N-022

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

小川健†1

概要：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技術であるが，その始まりともいえる Proof of Work(PoW)型暗号通貨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)などそこそこ有名な PoW 型暗号通貨を中心に 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．また，電力消費量の巨大化など PoW 型暗号通貨認証方式には環境問題の側面からも問題視されていて，今回の攻撃を機に PoW 型暗号通貨認証方式から他の方式への移行の必要性が数多くの PoW 型暗号通貨で指摘されている．しかし，その代替策として有力視されている Proof of Stake(PoS)型暗号通貨認証方式を初めとして，他の暗号通貨認証方式にもそれぞれ問題は存在し，2018 年 5 月時点で認証方式の最終的な決定版が存在しないのは事実である．加えて，PoS 等他の暗号通貨認証方式の中には先発隊が圧倒的に有利になる点など，一部では公平性(もっと言えば非中央集権制)を損なう可能性も考えられる．そこで本ポスター報告では PoW 型暗号通貨認証方式の長寿命化を念頭に，幾つかの提言を行う．その幾つかは PoW 型を暗号通貨の認証方式として寿命を延ばすことに役立ち，幾つかは別の認証方式の可能性を広げると考えられる．例として(1)1 ブロック毎に解いた時間からタイムスタンプと組み合わせて数分以内にその情報を登録強制し(解いたのを隠しておくのを無効化や，問題にワンタイム制を導入し時間切れで問題を変える)，(2)分岐の可能性を自動通知する，(3)強烈な巻き返し防止のため分岐の長いもの採用ルールに制限を設け，ある有限個まで承認が続いたら(例えば 6 ブロックなら 6 ブロック，50 ブロックなら 50 ブロック)，長いものを用意しても覆せなくする，等を提言する．なお，あくまで暗号通貨認証方式の範囲内での提言であり，他のブロックチェーンまでの波及は限定的とする．

キーワード：Proof of Work 型暗号通貨認証方式，分岐登録の強制，問題のワンタイム化，分岐登録の自動通知，巻き戻しブロック数の制限

A Proposal to Resurrect of “Proof of Work (PoW)” as a Certification Way for Cryptocurrency

TAKESHI OGAWA†1

Abstract: This paper considers resurrecting the way of Proof of Work (PoW) as a certification way for cryptocurrency. The way of proof of work is the first way of certification of blockchain for cryptocurrency (like Bitcoin), so the way are used in various cryptocurrencies of old types. However, in May 2018, Monacoin (MONA) was attacked with block withholding attack, which is different for various old-types attack for place of changing cryptocurrency. After this attack, like Verge (XVG) and Bitcoin Gold (BTG), the way of Proof of Work cannot be felt relieved, so some of PoW types’ cryptocurrencies are becoming changing other certification ways, for instance, Proof of Stake (PoS), and so on. Moreover, Proof of Work are told as not suitable for environment, especially for electric power. However, the way of Proof of Work is important in the viewpoint of decentralization. Thus, this paper considers some ideas to resurrect of Proof of Work as a certification way for cryptocurrency.

Keywords: Proof of Work, Force Branch Registration, Turning Quizes into One Time, Automatic Notification of Branch Registration, Restriction on the Number of Rewind Blocks

1. はじめに

Proof of Work (仕事量による証明，以下 PoW)は暗号通貨（仮想通貨）の始まりとされている Nakamoto [1] でも取り上げられている認証方式（コンセンサス・アルゴリズム）であり，その技術たるブロックチェーンが完成するきっかけとなった着想を基に作られている．野口（[2], [3], [4]），中島[5]，吉田[6]，岡田[7]，木ノ内[8]など暗号通貨やブロックチェーンの代表的な（非技術者用）一般向け解説書にも必ずと言っていいほど紹介されていて，解説サイト等にもその説明は多い（例えば[9], [10], [11]など）．暗号通貨に限って言っても，その始祖たるビットコイン（BTC）を初め，野口[12]などで少額送金手段への活用が指摘されているビットコインキャッシュ(BCH)やライトコイン（LTC），国産暗号通貨の有名例であるモナコイン（MONA）を初めとして，古典的な仕組みを踏襲した暗号通貨では数多くで採用されている．

その反面，小川[13]のように，計算機資源の現実状況や計算速度が有限であることについて，必ずしも一般常識ではない経済学系の学生に対しては PoW を直接は教えず，比ゆ的に世界中で監視しているから，の説明に留めた上で，食いついてきた学生にのみその安全性を担保する，不正意欲を削ぐ仕組みを説明してはどうかとする見解も出ている．

†1 専修大学
Senshu University

現在，PoW には様々な問題点が指摘されていて，イーサリアム（ETH）等では Proof of Stake（PoS）等 PoW から別の認証方式に切り替えた暗号通貨も存在し，PoW から他の認証方式へ切り替えるべきとの指摘も出ている（[14]）．NEM の Proof of Importance（PoI）等他の認証方法を採用した暗号通貨も登場してきている．PoW の問題点の 1 つ目は消費電力の問題があり（[15]），環境や参入可能性等の問題が指摘されている．2 つ目は決済が認証されるまでにかかる時間と認証されないリスクの問題であり（[12]），この部分の解決のためには代行業者も登場してきている（[16]）．

3 つ目が PoW の問題点を攻撃に用いたとされる Block Withholding Attack であり（本稿では敢えて Selfish Mining と区別しない），これまで理論的な問題点としてのみ指摘されてきた（[17], [18], [19]）．しかし 2018 年 5 月のモナコイン（MONA）への攻撃に始まる一連の事件は，従来の（Mt. Gox 事件や CoinCheck の NEM 流出騒動に代表されるように）交換業者側のセキュリティの問題と片付けられない，PoW という認証方法自身が抱える問題点が現実的に表面化した問題として認識され，ヴァージ(XVG),（51%攻撃を実際に受けた）ビットコインゴールド(BTG)などそこそこ有名な PoW 型暗号通貨を中心に攻撃を受け，大規模な「巻き戻し」まで起きている（[20], [21], [22], [23], [24], [25]）．

この攻撃はビットコイン（BTC）のように時価総額最大で採掘（マイニング）を争う計算機資源に強力なものが各地で争いを繰り広げるものを除けば，ほぼ全ての PoW 型暗号通貨で起きると言われている．この基本的な理由には「分岐したら長いものを採用する」という一見合理的な方式が PoW では問題点を抱える面が指摘されているが，この「長いものを採用」というルールを直接変更することは難しく，モナコイン（MONA）では PoS へと認証方法を変える動きまで出てきているとの指摘も出ている（[26]を参照）．

とはいえ，大石[21]にもあるように，「PoS では Nothing Stake 問題」つまり持ち分が多い人が好きにチェーンを作り直せてしまう問題点がある等，他の認証方式にもそれぞれ有名な問題点は指摘されている．

また，野口[2]にもあるように，暗号通貨に端を発したブロックチェーンの重要な意義の 1 つには「非中央集権制」があるが，誰でも「計算機資源さえ用意できれば」新規参入が理論的には可能な PoW と異なり，PoS 等では先に参入した側が圧倒的に有利な面等は（主な認証方式の比較などは例えば[27]を参照），本当に「事後的な場合も」非中央集権的か，という問題点が残る．パブリック・ブロックチェーンにおける PoW の重要性は未だ失われてはいない．

そこで本稿では，PoW の長寿命化に向けた提言を行う．特に現在問題となっている，Block Withholding Attack による「巻き戻し（ReOrg）」への対処を中心に提言を行い，後半部分では消費電力を考えた対応策も取り上げる．但し，参考文献が充分ではない状況の中での原稿のため，各項目についてはオリジナリティを確認できない限りはオリジナリティを主張しない．

2. 巻き戻し(ReOrg)が起きる理由と対処その 1

現在の暗号通貨では原理的には「分岐したら長いものが採用される」関係で，より長い鎖を準備できてしまえば全ての取引は（一度認証した，と思っていた部分まで含めて）覆る恐れがあることが指摘されている（[21], [26]等を参照）．木許[23]によるとあくまで「ブロックの確定の問題」であるとされ，「ブロックチェーンそのものが改ざんされた」訳ではないとされる．

(1) 各暗号通貨における「公式承認数」の設定

今回のモナコイン（MONA）（1 ブロックの承認時間は約 90 秒）への攻撃で実際に巻き戻ったブロック数は 20 以上であり（[21], [28]を参照），この数は「多くの取引所が入金を OK とする数」と言われているため（[21]），「直近で行われた幾つかの取引は無効になってしまう」ため（[28]），「入金の承認数を引き上げるしかない」（[26]）というのが暫定的な対処法の通説とされている．

しかしながら今回明らかになったこととして，各取引所などではその取引が成立した「と判断する」承認数を個々に定めていたことが挙がる．一説には 2 ブロックという例もあるとされるが，その数字が妥当かはともかく，ここまで積み上がっていたらもう覆ることはないだろう，とする想定である．実際，あまりにも過去の承認が今回の伏せて長い分岐を作り続けていた Block Withholding Attack で覆るなどしたら，その影響は甚大となる．

そこで提案 1 として，「分岐したら長いものを採用する」にしても，もうここまで来たら公式に覆せなくなる「公式承認数」を設定し，余りにも古い所からの長い分岐を過去に遡って用意しても承認されない形を取ってはどうであろうか．この数は今までの取引所・交換業者等で入金を認めてきた水準を参考に設定することで，過去における大規模な混乱というのを避けることが出来るようになる．

あくまで「分岐したら長いものを採用する」というのは，PoW 等の良い面の 1 つである，悪意を持った採掘者が覆すのが難しくなるための仕組みに過ぎない．しかし，それをいつまでも認めてしまう場合，例えば今の時代に急に 100 年後のスーパーコンピュータが現れたら全ての取引がほぼ覆せるだろうことが推測できることを思えば，分岐競争に「ゴール」を設定するのも大事なことである．これまでそのゴールは公式に設定されてこなかったが，公式に設定することにより，余りにも昔の取引が覆されて大騒ぎ，という可能性はなくなる．

しかし，当然これだけでは最終解決は見ない．次の提案に移ることにする．

(2) 分岐の強制登録と取引該当者に対する自動警告表示 1

今回のモナコイン（MONA）への Block Withholding Attack

が大きな問題になった点の 1 つに，巨大計算能力を有した悪意ある採掘者が，長い分岐を「隠れて」掘り続けたことが挙がる．現在の PoW の基本的な仕組みだと，各ブロック承認における計算問題を「解いた」ことは確認されても，「いつ」解いたかの確認がなされないので，水面下で解き続けることが可能になる．

しかし，今回明らかになったこととして，一旦承認されたと思い確定を待っている間に長い分岐が「急に」現れる危険性は，確定希望の取引の巻き戻し（ReOrg）への対処が困難になることを意味する．「分岐したら長いものを採用する」ルールの特性を活かすのに，採掘を「水面下で」続けなければならない理由はない．

そこで提案 2-1 として，タイムスタンプ等を活用し，解けてから登録までの時間制限を設け，分岐は 1 ブロックずつしか登録できないようにすることを提案する．こうすることで，長い分岐が「急に」現れる危険性を回避できる．こうした分岐の強制登録により，この一時承認段階となっている直近の取引が，実は覆る可能性があるかどうかをより早期に確認できるようになる．ここに取引該当者に対する自動警告を組み合わせることで，現在一時承認段階のこの取引が狙われていることが明らかになれば，完全に覆る前に取引の取り消しを図るなど，被害を最小限に抑えることが出来る．提案 1 の「ゴール」を決める部分と組み合わせれば，被害の危険性の有無がより認識し易くなる．

一般には「スマートコントラクト」のない種類の暗号通貨の場合には問題になるが，野口[12]で指摘のあるように，報酬の額が充分でない限り承認されずに放置されることが，ビットコインなどでも確認されている．代行業者の役割はこうしたリスクへの対処も存在するが，今回の分岐強制登録がシステムに組み込まれることで，リスク管理もよりやり易くなると考えられる．

(3) 分岐の強制登録と取引該当者に対する自動警告表示 2

提案 2-1 では「いつ解いたか」の情報が必要となってくる．そうするとワークステーションごとに時間設定を「いじられたら」どうするのか？という問題が出てくる．共通のタイムスタンプが活用できれば構わないが，個々のワークステーション毎に組まれた時間設定を活用できないとオフラインでは計算できないことになる．それに対しては不便の声が上がる可能性もある．

そこで，提案 2-2 として「問題自体を」ワンタイム化して制限時間を設けることを提案したい．つまり，問題の表示から解答までに（平均解答時間より長めではあるが，複数のブロックを承認できる程ではない）制限時間を設け，その制限時間を過ぎた場合には解答の登録が無効となる仕組みである．その場合には（ワンタイムパスワードのように）新たな問題が再び作成され，それを解かなければ解答登録が出来なくするのである．これならば，先の分岐の強制登録と取引該当者に対する自動警告表示と組み合わせれば，急に長いチェーンが現れる Block WithholdingAttack はし難くなる（少なくとも水面下で実施することはできなくなる）．特に Block Withholding Attack は水面下で次々と問題を解けたことが大きい．1 ブロックごとに登録しないと次の問題が表示されない形を取ることが望ましい．

この手法が持つ問題点として，正規の計算でもたまたま時間制限に辿り着かず一時承認が遅れることがある，という点が挙がる．先の代行業者を活用するにしてもこの確定が遅れるリスクは大きい．この間にも承認を求める取引は増えることになり，処理能力の問題が残ることがある．しかし，報酬を充分に設定すれば承認失敗が「続く」ことは考え難く，その意味では大きなリスクとは言い難い．

(4) 承認時間に平均解答時間を基にした開始時間を設定

但し，これまでの提言では Block Withholding Attack 等の持つ「本質的な」攻撃性は回避できない．今回のモナコイン（MONA）への攻撃に始まる一連の攻撃の中で，ビットコインゴールド（BTG）では特に 51%攻撃が行われた．PoW 型暗号通貨の持つ「誰でも計算機資源さえ用意できれば参入可能」という仕組みをある意味悪用された形になる．この問題点としては，急に巨大な計算機資源を用意すれば，容易に勝てる状態になっていることが挙がる．これは PoW の本質的な問題の 1 つであるが，かつてヘッジファンドが各国の中央銀行への外貨空売り攻撃等を仕掛けて金融政策を強制的に変えさせた事象に似ている．

小川[13]は経済系の学部生に対し，講義の中で PoW を直接教えるのは避けた方が良いとしている理由の中に，1992 年のポンド危機に対する説明を挙げている．ポンド危機とは巨大な資本を持つヘッジファンドが外貨たるドイツ・マルクを空売りし，（かつて国際金融の仕組みの原形を形作ったとも言える）イングランド銀行が買い支えられなくなって当時の固定為替相場制を放棄させた，という事件である．現代国際金融史を説明する上で欠かせない事象の 1 つである．この説明を頭に置く学部生からすれば，巨大な資本を以てすれば中央銀行の政策さえ変えられるのであれば，巨大資本が巨大な計算機資源を用意することで，容易に勝てる事態を想起させて暗号通貨（仮想通貨）に対する信頼を無くすことに繋がりかねない，との趣旨の指摘をしている．

これがまさに今回のモナコイン（MONA）やビットコインゴールド（BTG）等では起きている訳であり，前述の解説サイト等ではほぼ全ての PoW 型暗号通貨で起きる話と言われている（例えば[20], [29]を参照）．それは他の PoW 型暗号通貨に比べればビットコインでは巨大な計算機資源が次々と投入されているからであり，その計算機処理能力を他の PoW 型暗号通貨に振り向ければ荒らせることにも繋がる．ここを解消しない限りこの問題は解決しない．つまり，急に（その PoW 型暗号通貨では通常想定していないような）巨大な計算機資源が投入されたらどうするか，という問題に PoW は立ち向かう必要がある．モナコイン

（MONA）のような種類の難易度調整を行うことはやめにし，暗号通貨毎に問題の種類や最短解法を変えて総当たり以外には対処が困難にすることは求められるが，それだけでは解決しない．

そこで提案 3 として，最近の平均解答時間を基に，問題の難易度を想定解答時間に合うように調整するだけでなく，解答登録可能な時間にその平均時間を基にした「承認開始時間」を提案する．

定期試験を実施したことのある大学教員ならばイメージできるだろうが，1 時間かかると想定して作成した問題を 5 分で解いてきた学生がいた場合，もちろん天才的な手法で解いた場合もあるかもしれないが，通常は何か異常を疑う．それが問題の設定ミスでショートカットが可能な問題だったのかもしれなければ，何かしらの不正があったのかもしれない．巨大な計算機資源を急に突入させればもちろんこうしたことは可能になるだろうが，この意欲を削ぐためには 1 時間かかる想定の問題を 5 分で解いても 5 分で「提出できない」仕組みにすることが肝要である．

PoW 型暗号通貨でも同様で，継続的に短時間で解けてしまうような巨大能力を持ってきても充分に活かせない仕組みにすることが大切になる．仮に平均 10 分かかる設定の問題がこの暗号通貨には無い巨大計算機資源を持ち込むことにより 5 秒で解けたとしても，例えば解答登録は 8 分からしかできないとすれば，残りの時間は待たされることになる．その暗号通貨における従来の採掘計算機資源でも 8 分なら早ければ間に合ってしまう可能性も十分にあり，この巨大計算機資源を投入する意欲が多少削がれることになる．

従来の PoW ではこのような巨大計算機資源を持ち込めればほぼ確実に勝ててしまうが，ここまでの計算機資源をつぎ込むのが割に合わないとなれば，つぎ込む計算機資源も巨大なものではなく少し大きい程度に留めることになる．実際には想定時間の何割にするかは暗号通貨毎に考える必要があるが，この「巨大計算機資源をつぎ込むのが割に合わない」ことを示せることが肝要になる．

勿論，偶々解けてしまった，という場合もあると思われる．この場合には先のタイムスタンプと合わせてその後に誤りの部分をしらみつぶしに潰させる作業の提出をさせる，ということで可能になると考えられる．解かない，という選択を許した場合，その間に他の所を荒らしに行く，ということがありえる．もし「解く速さが読めない」のであれば，タイムスタンプ等を活用し，解き終わった後「計算機資源を休ませていた」証拠を提出することにすればよい．他を荒らしに行くことを防ぐのが肝要である．

3. Proof of Work (PoW)の電力消費問題対処へ

PoW 型暗号通貨でもう 1 つ無視できないのが消費電力の問題である．既に 1 国の消費電力を遥かに超える項目が採掘のためだけに使われていて，環境への問題と計算機資源の無駄遣いの両面から本来は懸念される．ここでは後者は置いておいて前者の問題に対処するために，PoW の仕組みを一部変更した仕組みを提案したい．

PoW では「常に解き続ける」ことによって消費電力の問題が残った．では「解かない」つまりワークステーションを「休ませる」時間を確保することを認証の優先手段としてはどうだろうか．具体的には初めと終わりのタイムスタンプを設定し，その時間そのワークステーションでは「事実上休ませていた」履歴を提出させ，締め切り時間を設けてその休息時間と届け出の速さとで承認権限をかくりつてきに割り振る仕組みを作るのである．

これは PoW とは違う認証の仕組みになるかもしれない．しかし，PoW の持つ電力消費問題への対処の一端になる可能性があるが，PoS のように先に動いて保有していた方が圧倒的に有利，という事態は避けられる．

但し，完全に新規も平等，という仕組みでは悪意ある参加者が紛れ込み易い懸念は残る．そこで，（PoS や PoI のいい所だけ真似て）そのワークステーションでの承認実績数をここに加えることで，新人にも公平に，との建前は崩れるが，いわゆる荒らし屋は意味をなさなくなると思われる．

4. おわりに

本稿では PoW 型暗号通貨の長寿命化に関する幾つかの提言を行った．未だパブリック・ブロックチェーンで重要性を失わない PoW がこの騒動を機にブロックチェーン自体の価値を損なわせるとして退場することになれば，ブロックチェーンの信頼そのものを失わせかねない．これはようやく広がりを見せるようになった，暗号通貨に留まらないブロックチェーン産業の広がりに水をさすものである．

確かにリップル（XRP）における Proof of Consensus（PoC）のように，報酬を目的としない認証も存在するが，PoC では暗号通貨の持つ「非中央集権性」は崩れる可能性が知られている．仮想通貨に端を発する一般向けの啓蒙書として知られているジョージ[30]でも指摘のあるように，採掘（マイニング）は認証における機会の公平と安定性を両立させる上でその重要性は残っている．

本提案のうち一部でも PoW の改善に繋がることを期待してやまない．

謝辞　本報告を許可してくれた SSS2018 の皆様に感謝するものである．また，妻木伸之先生（専修大学・法部非常勤講師）には本稿の構想を考える上で参考になる助言を頂いた．加えて小川ゼミ（生田）の 2018 年度入ゼミ生とは（ゼミ生への指導の中で）本稿を作成する上でイメージを構成する非常に有益なやり取りを行った．ここに記して感謝する．なお，本稿のあり得る誤りは全て著者単独に帰するものである．

参考文献

[1] Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System, 2009. https://bitcoin.org/bitcoin.pdf , （参照 2018-06-04）
[2] 野口悠紀雄．仮想通貨革命．ダイヤモンド社，2014．
[3] 野口悠紀雄．ブロックチェーン革命．日本経済新聞出版社，2017．
[4] 野口悠紀雄．入門 ビットコインとブロックチェーン．PHP ビジネス新書，2018．
[5] 中島真志．アフター・ビットコイン．新潮社，2017．
[6] 吉田繁治．仮想通貨 金融革命の未来投資図．ビジネス社，2018．
[7] 岡田仁志．決定版 ビットコイン＆ブロックチェーン．東洋経済新報社，2018．
[8] 木ノ内敏久．仮想通貨とブロックチェーン．日本経済新出版社，2017.
[9] “プルーフ・オブ・ワーク（PoW）を少し詳しく！”．http://www.tottemoyasashiibitcoin.net/entry/2017/01/09/163336 , (参照 2018-06-04).
[10] “Proof of Work(プルーフオブワーク）とは？PoW を分かりやすく解説します”．https://www.newscrypto.jp/articles/5647 , (参照 2018-06-04).
[11] MOBLOCK, “【基礎】ビットコイン（bitcoin）の Proof of Work(プルーフオブワーク）をわかりやすく解説”．https://moblock.jp/articles/17193 , (参照 2018-06-04).
[12] 野口悠紀雄.“ビットコイン消滅も、送金コスト高騰問題の行方”，2017．https://diamond.jp/articles/-/150612 , (参照 2017-12-28).
[13] 小川健. 非技術／情報系の経済系に仮想通貨・ビットコイン・ブロックチェーンをいかに教えるか. 専修経済学論集, 2018, vol.52, no. 3, p. 167-182.
[14] “イーサリアムの POS‘CASPER’が解決する POW の問題”．https://ethereum-japan.net/ethereum/casper-ffg-testnet-release/ , (参照 2018-06-04).
[15] CoinPost.“ビットコインマイニングの消費電力が世界 159 ヶ国の各消費量より多い現状”，2017．http://coinpost.jp/?p=9208 , (参照 2018-06-04).
[16] COINNEWS.“ビットコイン決済の代行サービスとは？～ビットコイン決済を導入する方法～”，2017．https://coinnews.jp/articles/105 , (参照 2018-06-04).
[17] Ittay, E., Emin, G.S., Majority is not Enough: Bitcoin Mining is Vulnerable, arXiv:1311.0243, 2013. https://arxiv.org/abs/1311.0243 , (参照 2018-06-04).
[18] 佐古和恵，古川諒.“ビットコインは本当に安全なのか、理論研究が示す意外な落とし穴”，日経 FinTech，2016. http://tech.nikkeibp.co.jp/it/atcl/column/16/062400138/112400011/, (参照 2018-06-04).
[19] “マイニングプールの収益配分と攻撃手法”，2017．https://www.slideshare.net/mosa_siru/ss-88102219 , (参照 2018-06-04).
[20] JunyaHirano.com. “暗号通貨史上で最も大きいブロックチェーンへの攻撃について. モナコインでの事件の重要性. ”, 2018. https://junyahirano.com/about_selfish_mining/ , (参照 2018-06-04).
[21] 大石哲之.“モナコインへの攻撃について（BLOCK WITHHOLDING ATTACK）”，2018. http://doublehash.me/monacoin-attacked/ , (参照 2018-06-04).
[22] 野口悠紀雄.“仮想通貨の資金消失をもたらした「51%攻撃」とは何か”，2018．https://diamond.jp/articles/-/171239?display=b, (参照 2018-06-04).
[23] 木許はるみ.“仮想通貨モナコイン「消失」で緊急説明会、杉井氏「ブロックの確定に問題」と説明”，2018. https://www.businessinsider.jp/post-168621, (参照 2018-06-04).
[24] TECHWAVE.“モナコインで莫大なプロセッサパワーをつかった重大な攻撃”，2018. https://techwave.jp/archives/monacoin-block-withholding-attack.html, (参照 2018-06-04).
[25] 平野淳也.“モナコイン(MONA)やビットコインゴールド(BTG)など複数のブロックチェーンに対して悪意あるマイナーが攻撃”，CoinChoice，2018. https://coinchoice.net/mona-bitcoingold-attack/, (参照 2018-06-04).
[26] CryptoTimes.“モナコイン、バージ、ビットコインゴールドのハッキング情報まとめ”，2018. https://crypto-times.jp/monacoin-verge-bitcoingold-hacking/ , (参照 2018-06-04).
[27] “分散合意形成アルゴリズムの種類（PoW、PoS、Pol)”, 2017. http://www.zbaron-newworld.com/entry/2017/02/04/000047 , (参照 2018-06-04).
[28] bit-life.“モナコインのブロックチェーンにマイナーの攻撃！手法と一連の流れ”，2018. http://bitlife.cryptopie.com/monacoin-block-withholding-attack/ , (参照 2018-06-04).
[29] “暗号通貨に対する「Block withholding attack」が初めて確認される”，2018．https://security.srad.jp/story/18/05/18/0630205/ , (参照 2018-06-04).
[30] ジョージ，S. MINE．冬至書房，2018.