様にゲーム理論による詳細な検証が必要と考えられる．

謝辞

本論文は，古味佑樹の卒業論文に基づいて新たな知見を追加し再構成したものである．卒業論文を査読していただいた榎本隆二教授，論文に有用な意見を出して下さった中山昌勲氏，濱田幸希氏，長谷川和葉氏に感謝の意を表する．また，英文校正については，エディテージ（www.editage.com）に世話になった．

参考文献

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”
`https://bitcoin.org/bitcoin.pdf`

[2] Bitcoin energy consumption index (Digiconomist).
`https://digiconomist.net/bitcoin-energy-consumption`

[3] P. Tasca and C. J. Tessone, “A Taxonomy of Blockchain Technologies: Principles of Identification and Classification”, Ledger, 4. (2019)
`https://doi.org/10.5195/ledger.2019.140`

[4] Ethereum: The Merge
https://ethereum.org/en/upgrades/merge/

[5] D. R. L. Brown. “Recommended Elliptic Curve Domain Parameters.”, Tech. rep. Certicom Research, Jan. 2010.

[6] V. Buterin and V. Griffith, “Casper the Friendly Finality Gadget”, arXiv:1710.09437.

[7] I. Fisher, “The Equation of Exchange 1896-1910”, American Economic Review 1, 296-305 (1911).

[8] L. Kristoufek, “Is the Bitcoin price dynamics economically reasonable? Evidence from fundamental laws”, Physica A, 536, 120873 (2019).

[9] S. Park *et al.*, “SpaceMint: A Cryptocurrency Based on Proofs of Space”, in International Conference on Financial Cryptography and Data Security. Springer, 480-499 (2018).