暗号資産の非中央集権化のためのProof of Work長寿命化

Extending Life of Proof of Work for Decentralization of CryptoAsset

小川健†
Takeshi OGAWA†

† 専修大学 経済学部（国際経済学科）
† School of Economics, Senshu University

要旨:

最早技術/情報系の枠を超えてその重要性と可能性が一般にも浸透を始めたブロックチェーン・分散型台帳技術であるが，その始まりともいえる Proof of Work(PoW)型暗号資産認証方式は理論的に攻撃の可能性として指摘されていながら現実的ではないとされてきた Block Withholding Attack を含む攻撃等により，モナコイン(MONA)，ヴァージ(XVG)，ビットコインゴールド(BTG)，イーサリアムクラシック(ETC)などそこそこ有名な PoW 型暗号資産を中心に 2018 年 5 月頃から攻撃が続き，巻き戻しも大掛かりに起きている．しかし，その代替策として有力視されている Proof of Stake(PoS)型暗号資産認証方式を初めとして，他の暗号資産の認証方式にもそれぞれ問題は存在する．そこで，本稿では PoW 長寿命化に向けた提言を行う．

Abstract:

This paper considers resurrecting the way of Proof of Work (PoW) as a certification way for cryptoasset. The way of proof of work is the first way of certification of blockchain for cryptoassets, so the way is used in various cryptoassets of old types. However, after Monacoin (MONA) was attacked with block withholding attack in May 2018, like Verge (XVG) and Bitcoin Gold (BTG), the way of Proof of Work cannot be felt relieved, so some of PoW types' cryptoassets are becoming changing other certification ways. However, the way of PoW is important for decentralization. Thus, this paper considers some ideas to resurrect of Proof of Work as a certification way for cryptoasset.

1. はじめに

2018(平成 30)年 5 月の MONA コイン騒動に始まる一連のブロックチェーン(BC)への攻撃は，CoinCheck の NEM 流出騒動のような旧来の暗号資産交換業者への攻撃とは異なり，51%攻撃や Block Withholding Attack (BWA)等 Proof of Work (PoW)型 BC 自体への信頼が揺らぐ攻撃が現実になった点に大きな特徴がある．その後 MONA コインは Proof of Stake (PoS)への変更を宣言した．こうした攻撃は 2019(平成 31)年 1 月の PoW 型イーサリアムクラシック(ETC)への 51%攻撃などを見ても昔の話ではない．PoW 型はある意味時代遅れ感を持ってしまった．

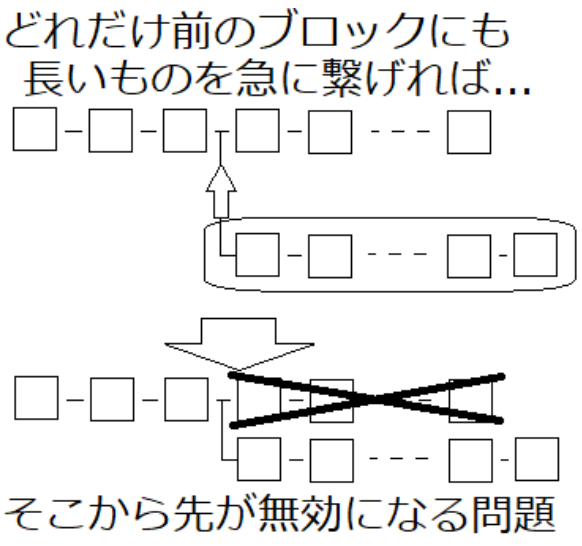
しかし，Nakamoto(2009)[1]が BC 技術の基礎を提示した際に目指した非中央集権性は，その後数多く提案された改良型でも失われる方式が多い．先の PoS やその改良版 Delegated Proof of Stake (DPoS)，更には Proof of Importance (PoI)でさえ事後的には非中央集権性が確保され難い．PBFT (Practical Byzantine Fault Tolerance)等では認証者(Validation Peer)を増やし難いため分散性に欠け，非中央集権性の鍵となるトラストレスが欠けるため，パブリック・ブロックチェーンには使い難い．分散型台帳技術でも XRP Ledger 等では誰でも認証できる訳でなく分散性も未だ乏しい．非中央集権化の上で PoW 型の役目はまだある．

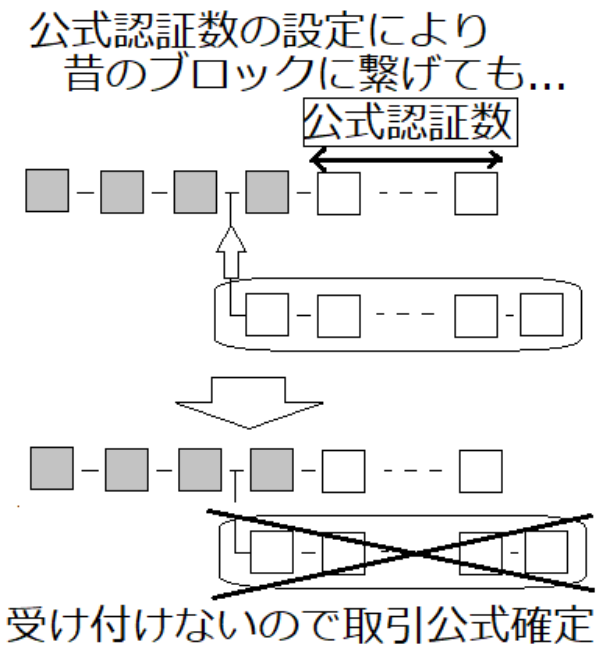
本稿では PoW 型認証方式の長寿命化への提言を行う．

2. 提案 1:公式認証数の設定と巻き戻し(ReOrg)

ブロックチェーン等の多くで分岐したら長いものを採用する仕組みを取るが，暗号資産の取引所・交換業者の多くである程度のブロック数が繋がれば多分覆らないと判断して扱う慣習がある．しかしビットコインを始めとして，長いものを後から用意しても接続できてしまう所に BWA の余地を残してしまう所がある．しかも，UASF(User Activated Soft-Fork)の際にも心配され，MONA コイン騒動で明らかになった様に，大規模な巻き戻し(ReOrg)が起きると取引の信頼性にも影響を来す．過去の取引を掘り返されて無効にされるとなるとその後の取引の信頼性にも関わるので，過去の取引の確定は非常に大事になる．

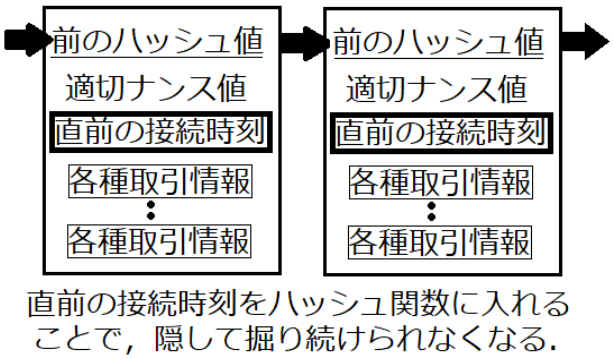
そこで提案 1 として，各種交換業者の慣例を参考に公式認証数を設定し，このブロック数だけ繋がった場合にはこれより前のブロックには繋げられなくすれば，直近数ブロックを除いて取引が確定し，大規模な巻き戻しも無くなる．





3.　提案 2:接続時刻の入力情報化と強制接続

BWA の問題点は隠して掘り続けられる点にある．これを解消するには，PBFT 等でも採用されている，直前のブロックへの接続時刻をハッシュ関数に入れる形式にすれば良く，これにより隠して掘り続けることが出来ず，強制的に 1 ブロックずつ公開接続することになる．その上で分岐後接続が続きそうな場合には警告表示を自動通知・表示可能な設定にすれば，今この取引が無効化する危険性が迫っているのか分かる．



なお，この接続時刻は情報として用いるだけなので，正確な時刻であるかどうかが重要なのではなく，時刻の情報が重要なのであり，接続時刻が正確な時刻からずれているかどうかについてはあまり重要ではない．

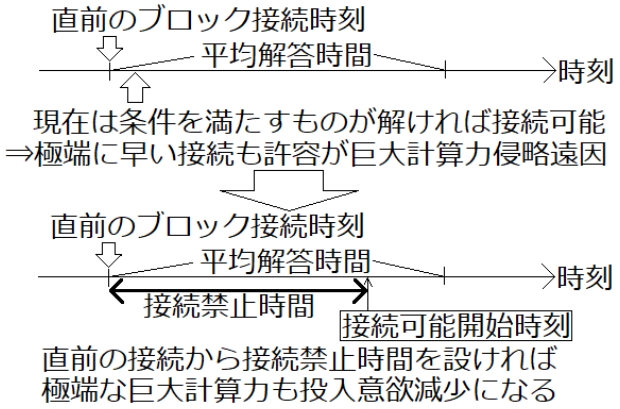
4.　提案 3:接続可能開始時刻の設定と巨大計算力

2019(平成 31)年 1 月にイーサリアム・クラシックで 51%攻撃が行われたが，寡占的な認証状況設定だけでなく，量子コンピュータの登場など革新的な技術革新によっても従来の認証コンピュータより遥かに優れた巨大計算力が突如登場することはある．これは PoW 型認証方式においては著しく脅威の元凶となり得る．この原因は前の認証を行った後，暗号が解ければ著しく速い場合でも接続を可能とする事から起きる．

大量即時処理の観点からはむしろ望ましい面ではある．しかし，安全性という観点を考えた際，ここが 51%攻撃や BWA 等の元凶の可能性がある．各 PoW 型暗号資産は難易度設定に際し平均解答時間を設定しているわけであり，それを著しく縮める事例も無くはないものの，その多くは何か事が起きている可能性も否めない．

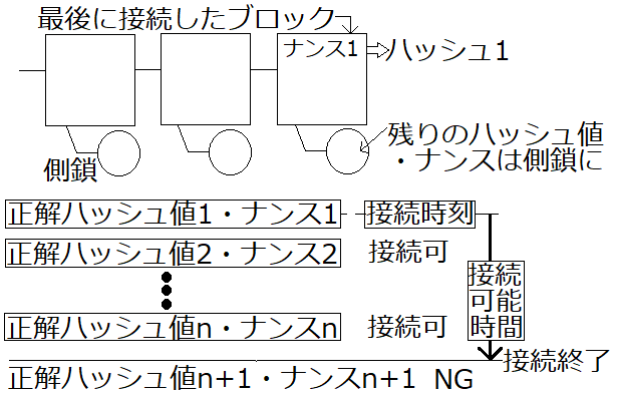
小テスト等での解答時間を例に考えてみよう．10 分用の解答時間の問題を例えば 5 秒で解いたとなれば，通常はまともなことが起きていない．その多くでは不正が起きたか，問題設定にミスがあったか，何か緊急事態が起きていることは容易に想像できる．PoW 型も本来は同じである．

そこで平均解答時間を基に一定割合を決めておいて，接続開始可能時刻をその都度設定することで，巨大計算力があっという間に解いたから直ちに，という形でなくなる．そのため，巨大計算力の投入意欲が削がれる．



5.　提案 4:異なる組み合わせによる複数報酬制

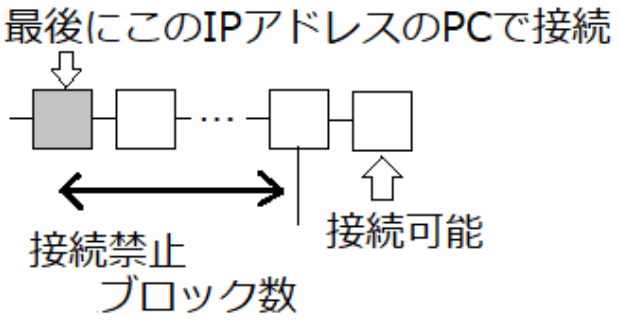
現在の PoW 型の多くが最初の接続者のみの報酬となっている．しかし，条件を満たすハッシュ値と対応するナンス値との関係は一意とは限らない．そこで，最初の接続時刻から接続可能期間を設け，同じ取引情報の組み合わせにも関わらず条件を満たしながらも各々異なるハッシュ値と対応するナンス値で異なる IP アドレスから最初に接続申請した場合には，序列を付けての複数接続者による報酬の案分を設定する．こうすることで，巨大計算力を投入しても割に合わなくなるので，巨大計算力の投入意欲が削がれる反面，組み合わせが異なれば報酬を得られるので，想定計算力を持つ色々な小規模母体でも報酬を少しずつ得られる形となり，分散化が進み易い．前のハッシュ値は最初の接続のものを扱い，他の組み合わせは側鎖に入れる．



なお，あまりに巨大な計算力の場合にはその答えとなる組み合わせを数多く見つけてしまう可能性は理論的にはあるが，案分されることからそこまでのインセンティブは働きにくい．つまり巨大計算力の突如投入意欲を削ぐのである．

6. 提案5: 同一IPアドレスで接続可能なブロック数設定

更に，巨大計算力による占有を防ぐため，形式的に 1 つの IP アドレスで 1 度接続が成功した場合，次に接続可能になるブロック数を決めておく．こうすることで，巨大計算力単体による占有を防げる．この設定は決して本質的な解決を招かないが，別 PC を経由する時間が必要になるだけに，先着争いではこの条件は死活問題となる．その結果，巨大計算力の突如投入意欲を削ぐことができる．



7. 補足：非中央集権性は無駄な視点か

ブロックチェーンにはブロックチェーンのトリレンマから，大量逐次処理・非中央集権性(分散性)・安全性の 3 つの中で犠牲にするものが 1 つ(ないしは各特性が程々に)となる．ビットコインでは 1 ブロックに入る項目が少ないが，10 分程度 1 ブロックの承認までにかかる時間があるため，大量逐次処理を犠牲にしているといえる．しかし，その後の技術の進展を考えると，大量逐次処理と安全性を重視して非中央集権性(分散性)を諦める方向性が重視された風潮が見られる．

しかし，デジタル人民元には非中央集権性の発想は必要ないと思われるが，Nakamoto(2009)が出た頃以上に FAANG (GAFA+Netflix)や BATH(BAT+Huawei)等の IT・ICT 巨大独占企業が力を持ち，集めた情報を各利用者の思いもよらぬ形で活用することは当たり前になろうとしている．日本国内だけでも，2019 年に内定辞退予測率を提供したリクルート社のリクナビ情報提供事件における反応を見ると，同意を取ってあればむしろ活用すべき情報であった（のでこの事件でやり難くなった）という論調も少なくなかった．情報活用が主となる形が進展していくなら，自らの情報を管理する観点，及びプライバシーの保護等の観点からも対抗手法は大事になる．

Nakamoto(2009)はハイエクの「貨幣の脱国家論」構想を引き継いでいると言われている．これが書かれた 1976(昭和 51)年当時はニクソン・(ドル) ショックなどによりブレトンウッズ体制が崩壊し，世界各国で中央銀行・通貨当局による（本当の意味での）不換紙幣と変動為替相場制が導入された後の頃であり，中央銀行という中央集権的な決定で金融政策そして経済に影響を与える組織に対し，その不信感から貨幣の脱国家論は登場している．Nakamoto(2009)が登場した頃も，ジンバブエではハイパーインフレが起きていたように，通貨当局だけに任せる在り方には疑問符は付いていたが，2018(平成 30)年頃のベネズエラのハイパーインフレに対し，ビットコインを知っている側は自国通貨・ボリバルにかえてビットコインを重視した例を見ても，中央集権的なものだけでは解決にはならないことが分かる．それだけでなく，自国発の暗号資産・ペトロにこだわっていたベネズエラ政府さえもビットコインやイーサを外貨準備として検討し出した例[3]などは，中央集権的なものしかなければ（USA から経済封鎖をされている現状では）取りえなかった選択肢であろう．非中央集権的な選択肢の重要性は残っているのである．

Proof of Work(PoW)より非中央集権性を残した認証方法として優れた選択肢が出てくれば，それに取って代わられるべき PoW であるが，たとえどれだけビットコインの電力問題を言っても情報系では全く相手にされないことを見ても，PoW の重要性はまだ残ると考えられる，ならば PoW の長寿命化のための提言はまだする必要があると考えられる．

8. おわりに

本稿では Proof of Work(PoW)長寿命化のための提言を行った．この提言により大型計算力が参入を諦めてしまう危険性はあるが，認証の安全性と非中央集権性を確保できる．

9. 謝辞

本稿は FIT2018 及び情報処理学会 2019 全国大会での報告を基にしています．フロアの皆様からの建設的で有意義な質問・コメントに感謝致します．全ての在り得るべき誤りは筆者に帰します．

参考文献

[1] Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2009. https://bitcoin.org/bitcoin.pdf (2019 年 1/11 接続)

[2] Vasquez Alex and Patricia Laya, “Venezuela Has Bitcoin Stash and Doesn’t Know What to Do With It,” Bloomberg 2019-09-26, https://www.bloomberg.com/news/articles/2019-09-26/venezuela-has-bitcoin-stash-and-doesn-t-know-what-to-do-with-it (2020 年 1/7 接続)