Jun. 2018
株式会社 Baroque Street

Baroque Monthly

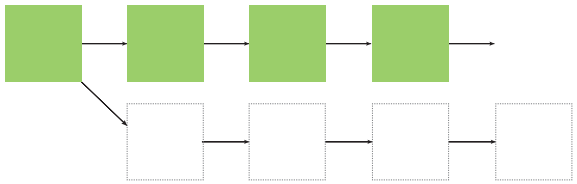
TOP NEWS

相次ぐマイナーによる攻撃

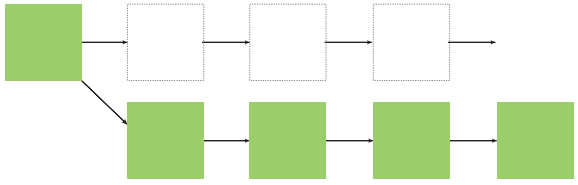
5/15、日本発の暗号通貨としても知られるモナコイン（MONA）に対してマイナーによる攻撃が行われた。これは Block Withholding Attack あるいは Selfish Mining と呼ばれる攻撃で、以前から業界内で懸念されてきたものである。今回の攻撃で被害を受けた事業者は Livecoin という小さな取引所で、被害額については公表されていないが、おそらくこれまでのハッキングに比べれば少額であったと思われる。しかしながら、この事件がこれだけ注目を集めたのは、マイナーによるチェーンへの攻撃が実際に行われた、非常に稀有なケースだった為である。

Block Withholding Attack は次のような流れで行われる。1) 通常マイナーはブロックを発見した際にはネットワーク上に公表するのだが、それをすぐには公表せずに隠れてマイニングを継続する。2) 悪意あるマイナーが意図した取引を実行。3) チェーンがある程度分岐したタイミングで隠れて掘っていたブロックを一斉に公表する。4) 正規（最長）のチェーンが塗り替えられ (Reorg)、その間に行われた取引が無効となる。今回で言えば、攻撃者は MONA を取引所に送金し別通貨に換えて出金した後、機を見て Reorg したと言われている。

【ブロック公表前】



【ブロック公表後】



このような攻撃は、PoW や PoS といったアルゴリズムを用いるパブリックブロックチェーンの特性、すなわちファイナリティが無く最長のチェーンを正規のものとするといった決まりを上手く利用している。通常、ビットコイン（BTC）やイーサリアム（ETH）といったパブリックチェーン上では、ブロックが確定するタイミングが明確には存在しない。業界では 6 ブロック承認が一つの目安となっているが、これはあくまで確率論的に 6 ブロック承認されれば改竄される可能性は少ないだろう、といったことで決められている。サービス上いつをもって取引完了とみなすかは各取引所、交換業者によって様々であり、各々の判断でそれを 3 ブロックとすることもできれば 10 ブロックとすることもできるのである。余談ではあるが、エストニアの ATM では 2 ブロック承認が目安であった。

この事件発覚後、多くの取引所は MONA の取引目安となるブロック承認数の引き上げを行なっている。ハッシュレートの多くを特定のマイナーに握られてしまった以上、サービス提供者として打てる対策がこれ以外に無い為である。開発者側の対策としては、「今後 PoS 等への移行も視野に入れていく必要がある」と開発者の Watanabe 氏から発言があったように、アルゴリズムを見直すといった対応も考えられるだろう。しかし、PoS もまた富の集中化や Nothing at Stake 問題、Long Range Attack といった課題があり、PoW も PoS もその他アルゴリズムについても現状は一長一短であると言える。

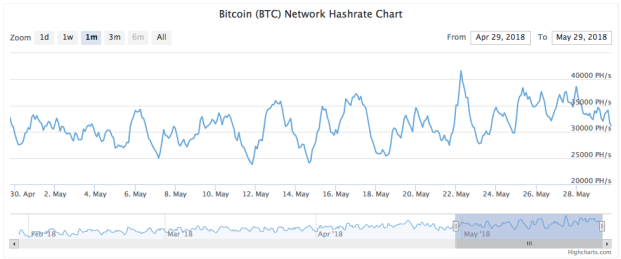
今回 MONA がマイナーの攻撃対象となった理由は「ハッシュレート」この一言に尽きるだろう。MONA のハッシュレートは執筆現在 2.0TH/s 前後で推移しており、BTC の 33EH/s(=33,000,000TH/s)、ETH の 270TH/s と主要通貨に比べて極めて低いことがわかる。BTC は ASIC マイニングが主流である為桁違いとなっているが、MONA と同様 GPU マイニングが主流

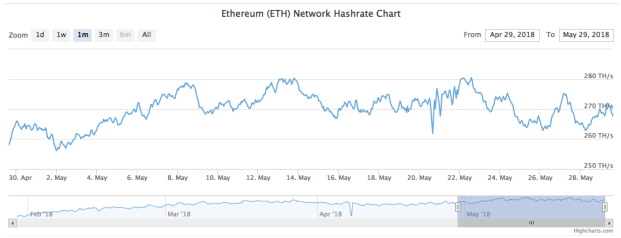
となっている ETH と比べてみてもその数値は 1/100 以下である。つまり、一例ではあるが ETH で 2.0TH/s のパワーを使っている人が一時的にその全てを MONA に向けることによって、MONA のハッシュレートの 50% 以上を占めることは実質的に可能なのである。このことを考慮すれば、ハッシュレートの低い通貨で時価総額上位の通貨は悪意あるマイナーによる攻撃インセンティブが高く、今後同様の事件は増えていくかもしれない。ここでは詳細に触れないが、実際に MONA に続いて 5/18 にはビットコインゴールド（BTG）、5/22 には匿名通貨ヴァージ（XVG）が同じくマイナーによる攻撃を受けている。

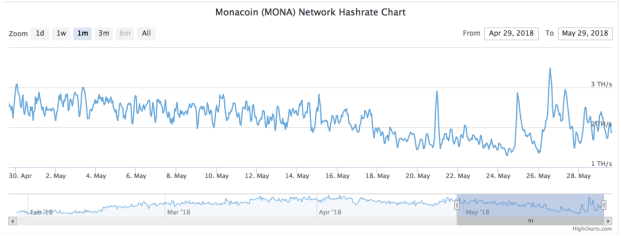
今年に入り、ようやく各方面で暗号通貨に関する議論が展開されるようになってきた。Coincheck 騒動以降の取引所リスク、SEC 主導の暗号通貨の証券性に関する議論、そして各国規制である。今回の一連の事件は暗号通貨・ブロックチェーンそのものの安全性を改めて考えさせる良い契機である。ハッシュレートは通貨の安全性に直結しておりマイナーによって分散化されるべきであること、また、ブロック承認速度は通貨の安全性とトレードオフの関係にあることを我々は再認識しなければならない。これらを踏まえて、今後ブロックチェーンの合意形成アルゴリズムに関する議論も増えてくるだろう。

私が思ったことがもう一つ、それは過去 5 年間と同様、この先 5 年で CoinMarketCap(CMC) の順位はやはり大きく変動するだろうということである。今回ハッシュレートの低い通貨が攻撃対象となったが、この流れはしばらく継続すると考えられる。そもそも 51% 攻撃は、攻撃があったとしても周知されることで通貨の価格が下がる為、マイナーのインセンティブが働かないという前提があったが、今回のように CMC の順位も比較的高く短期的に犯行が行われれば、攻撃を回避することは難しいように思う。だとすれば、長期的に生き残る通貨はハッシュレートの高い一部の通貨に限られると考えるのが自然であろう。

今後予想されるマイナーの攻撃は、取引所を対象にしたダブル・スペント攻撃が主であると思われる。取引所そして開発者側は、この脅威に対して何かしらの対策を講じるだろう。取引所はハッシュレートの低い通貨に関してブロック承認数を引き上げるかもしれない。開発者側はアルゴリズムの見直し、改良を図るかもしれない。今回も然り、事件が起きてすぐ皆が周知し、議論され解決に向かう。これが暗号通貨・ブロックチェーンの面白い世界である。







引用：https://www.coinwarz.com/cryptocurrency

BCH ハードフォーク

5/15、予定されていた通りビットコインキャッシュ（BCH）のハードフォーク（HF）が行われた。今回の HF の主な目的はブロックサイズの拡大とオペコードの追加・改良である。ブロックサイズは 8MB から 32MB へと引き上げられ、オペコードは OP_AND や OP_OR 等複数のコードの追加、過去に攻撃への懸念から無効化されていた OP_CAT の復活、OP_RETURN の取扱可能なデータサイズの拡大が行われた。より簡潔に言えば、オンチェーン上のスケーラビリティ問題の改善、スマートコントラクトを構成する為のオペコードの追加、オンチェーンに記録できるデータサイズの拡大、以上が今回の HF によって変更された点と言える。

BCH はニューヨーク合意（NYA）等 BTC のスケーラビリティに関する一連の議論の末、2017/8 月に誕生した。ライトニングネットワーク等の 2nd レイヤー技術でスケーラビリティ問題の改善を目指す BTC とは違い、BCH はオンチェーン上での改善を目指している。今回のブロックサイズ拡大はその流れから行われたものであり、この変更により取引処理速度の向上が見込まれる一方で、マイナーの寡占化を促進するとの懸念もある。スモールブロック派とビッグブロック派との対立については、前にも述べたことがある為ここでは深く踏み込まないが、今尚賛否両論に議論され

る重要な内容である。

今回の BCH の HF に関しては、何か意見の食い違いが生じて新しい通貨が生まれるといった類のものではなく、どちらかと言えばソフトフォークに近い性質のものであった。改善内容の都合上互換性を持たせないアップデートとなり HF の形をとったが、今回 HF と聞いて「新しい通貨は誕生しないの」と疑問に思った人も少なくないだろう。それほどに昨今のメディアの影響により「HF= 新通貨の誕生」というイメージが（アマチュア）ユーザーには植え付けられている。HF 前には新通貨の付与という虚構の期待から買いに動いた人も一定数いたのではないだろうか。確かに過去の経験則から HF 前に価格は上昇したが、多くの人が表面ばかりに注目し肝心の中身を見過ごしている。

今回の HF はソフトフォークに近い性質のものであったと述べたが、実際に BCH コミュニティ内での対立は起きなかったのだろうか。通常何か大きな決定を行う時はコミュニティ内で投票を行うことが多いのだが、どういうわけか今回の HF は投票無しに決定されている。このように聞くと反対の声も上がるのではないかと思うが、一部を除いて開発者とユーザーともに賛同する声が多く、現状大きな分裂の動きは出ていない。執筆現在ハッシュレートも安定的に推移しており、マイナーが離れる様子も見られない。ここからは BCH コミュニティのまとまりが伺える。

このようなコミュニティのまとまりを生み出す大きな要因として、開発者側とマイナーとの密接なつながりが挙げられるだろう。BCH 開発者側の Bitcoin ABC は 2017/12 月に中期開発計画という名で 2018 年度のロードマップを公表した。そこでは、BCH 開発者側の中心とも言える Bitcoin Unlimited をはじめ複数の開発者と連携して話を進めているとの記載がある。Bitcoin Unlimited とは、BCH が誕生するきっかけとなった BTC のスケーラビリティ問題を巡って、Bitcoin Core と対立した開発者コミュニティである。主にマイナーで構成され、最大手マイニング会社 Bitmain 社の Jihan Wu 氏が支持することでも知られる。BCH コミュニティでは開発者とマイナーとが表裏一体の関係にあると言えるのかもしれない。

Bitcoin ABC は今回の HF とは別に 11 月にも HF を行う予定であると公表している。具体的な内容については 3 ヶ月前の 8 月に発表されることになっているが、次回も大きなアップデートが行われることが予想される。BCH コミュニティは、ETH のようにブロックチェーン上でスマートコントラクトを実装する構想を持っており、その線に沿った改善が行われるのではないかと思われる。いずれにせよ今後の BCH の動向に注目である。

SEC 'HoweyCoin' 作成

5/16、米国証券取引委員会（SEC）は HoweyCoin という名の模擬 ICO を立ち上げた（名前は証券性を判断する HoweyTest から来ている）。これは最近における ICO 詐欺の増加を受け、SEC が投資家への注意喚起の目的で作成したものである。実際の HP は、会社紹介から簡単なホワイトペーパーまで一通り ICO プロジェクトによく見られる形式でまとまっている。内容についても「旅行で使える暗号通貨」「米国政府登録」「SEC 規制準拠」とそれらしい言葉が並べられており、素人目では一見しただけで詐欺かどうかを判断することが難しい。SEC は「ICO サイトはこれだけ簡単に作ることができる」ということを訴えかけており、今回の取組を通じて投資家の認識を改めようとしている。実際にユーザーが HoweyCoin を購入しようとした際には、注意喚起サイトに推移するようになっている。

SEC は自分たちのこれまでの経験から考えうる詐欺 ICO の特徴を当該サイトに複数盛り込んでいる。まず始めに、リターンの保証が挙げられる。模擬 ICO では 1 日 1%、年間で 7% ～ 15% のリターンが得られるとの記載があり、魅力的なハイリターンに騙される人も少なくないだろう。次に、著名人による後ろ楯のコメントである。ここでは、3 名の著名人による HoweyCoin へのコメントが紹介されていたが、自身の好きな著名人がそのプロジェクトを支持しているとの理由で投資してしまう人もいるのかもしれない。さらなる特徴としては SEC 規制準拠との記載が見られ、SEC は今後 SEC 規制準拠と主張する ICO が増えるのではないかと懸念している。その他、クレジットカードでの購入が可能、Pre-ICO のスペシャルオファーがあるといった特徴が挙げられていた。SEC に登録済の企業の中でクレジットカードでの投資資産購入を認めている企業はほとんどなく、Pre-ICO のスペシャルオファーは Pre-ICO 後の Pump&Dump スキームに利用されることが多いとの見解であった。

私も職業柄今ある ICO プロジェクトについて調査を行う機会も多いが、もはや数が増えすぎて事業内容、トークン設計に目新しさを感じることも少なくなってきた。似通った ICO が乱立するだけでなく、次から次へと新しい ICO が現れる。その中には SEC の言う

詐欺 ICO も多く含まれるだろう。私が思うに、今ある ICO の中で実際にユースケースとして定着するものはほんのごく一部に限られるだろう。詐欺の定義は人それぞれである為、あくまで個人の意見として聞いてもらいたいが、仮にユースケースとして定着する可能性の高いプロジェクトを正常な ICO と定義するのであれば、今あるほとんどの ICO は詐欺である。

事業内容は別として、私の言う「詐欺 ICO」は大きく分けて 3 パターンあると考えている。第 1 に、プロダクトも無く誇大広告で投資を煽るような一般的な詐欺プロジェクトである。暗号通貨の世界にしばらくいる人であれば、この類の ICO に騙されることはほとんど無いだろう。第 2 に、マーケティングばかりが先行し、開発が追いつかないようなプロジェクトである。これは構想が壮大過ぎる場合と技術者が不足している場合と両方考えられるが、どちらの場合にせよプロダクトが実用化されるまでには長い年月がかかると思われる。そして第 3 に、ICO で資金調達したものの構想自体が安易であり、事業内容そのものに魅力が無いようなプロジェクトである。これは主にスタートアップ企業に近い性格のもので、創業者を含めチームメンバーの経歴が浅い場合に多く見られる。

以上、「詐欺 ICO」について述べたが、ICO の大きな問題点は上に述べたようなことは投資家にとっては正直どうでも良いということである。たとえそれが本質的には詐欺でハイリスクであるとわかっていても、価格が変動するもので大きなリターンが見込まれるのであれば、投資家は多額の資金を投じることを惜しまない。だからこそ、適当なプロジェクトであっても簡単に数億円単位の資金を ICO で調達することができるのである。株式などと同様にプロ投資家とアマチュア投資家とで別のルールを設けることが良いとは言わないが、何かしらの策が講じられなければ今の状況が変わることはしばらく無いだろう。

今回 SEC が注意喚起目的で作成した模擬 ICO は、確かに経験の浅い一部の投資家に対しては効果的であったと思われる。しかし、大半のプロ投資家にとってはさして影響が無いと考えるのは私だけだろうか。彼らにとって ICO 投資はあくまで余剰資金を使ったマネーゲームである。株式や為替への投資に飽き飽きしていた頃に面白い金融商品が現れたといったような感覚なのだろう。年利わずか数 % と言われる株式に比べれば、ほんの数ヶ月で数倍、数十倍と一攫千金が狙える ICO 投資はある意味刺激的で面白い。BTC や ETH といった主要通貨ではなく、マイナーな ICO に興味を持つ投資家の多くはリスクを十分把握した上で多額の資金を投じている。このことを示すように、私が海外に来て参加したミートアップ、あるいはカンファレンスには必ずといって個人投資家が参加していた。このような ICO の現状を SEC は理解した上で規制の議論を進めていかなければならない。

金融庁 交換業審査を厳格化

5/5、金融庁が暗号通貨交換業者の新たな審査基準の策定を検討していることがわかった。主な重点項目は以下の 5 つ。1) 顧客資産の分別管理 2) 株主と経営の分離 3) システム開発と経営の分離 4) ホットウォレットでの資産管理禁止 5) 匿名（暗号）通貨の取扱禁止である。Coincheck 騒動以降、金融庁は暗号通貨関連業者への取り締まりを強めるばかりであるが、今回の発表を受け「日本の暗号通貨業界の発展は終わった」と悲観する声も多い。このような動きの中、登録申請を辞退する業者も相次ぐ一方で、メルペイや LINE、マネーフォワードと言った大手 IT ベンチャー企業は新規参入を表明しており、今後の審査状況に注目が集まる。

金融庁が掲げた上記項目の中で 1) から 3) までは、内容が厳しくベンチャー企業による新規参入が難しくなったと批判する声も聞かれるが、金融業を営むのであればごく当たり前の要件であるように思う。金融業に数年間務めた身として言うが、そもそもコインチェック騒動で見られたように、経験の浅いベンチャー企業が金融業を行おうと会社を立ち上げること自体、悪いとは言わないが、考えが甘い。仮にこれが厳しいと言うのであれば、それは金融の歴史に取り残された人の単なるわがままである。(規制が良いと言っているわけではなく、あくまで人の資産を預かる立場として当然と言っていることを理解してほしい。)

4) と 5) については明らかに時期尚早の判断であると言わざるを得ないだろう。4) に関して、通常多くの取引所は資産をホットウォレット（オンライン）とコールドウォレット（オフライン）とで 2 : 8 あるいは 1 : 9 等の割合で分けて管理している。それはコールドウォレットの方が資産を安全に管理できる一方、資産の一定割合をオンライン接続のままにすることで、入出金速度等の UX を高める狙いがあるからである。ホットウォレットでの管理はハッキングリスクがあるものの、ユーザーの取引に素早く対応できるというメリットがあるのである。個々の取引所はこのトレードオフの関係を十分に検討した上で、これまで資

産管理の方法を決めてきたのである。

5) に関して、匿名通貨についてはマネロンやテロ支援等の犯罪防止の観点から、これまでも多くの議論がなされてきた。そもそも、匿名通貨はなぜ誕生したのか。その理由は BTC の不完全な秘匿性にある。BTC は一見匿名性を担保しているかに思われるが、全ての取引は誰もが確認できる形でブロックチェーン上に記録されている。確かに、BTC アドレスは 30 文字程度の英数字でできており個人を特定することは難しい。しかし、情報の連結性を辿りアドレスが一度個人情報に紐付けられてしまえば、そのアドレスを使った過去、現在、未来のあらゆる取引のプライバシーは失われるのである。そこで、より現金に近い形で匿名性を担保しようと生まれたのがダッシュ（DASH）やモネロ（Monero)、ゼットキャッシュ（Zcash）と言った匿名通貨である。

仮に匿名通貨が今ある現金に近い匿名性を備えたとして、これらの一番の違いは何だろうか。それは当たり前のことであるが、匿名通貨による国際間の資金移動が容易であるということである。一般の店舗決済等で匿名通貨が使われる分には、金融庁もおそらく大きな懸念は示すことは無い。しかし、それが国際送金等に持ち込まれた際には規制を検討せざるを得ない。現金決済と同様、匿名通貨を用いて国際決済をした際には誰もその経路を追うことができない為である。

政府がこのような思考に行き着くのは容易に想像がつく。「お金」はいわば国力の象徴であり、争いの源であるからだ。だからこそ、これまでも国際間で資金を移動する際には銀行という仲介機関を通し、一定額を超える場合には政府への報告を求めて来た。金融庁は、5/18 に暗号通貨による国際送金についても外為法を適用し、3,000 万円を超える場合には財務省への報告を求めると周知している。おそらく取引所がその確認業務を担うと思われるが、取引所を介さない P2P 取引については金融庁がどこまで追えるのか甚だ疑問である。

今回の措置は、改めて国を跨いで資金を移動することの難しさを訴えている。それはモノの移動であれ同じである。グローバル化が進んだとはいえ未だに国境の壁は高く、国際間のお金・モノの交換には国内事情だけでなく国際事情、現在だけでなく過去すなわち歴史が関わってくるのである。このような現実世界と、BTC が生み出した真にボーダレスなヴァーチャル世界とが今後どのような形で交わるのか、5 年後 10 年後の未来が楽しみである。

Consensus2018 開催

5/14-16、大手暗号通貨メディア Coindesk が主催する Consensus2018 が米国ニューヨークで開催された。本イベントは業界の一大イベントとしても知られ、今年で 4 回目となる。今年はニューヨーク州初の取り組みとなるブロックチェーンウィーク（5/11-17）のメインイベントとして行われ、世界各国から大手取引所や有名プロジェクトの CEO、開発者と言った業界の要人らがスピーカーとして登壇した。日本からは bitFlyer CEO：加納雄三氏がスピーカーとして参加している。来場者数は正式には公表されていないが、昨年 3,000 人程であったことを考えると今年はそれを遥かに上回る数であったと思われる。

このイベントでは確かに各企業から重要な発表も一部行われるが、正直なところ講話内容については全く興味が無い。それは今の時代事後的に Youtube で確認することができる為である。以下では、この業界だけでは無いかもしれないが、私の思うカンファレンスの特異性について簡潔に述べる。

「カンファレンス」と聞くと、パネルディスカッション等で業界の有識人らが意見を述べる姿を想像する人も多いと思われるが、今世界各国で行われている暗号通貨・ブロックチェーン関連のカンファレンスはどうやら様子が異なる。一部上述したようなものも存在するが、そのほとんどは PR 色が強い。ICO 後に自社を宣伝するもの、ICO 前に公募を募るもの、いずれにせよ登壇目的は同じである。調べればわかる内容を一大発明をしたかのように大袈裟に話す。リスナーとしては学校の校長先生の話くらいに退屈である。

来場者についてもどこか性質が違う。メディアの来場者が多く、一般で来場した人もおそらくその多くが自国に戻った後何かしらイベントを行う為に来場している。それを示すように本イベント後には Consensus 報告会という名のイベントが散見された。そのイベントにも話を聞こうと多くの人が集まったらしい。

運営側もボロ儲けである。チケットは 1 枚 10 万円するものも少なくないが、不思議なことに売れている。これだけチケットが高くとも、カンファレンスを開催するだけで、これだけ人が集まる業界も珍しいだろう。その為、世界各国で同様のイベントが乱立し運営側も PR を必死に行う。私は運営サイド、登壇者、来場者これら一連の流れを「PR の連鎖」と呼んでいる。

著：松嶋