(1)ブロックチェーンって何？
ビットコインのマイニングとは何なのか？これを知るにはまずは「ブロックチェーン」の仕組みを知る必要があります。

ブロックチェーンとは、世界中のたくさんののコンピューターに、数珠つなぎに保存されたデータのことです。（このコンピューターのことを、専門用語では「ノード」と言いますが、ここではコンピューターと言います）

ここで大事なのは

①「ブロックチェーン」と呼ばれるように、データが「チェーン」のように連なって保存されているということ

②「世界中のたくさんのコンピューターにデータが保存されている。」ということ

という2つのポイントになります。

①昔から現在までの全部のデータを数珠つなぎに保存するブロックチェーン

まず、ブロックチェーンに保存される情報やデータはどのようなものなのか、見てみましょう。例えば、

「ウォレットXから、ウォレットYにビットコインを0.001BTC送金した。」（「BTC」は、「円」「ドル」のようなビットコインの取引単位）

「ビットコインのウォレット（財布）を新たに作成した。」

といった情報になります。

現金で取引をするときの流れは
(i)財布を用意する。
(ii) お金を財布に入れて保管する。
(iii) 財布からお金を出して払う。
となります。

ビットコインの場合は、
(i)ウォレットを作成する。
(ii)ビットコインをそのウォレットに電子的に保存する。
(iii)ビットコインを他の人のウォレットに送信する。
という流れになります。ビットコインも現金と全く同じです。違いは全部コンピューター上の電子データで取引されることです。

ビットコインのブロックチェーンには、こうしたビットコインの取引に関係する記録の全部が保存されます。

ビットコインは2009年1月に誕生してから、今、皆様がこの文章を読んでいるこの瞬間にも取引が続いています。

では、そうした取引データはどのように保存されるのでしょうか？

ここで考えなくてはならないのは、皆さんの手元にある円やドルといったお金がどこから来たのか、ということです。言うまでもなく、コインであれば、日本の造幣局でコインが作られて、銀行からいろんな人の手にわたり、皆さんの手元に来ています。お金は「天下の回りもの」と言われるように、お金が作られてから

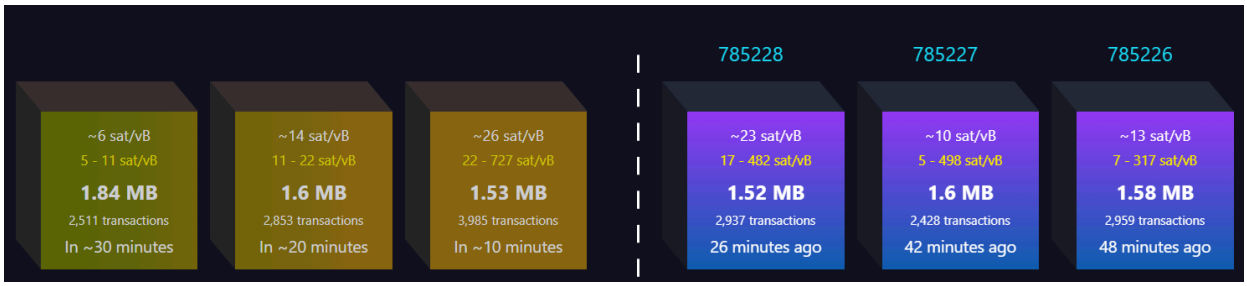
造幣局→○×銀行→ AB株式会社→Aさん→あなた

というような流れであなたの手元に来たわけです。
手元のコインは空気から生まれたわけでなく、造幣局からあなたに届くまでチェーンのようにつながってないとおかしいのが、わかると思います。

ビットコインも、これと同じように、ビットコインが作られるところから、今現在起きている取引（一番新しい取引）まで、一つのウォレットから別のウォレットに移動していくのを、チェーンのように数珠つなぎに記録をしていきます。その取引データをまとめて一つの電子的な「ブロック」に保存して、チェーンのようにデータを繋いでいったのがブロックチェーンなのです。

ビットコインのブロックチェーンは、だいたい10分おきに、新しい取り引きを保存した新しいブロックが、過去の取引すべてを記録しているチェーンに追加されされます。
数珠つなぎにブロックがチェーンのようにつながっているので、まさに「ブロックチェーン」ですね。

今現在のビットコインのブロッチェーンがどうなっているか、[このウェブサイト（Mempool.space）]で見ることができます。。この文章を書いているときのブロックは785,228個目のブロック（下の図の右側紫色のブロック）までが取引が確定されてチェーンにつなげられたブロックになります。



取引は開始されたが、未確定の取引が保存されているブロックが黄色のブロックになります。

一番左側の黄色のブロックが、取引内容が確定をすると、点線の右側に移動し、ブロックの番号が割り振られて取引内容が確定した青色のブロックになります。

②世界中のたくさんのコンピューターにデータが保存されているビットコインの取引データ
ては、ビットコインのブロックチェーンのデータはどこに保存されているでしょうか？

ここで、みなさんの手元にあるお金の取引データがどこに保存されているか、想像してみましょう。コインやお札は残念ながら、コインが作られたり、お札が印刷されてから、誰の手をわたってみなさんの手元に来たのか、データは保存されてないので、わかりません。
銀行にある貯金はどうでしょうか？銀行口座にあるお金は銀行が保管していて、それを誰に送金したのかデータが保存されてます。過去からのデータを見たければ、インターネットバンキングで取引記録をみたり、預金通帳を見たりします。銀行はこの取引データを万が一でも無くすことが無いように、大事に保管しています。コンピュータウィルスでデータが盗まれたり、地震でコンピュータが壊れたりしても、データが取り出せる

ようにコンピュータを複数の場所に分けて、それもセキュリティを厳重にして保管してます。銀行によってはその保管のために何百億円というお金をかけていると思います。
お金をかけているから安心、といわれれば、そうですが、もし、銀行が、取引データを保存しているコンピュータの場所の情報が漏れて、コンピュータが乗っ取られたりしたりしたら、みなさんの預金データは消えてしますかもしれません。可能性は低いかもしれませんが、コンピューターをテロリストが破壊したり、日本であちこちで大地震が来て、たまたまデータを保存しているコンピューターが全部壊れてしまう可能性もあります。

ビットコインの場合は、過去のすべての取引内容が保存されたブロックチェーンのデータが、世界中のコンピューターに保存されます。世界中のコンピューターが全く同じ取引データを保管しています。そのコンピューターの数は、2023年7月現在xxxxx台（出所：Bitnodes）です。
コンピューターといっても銀行が使っているような大規模なコンピューターではなく、みなさんのパソコンような小さいものでも保管ができます。
10万円もあれば、ビットコインのデータを保存するコンピューターを用意することができます。
つまり、ブロックチェーンのデータを保存しているコンピュータは簡単に増やせるのです。
世界中にたくさん散らばってるビットコインの取引データが保存されているコンピューターと、複数箇所にあるかもしれないが、日本国内に置いてある銀行のコンピューターのどちらが安全でしょうか？

この銀行とビットコインのコンピューターのちがいは、実はみなさんが使ってるインターネットそのものの仕組みと似ています。もともとインターネットはアメリカ政府の国防省が、アメリカの軍事・防衛に関する情報が集まってる国防総省が核攻撃されても通信が途絶えないようにするために考案されました。

アメリカもインターネットが考案される前は、銀行と同じように大規模なコンピュータでデータを集中管理・保存してました。インターネットができてからは、アメリカ全土に網（ネット）のように張り巡らせたコンピューター網で核攻撃に耐えられる通信ネットワークを作りました。その技術が一般にも開放されたのが、みなさんの使っているインターネットです。

ビットコインも、インターネットを使い、世界中のコンピューターを繋ぎ、次々に更新されるブロックチェーンの取引データを世界中のたくさんのコンピューターに送り、保存しているのです。核攻撃にも耐えうるお金、と言ったら言い過ぎでしょうか？

nn