2019 年 6 月 5 日
5 班(相田、柴田、舘林、古森)

これで分かったビットコイン〔生きのこる通貨の条件〕

著書/編集：斉藤賢爾、発行元：太郎次郎社
～しくみ編～

（柴田）p.1～p.7

【基礎技術「ハッシュ値」】

○大きなデータを扱いやすくする工夫
ビットコインは暗号技術を用いて作られている。→ハッシュ値(暗号学的ハッシュ値)を基本概念としており、これはダイジェスト。
ダイジェストみたいに大きなデータを調べなくとも正しくコピーできたか確認出来る。→ハッシュ値を得るための暗号学的ハッシュ関数はデータを圧縮しても戻せない。

○ハッシュ関数とその種類
暗号学的ハッシュ関数のなかに SHA というものがあり米国の NSA により設計されている。よく使われる SHA-1 は 160 ビットの数字列をハッシュ値として出力する。
こういったハッシュ関数は複雑だとされることがあるが、なるべく省メモリでハッシュ値を求められるよう設計されているので、あまりそういったことは言えない。

【デジタル署名とその使われ方】

○デジタル署名とは何か
公開鍵暗号系の技術から生まれたもので、本人が署名したことと、それを改竄していないことが証明できる。→公開鍵暗号とは、公開鍵と秘密鍵を利用者がもち秘密鍵を隠し持ち公開鍵で公開することで秘密鍵によって暗号化したデータは公開鍵でしか解読できないシステムである。
デジタル署名では、署名したい内容のハッシュ値を求め自分の秘密鍵によって暗号化し相手に送ったのち受け取った側は同じようにハッシュ値を求め送り手の公開鍵によって確認することにより本人のものだと確認出来る。
→通販などでもこういった技術が使われている。

○BTC 取引とデジタル署名
ビットコインはデジタル署名を繋げて BTC の取引を表現する。

コインを支払う際、コインの所有者は現在のコインと相手の公開鍵を合わせたデータに対して秘密鍵を用いて署名する。→相手は、その署名をハッシュ値を再計算する事によって正当な所有者から渡されたものだと確認することが出来る。
コインの所有者は公開鍵によって判別するため、それを隠し通せば匿名で使うことが出来る。これはビットコインの目的には準じているが、設計面では取引がオープンなため乖離が見られる。

〇二重消費とは何か
デジタルデータを本当の貨幣のように使うには、二重消費への対策が必要である。→コインのデータのコピーをまた使うことのないようにしなければいけない。コピーを使った場合でもハッシュ値などは正しく求められてしまう。
ビットコインでは特殊な対策を行っている。

〇ブロックチェインに正しい取引を埋め込む
ビットコインではネットワークで二重消費を監視している。
取引のデータをブロードキャストすることにより、取引をまとめてブロックチェインを形成する。
ブロックチェインないの取引では二重消費などの正しくない取引は拒否される。
ブロックチェインの大きさは年々大きくなっている。
古くなった不要なデータは捨てても良いように改善されている。

【コメント】
ブロックチェーンは、改ざんなどの不正を行うことが出来ない為、信頼をとてもおける技術であるといえる。この技術を使っていると企業は利用者に安心したサービスを受けてもらえるようになると思い、

(相田)p.7～p.11

【《マイニング》は何を保証する仕組み】

〇マイニングの正体はくじ引き
・1 度承認された取引方法が改ざんされることを困難にするため、ブロックチェーンのブロックの追加に、コストを設けている
・ ブロックは数学的な方法(マイニング 採掘)されなければならない。
・ブロックを作るのには大きな計算パワーが必要。

前のブロックと新しく作るブロックに、ハッシュ値(256bit)を格納。
☆新しいブロックに対して、ある値を暗号学的ハッシュ関数 (sha-256)に適応させて、それで得られたハッシュ値がターゲット以下(ネットワーク内で、もともと合意されている条件を満たす値)になるまで試していく。

⇓

二次方程式のようなもの

因数分解や公式を使って答えを出すことができる。
マイニングの場合
因数分解や公式というものが全く分からないのに答えをだそうとしている状態。つまり、適当に値をハッシュ関数に代入して答えを出す。

・適切な値＝ターゲット以下の値＝ナンス(32bit)なるように 0 から順にひとつずつ増やしながら試していきます。
32bit→ 2 進数の 32 桁
・適切な値 ナンスは 2 進法で表されている。

・0 から順に増やしていく人と、0 になるまで減らしていく人と、マイナーによって異なる。

・適切な値 ナンスが見つかったら、新しいブロックとしてブロードキャストします。

・他のコンピュータはその新しいブロックが正しいものなのか検証し、正しければチェーンの末尾として承認する。それから新しいブロックのマイニングを進めます。

・報道では複雑な計算と言われているが、この操作を簡単に表すとしたら「くじ引き」
・偶然、適切な値 ナンスが見つけられるように、確率を調整しながら、1 秒に何百億回というペースでマイナー達がくじを引いているようなもの。

〇マイニングは何を難しくするのか

・ターゲット(ネットワーク内でもともと合意されている条件)の値を小さくすると、「適切な値」ナンスを見つける時間が長くなる。これを使ってブロックが作られる時間を 10 分になるように調整している。

・調整は 2016 個のブロックが生成される事におこなわれる。2 週間ちょうどの間隔

・ビットコインにはネットワーク全体を管理する仕組みが入っていないため、これらのこと

は競争的かつ協調的なプロセスとして自律的に進行します。

・別々のブロックが同時にブロードキャストされたり、通信障害や遅延などの理由で、チェーンが分岐してしまうことがあるが、その場合、最長のチェーンが採用される決まりになっている。 ブロックが再計算され、改めて最長のチェーンの末尾に追加されることで問題はいずれ収束します。

・悪意のある利用者が取引を偽造する時、取引のデータを変更するのではなく、ブロックのマイニングの手続きもやり直さなければいけない。

ブロックの内容の変更→ハッシュ値が変わる→内容の変更をしたブロックに続く全てのブロックのマイニングをし直さなければいけない。

・善意の計算パワーが悪意の計算パワーを上回っているかぎり、システムの健全性は維持される。

・この悪用を防ぐ方法は一般的に POW(proof of work)と呼ばれている。多くのデジタル通貨のシステムが POW を採用している。

【コインが誕生するしくみ】

〇《マイニング》の報酬としての BTC
・マイニングの手続きに多くのコンピュータが参加しなければビットコインが成り立たなくなってしまう。
・ブロックをマイニングしたユーザーが報酬を獲得できるしくみになっている。
・ブロックに格納する先頭の取引を自分のアドレスに宛てられた取引にすることが許されている。
・BTC は総量が決まっているので、全てマイニングされたあとは、取引で生じる手数料のみが報酬になる。

〇減っていく報酬
・報酬で得られるコインは 4 年ごとに半分になる。鉱物資源が容易な所から掘り出され、じょじょに採掘が困難になり、コストが上昇していくことに対応している。

↓

コインの希少性が演出されている。

〇巨石貨幣との類似点と相違点
・ヤップ島の石貨は大変な労力をかけてパラオなどから運ばれてくる。その苦労の物語によって仲間達から価値を認められる。
BTC もマイニングによる莫大な計算をしたという物語が、マイナー達に価値が認められるともいえる。
・ヤップ島の石貨も BTC も、実体経済から見て生産的ではない。
・ヤップ島の石貨は所有権の移動のみが石に刻まれていく。
BTC も所有権の移動のみがブロックチェーンに刻まれていく。

二つの違い＝ヤップ島の石貨は仲間づくりのためであって、格差を生むためでにあるのではない。
BTC は希少性を持つようにしているため、権力を呼び込むしくみを内包している。

【コメント】
前にモナコインという仮想通貨に、一番最長のチェーンが採用されるのを悪用した事件があったことを思い出した。当時は何のことか分からなかったが、今回調べて少し理解することができた。ブロックチェーンは安全と言われているが、前の事件のように今後も悪用されることがあるかもしれないので、仮想通貨は少し危ないと思った。

(舘林)p.11～p.16

【システムに欠陥は？】

●貨幣のかたちを 360 度変え、欠陥を引き継ぐ
・貨幣自体の構造的欠陥を、ビットコインも備えていて、それは拡大されているともいえる。
・ビットコインには社会的保障がない。
→社会が新しい技術に対応しておらず、技術の側も社会的な保障の考え方を導入する下地がつくられていない。
→≪プライベートキー≫をなくしたらアウト

●ビットコインにたいして可能な攻撃

〇トランザクション展性を突いた“受け取ってない詐欺“
※トランザクション展性：署名データ自体は表現規則がゆるいところがあり、変えても取引自体の意味は変らず、検証を通過してしまう性質。
・ビットコインの取引データはデジタル署名されているため、改ざんがあった場合は署名に

より検出。
→取引データの全体に署名が掛かっているわけではなく、一部、変更しても検出されない箇所がある
・取引の識別子として取引データのハッシュ値を用いるが、ネットワークの中継点のどこかでトランザクション展性を突いた改ざんがおこなわれ、≪マイニング≫によりそちらが承認されると、送金者が識別子をキーに取引が承認されているか探そうとしても、≪ブロックチェイン≫のなかにその取引を見つけることができない。
→取引が承認されているかが確認できない。
・送金の受け手は、手元の情報を≪ブロックチェイン≫と同期させて、自分の≪アドレス≫宛の入金を確認するので、取引が成功しているかどうかが確認できる。
・受け手の入金されていないという虚偽に応じて 2 回送金する場合がある。
・送金側は、最初の取引は失敗しているのでそのコインは未使用だと勘違いし、取引を実行しようとすると、二重消費と判断されエラーになる。

○ネットワーク各所に潜伏する“シビル攻撃“
・ネットワーク上に自分で制御可能なコンピュータを大量に参加させ、他のコンピュータをウィルス感染させ、そこから参加させることで大きな影響をおよぼすことが可能になる。

○「世界」を分断する“エクリプス攻撃“
・P2P のネットワークのなかで中継の要となる複数の地点に自分が制御できるコンピュータを配置し、有効な配置ができたら中継する方向を変え、分断された≪ブロック≫を形成していく。
・分岐された≪ブロックチェイン≫が、取引が起きている世界と起きていない世界に分かれることになる。
・取引が起きていない世界でその取引に基づいた次の取引を行おうとすると、承認されないことになる。

○あと出しでほかの≪プール≫の作業を無効化する“利己的≪マイニング≫“
・ほかの≪マイニングプール≫に参加しているコンピュータに無駄な計算をさせることで、自分の≪プール≫が相対的に有利になる。
・利己的な≪マイニング≫を行う≪プール≫では、正しい≪ブロック≫が得られても、それをネットワークにブロードキャストすることを遅延させ、次の正しい≪ブロック≫を得るために、黙ったまま≪マイニング≫を継続する。
・ほかの≪プール≫からの≪ブロック≫のブロードキャストを察知した時点で、自分が得た連続する 1 個以上の≪ブロック≫をブロードキャストすることで、ほかの≪プール≫が≪マイニング≫した≪ブロック≫を無効化しようとする。

⇒ほかの≪プール≫よりも有利に報酬を得られるようになり、≪マイナー≫がほかから移ってくるようになる。
→計算パワーが増大すると、利己的な≪マイニング≫が成功する可能性がさらに高まり、さらに新たな≪マイナー≫を呼び込むことにつながり、最終的にネットワーク全体の計算パワーの過半数を掌握できる。

○過半数を占めなければなんでもできる？“51%攻撃“
・≪マイニング≫に参加する計算パワーの過半数を掌握すると、≪ブロックチェイン≫をより長く伸張させていくことができる。
→任意の取引を承認させることができる。

●最大の欠陥？―世界から切り離されると使えない
・ビットコインの取引はネットワークにより承認されなければ完了しない。
→インターネットにつながっていることが大前提
・大きな災害が発生して、通信インフラが破壊されたとき、ビットコインは使えない。
・政治的に国民がインターネットから切り離されたとき、ビットコインは使えない。
⇒インターネットへの安定した接続性がなければならない。

【コメント】
　表紙の筆者のコメントを見ると、筆者はビットコイン推奨派のように感じていたが、最後のしくみ編を読んでいると、ビットコインのシステムは複雑であるが故の危険性を孕んでいて、筆者はその危険性を理由にビットコインに反対の立場を取っている印象を受けた。