7G-04

仮想通貨の非中央集権化のための Proof of Work 長寿命化

小川　健†

専修大学†

1. はじめに

2018 年(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，旧来の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．PoW 型はある意味時代遅れ感を持ってしまった．

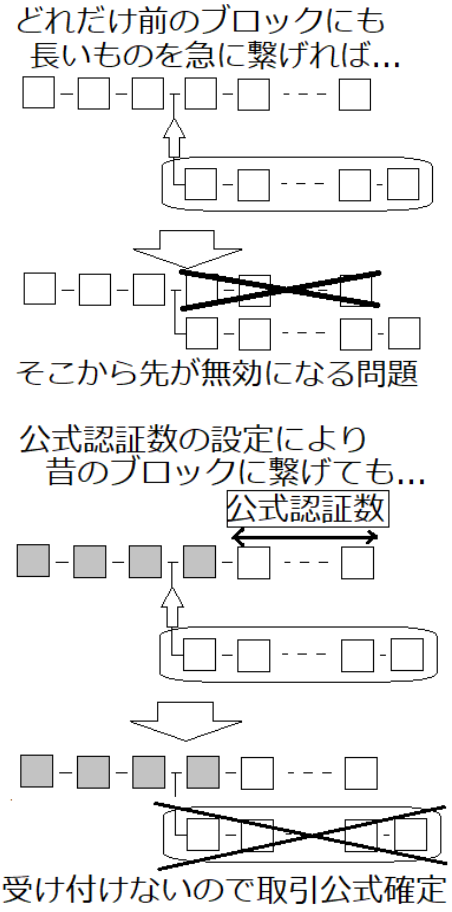
しかし，Nakamoto(2009)が BC 技術の基礎を提示した際に目指した**非中央集権性は**，その後数多く提案された**改良型でも失われる**方式が多い．先の PoS やその改良版 Delegated Proof of Stake (DPoS)，更には Proof of Importance (PoI)でさえ事後的には非中央集権性が確保され難い．PBFT (Practical Byzantine Fault Tolerance)等では認証者(Validation Peer)を増やし難いため分散性に欠け，非中央集権性の鍵となるトラストレスが欠けるため，パブリック・ブロックチェーンには使い難い．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．**

そこで本報告では小川(2018)を改善することで，**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)

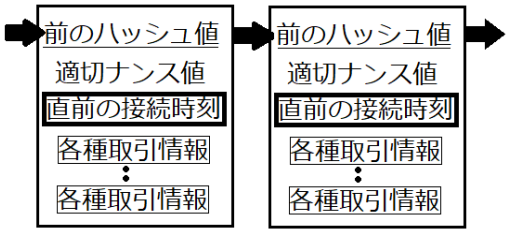
ブロックチェーン等の多くで分岐したら長いものを採用する仕組みを取るが，仮想通貨（暗号資産）の取引所・交換業者の多くである程度のブロック数が繋がれば多分覆らないと判断して扱う慣習がある．しかしビットコインを始めとして，**長いものを後から用意しても接続できてしまう**所に BWA の余地を残してしまう所がある．しかも，UASF(User Activated Soft-Fork)の際にも心配され，MONA コイン騒動で明らかになった様に，大規模な巻き戻し(ReOrg)が起きると取引の信頼性にも影響を来す．

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．



直前の接続時刻をハッシュ関数に入れることで，隠して掘り続けられなくなる．

Long prolongation of Proof of Work
for decentralization of Cryptocurrency
† Takeshi OGAWA (Senshu University)

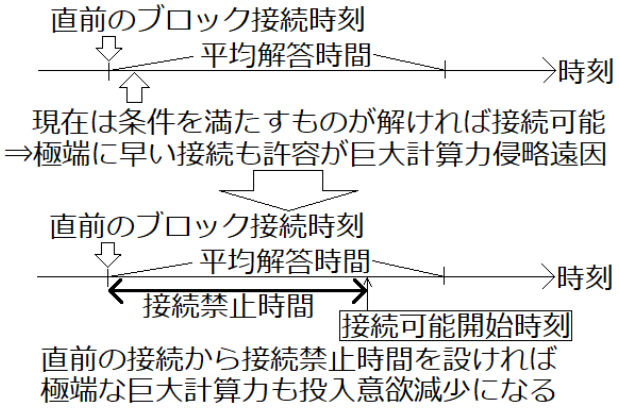
4. 提案 3:接続可能開始時刻の設定と巨大計算力

最近も(2019 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 型仮想通貨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．

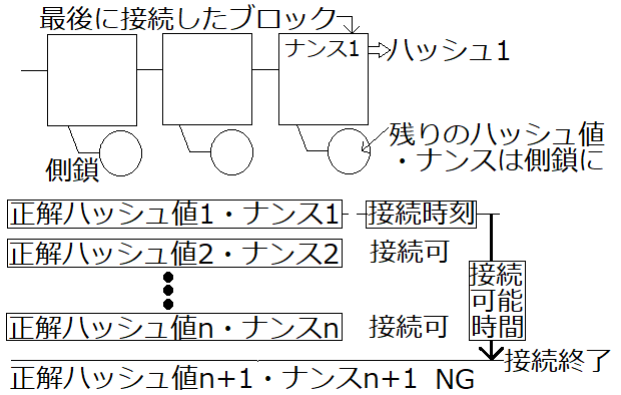
小テスト等での解答時間を例に考えてみよう．10 分用の解答時間の問題を例えば 5 秒で解いたとなれば，通常はまともなことが起きていない．その多くでは不正が起きたか，問題設定にミスがあったか，**何か緊急事態が起きていることは容易に想像**できる．PoW 型も本来は同じである．

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

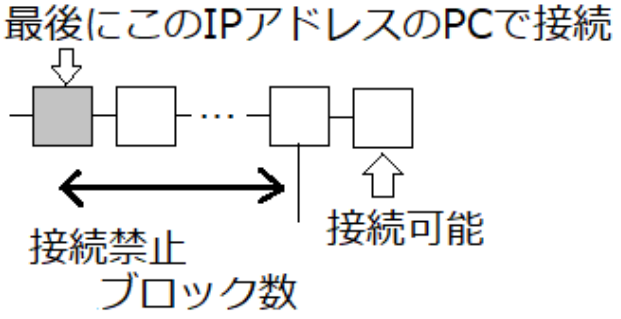
現在の PoW 型の多くが最初の接続者のみの報酬となっている．しかし，条件を満たすハッシュ値と対応するナンス値との関係は一意とは限らない．そこで，最初の接続時刻から接続可能期間を設け，同じ取引情報の組み合わせにも関わらず条件を満たしながらも各々**異なるハッシュ値と対応するナンス値で**異なる IP アドレスから最初に接続申請した場合には，**序列を付けての複数接続者による報酬の案分**を設定する．こうすることで，巨大計算力を投入しても割に合わなくなるので，巨大計算力の投入意欲が削がれる反面，組み合わせが異なれば報酬を得られるので，想定計算力を持つ色々な小規模母体でも報酬を少しずつ得られる形と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

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．



参考文献

[1] Nakamoto, Satoshi (2009) “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf (2019 年 1/11 接続)
[2] 小川健(2018)「Proof of Work(PoW)型暗号通貨認証方式の長寿命化に向けた 1 提言」FIT2018 報告(2018 年 9/20，会場:福岡工業大学)