2018年9月22日　担当:中西朗子

＜ブロックチェーンとは＞

・分散型台帳を作る技術です。（ここではビットコインに基づいての話になります）

ブロックチェーンはビットコインに使われる技術として、2008年にサトシナカモト（匿名）という人物がインターネット上で論文を発表しました。

ブロックチェーンによる取引はすべて公開されます。それと同時にネットワーク上の不特定多数のコンピュータの管理下に置かれます。一部を改ざんしようと思ってもほとんど不可能に近いと言われています。

つまり衆目皆で見張っている状態P2P（ピアツーピア）方式です。だからこそ、ビットコインはじめ仮想通貨はその信憑性も高いのです。ブロックチェーンは全てのデータを上書き更新もせずに保存しています。

・ブロックチェーンとはどんな技術なの？

取引の参加者が不正を行いにくいようにたくさんの場所で同じ情報を保管している技術です。

例えば、A さんが B さんへ持ってもいないお金を送金しようとお金を多く持っているように見せかけても、Cさん Dさん、Eさんたちが持っている情報と照らし合わせ不正な情報とわかるようにしてます。

この技術を利用するために、ブロックチェーンの参加者はお互いに通帳を見せあい、自分と取引相手の監視だけでなく、第三者ももともとの記帳残高や取引記録を保存し監視下に置くことになります。

不正に遭わないために通常の取引であれば自分自身で確認作業をする必要があります。しかし、ブロックチェーンの技術を用いれば、監視に協力しているのはブロックチェーンに参加している全員であるため、参加者のコンピュータが自動的に不正でないことを確認し取引ができるのです。

・ブロックチェーンのブロックとは

トランザクション(取引データ)を集めたものです。例えば、Aさんの所持金が1BTCあり、B さんに0.5BTCを送金しました。ブロックに書き込まれたのはA さんが B さんに0.5BTC送金したという事実です。この時Aさんは送信時に電子署名をします。電子署名によってこのデータは送信者から正しく送信したものであることを証明することができます。

※ではどうやって残高の管理をしているかというと送金時に残高分のデータを自分あてに送る事でまかなわれています。

ブロックチェーン(厳密にいうとビットコイン)は、新しいブロックの生成に10分程度かかります。なぜかというとナンスによって暗号解読にそのぐらい時間がかかるよう無理やり計算量を調整しているからです。その間に世の中でたくさんの取引が行われると１つのブロックに入る取引量は限られているので、新しいブロックの生成待ち状態で取引成立が遅延してしまいます。

・ブロックチェーンのチェーンとは

延々と続くブロックの繋がりです。各ブロックには“複数の取引データ”” 前の取引データのハッシュ値 “” ナンス “が含まれています。ブロックを繋げるのに必要なのは１個前のブロックのハッシュ値です。

・ハッシュ値とは

ブロックチェーンにおいて使われているブロックを守っている暗号のことです。通常の暗号化の技術では元の単語を割り出されないようハッシュ値を利用しています。

ブロックチェーンが通常と違うところは、**元の単語を割り出すための計算式が用意された状態**で運用されています。元の単語を割り出されてはわざわざ暗号化した意味がないものと思われますが、ブロックごとにハッシュが仕込まれている事によって、仮に改ざんしようとしても悪事を働くのが難しいのです。

・ナンスとは

“number used onece“の略で一度きりの使い捨ての数字でブロックを生成するためには必要な数値です。

ナンスを求める手順は「前のブロックのハッシュ値」と「トランザクション（取引データ）を足し合わせて」ハッシュ化します。このデータを「ある一定以下のハッシュ値に変化させるナンス」を発見することです。

このナンスを求めるのには膨大な計算をしなければならないのですが、ビットコインではこの作業のことを**マイニング**と呼びます。ブロックチェーンを語る上ではマイニングは外せません。なぜならマイニングすることによってそして適切なナンスを一番に発見しその正当性がほかの参加者マイナーによって承認されたときにブロックチェーンにブロックが追加できるのです。それによって取引が完了するのです。

・マイニングとは

ビットコインの取引を処理し、分散型台帳（ブロックチェーン）を作成していく作業の事です。これらの作業をする事によってマイニングをする人（マイナー）は報酬を得る事ができます。

報酬ー<u>かかるコスト（設備費や電気代等）がマイニングの利益</u>になりマイナーは「ビジネス」としてマイニングを行います。

ビットコインの取引は「マイニング」という処理（検閲も含め）によってのみ承認されます。

例えば「A さん⇒B さんへ 1 BTC 送信」という取引が参加者（ノード）皆へ伝えられたとしても、それをブロックチェーンに載せる「マイニング」という作業（作業者のこと）を経なければその取引は完了する事はありません。ブロックチェーンに載って初めて取引は正当なものとして承認されます

マイニングをする人達によって取引が正当かどうか確認・承認をされブロックチェーンに載せられていきます。

つまりマイニングをする人が取引を確認する、という段階こそが取引を完了する為には必要なのです。

・ブロックチェーンのメリット

コスト削減　金融機関の国際送金の場合、送金元銀行、中継銀行、受取元の送金先銀行の存在があり、送金するだけで 2 つの銀行を経由して中間手数料と送金から着金の時間まで多くの時間を必要でした。この仕組みをブロックチェーンに代替えすると中継銀行不要、送金元、送金先の銀行は、即座に送金、着金が可能になります。銀行から見ればコスト削減依頼者から見れば安い手数料と時間短縮で送金を行うことができるようになります。

セキュリティの高さ　特定の部署や機関がデータを扱う中央集権的管理と異なり、分散管理できるブロックチェーンでは局所的なサイバー攻撃の心配もしなくてもよくなります。さらに保存されたデータが改ざんされることは事実上不可能であることから、関係者の不正も防ぐことが可能です。

・ブロックチェーンのデメリット

51%攻撃問題

ブロックチェーンは P2P 方式です。Peer とは対等という意味もをちノード（ブロックチェーンに参加している人）もマイナー（マイニングする人）も対等な人たちの集まりで第三者機関不在の環境です。しかし弱点もあります。ネットワークの過半数がマイニングを独占する状態で、問題は強者による独占にあります。今後、このマイナーが結託して過半数を占めたら、また悪意を持ちマイニングしたらブロックチェーンの信頼性は失われることでしょう。

今ビットコインのマイニングは取引増加によって熾烈な競争を生み、きわめて高性能なスペックのコンピュータと膨大な設備を持つマイナーのみがマイニング、ブロックを担当しています。

今後 51%攻撃は発生しないとも限りませんがこの対策は今のところないと言われています。

*****メ　モ*****

マイニングプールとは

単独で行うことが困難なビットコインなどの仮想通貨のマイニングを集団で行うグループのことです。

マイニングの貢献度に応じて報酬を支払います。

報酬を得るため計算力のあるコンピュータとそれを稼働させ続けるには膨大な電力を消費します。

これらを実現するには資金力と組織力が個人より有利であると考えられます。

しかしながら現在、特定のマイニングプールによってマイニングのための計算資源が集中しすぎる問題が発生しています。また、マイニング専用のチップまで開発導入しており、個人では到底かなわない状況になっているそうです。

ハッシュレートとは

・日本語に訳すると採掘速度の意味です。

ハッシュレートで第 1 位は中国です。マイニングプールのハッシュレートのシェア率（確率）の高いのがほとんどが中国なのには理由があります。中国には、コンピュータチップを作る企業が集結しており、マイニングプールを運営する，企業はコンピュータチップを開発する事業も持っているからです。

中国は世界最高のコンピュータを作れる技術があり、アメリカや日本よりも群を抜いているそうです。それゆえ、マイニングマシン専用のコンピュータを設計するのも得意としていることになります。

更に石炭などの資源により電気代が安く提供できる環境であるため、より少ないコストでマイニングを実施することが可能となります。ゆえにこれだけのシェアが獲得できるという仕組みです。