Web3の基礎をなすブロックチェーンについて

2022年11月30日

株式会社 bitFlyer Blockchain

CTO 小宮山　峰史

bitFlyer Blockchain

ブロックチェーンで世界を簡単に。

Web3において大切なもの

　Web3には様々な特性がありますが、その多くはブロックチェーンテクノロジーに起源をもちます。それを端的にいうなら次のように言えるのではないでしょうか。
「Anonyumous な環境で信頼を作る」

そしてそれは大きく以下の3つから成り立ります。本ドキュメントではこれらを技術的に紹介していきたいと思います。

1	**データが改ざんされていないこと**
2	**権限を持つものによってトランザクションが作られていること**
3	**情報ソースが信頼できること**

１．データが改ざんされていないこと

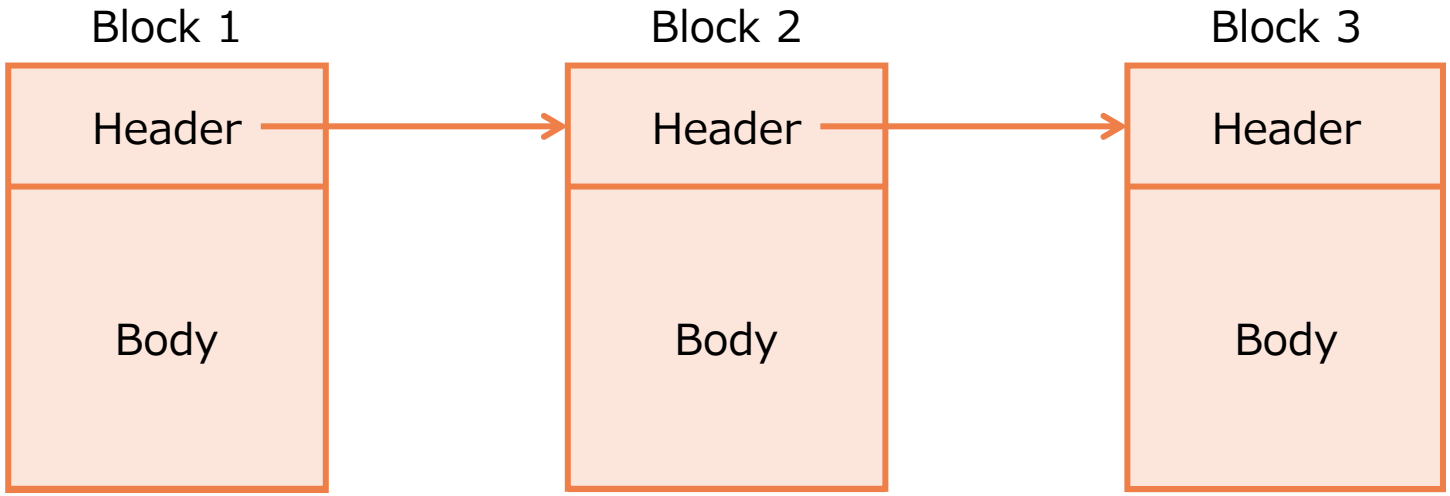
　これが最も分かりやすい特性です。
ブロックチェーンでは次の２つのテクノロジーを用いてそれを実現します。

1-1	**ハッシュチェーン**
1-2	**署名暗号**

１－１．ハッシュチェーン

ブロックチェーンという言葉は文字通りブロックがチェーンしていることからきています。さてブロックというのはデータの塊ですが、チェーンとは何でしょうか？
ブロックチェーンでは下図のように前のブロックのハッシュ値を次のブロックのヘッダーに含めます。これがブロックがつながっているように見えるのでブロック「チェーン」というわけです。

ここでポイントはつないでいるのは「ハッシュ」であることです。前のブロックのハッシュ値をヘッダーに書き込むことで、前のブロックの中身を変更するには次のブロックのヘッダーを変更する必要があり、それは再帰的にずっと続きます。
この性質によりブロックチェーンでは一部だけを変更することはできず、改ざんは事実上できなくなっています。



１－１．ハッシュチェーン（トランザクションとステート）

しかし実用上はいくつか問題が生じます。ブロックチェーンに保存するのはトランザクションです。ビットコインであれば

【A さんから B さんに 1BTC 送る】

のようなものです。このトランザクションそのものを改ざんしてしまうとすぐにばれるのですが、そもそも A さんが 1BTC 持っているかどうかは簡単には判定できません。

【A さんはいくら持っているか】

という情報（ステート）はそもそもトランザクションとして記載されないからです。残高がいくらか？という情報はすべてのトランザクションを実行した積み重ねの結果として初めてわかることです。

これは何が言いたいかというとブロックチェーンにおいて改ざんは困難だけれども、ステートが改ざんされていないことを確認するには過去のトランザクションの実行が必要になるということです。

もちろんこれは大変なことなので、ほかのサービス業者に依存することはできますが、そのサービス業者が信頼できるかどうかは、数学的に証明できることではないことを覚えておくべきです。

ブロックチェーンにおいて改ざんされていないことを確認するためには自分で計算する必要があります。なので PoS のように自分ではマイニングができないとしても自力でノードを運用することに意味はあります。

１－１．ハッシュチェーン（分岐・フォーク）

自力でノードを運営してても、ステートは改ざんすることができます。それはどちらも正しいトランザクションだけど相容れないものを作ることができるからです。
例えば 100 BTC しかもっていない人が A さんと B さんにそれぞれ 100 BTC 渡すというトランザクションを作ったとします。するとどちらかのトランザクションは失敗するのですが、そのどちらが失敗するかを決めるのはトランザクションの実行順序です。

先に実行されたほうが成功するというわです。
個々のトランザクションを正しいのに、トランザクションの順序を変えてしまえばステートは変えることができるということです。
ブロックチェーンではブロック内にトランザクションの順序も保存されているので順序も改ざんできないのですが、ブロックが二股に分岐するとそれぞれの歴史でトランザクションの実行順序が変わってしまいます。
だから歴史が分岐しないように、どの歴史が正しいのかを認定する必要があります。そのためにあるのが、コンセンサスアルゴリズムです。

コンセンサスアルゴリズムは重要ですが、もしステートに興味がなく、トランザクションの改ざん耐性だけあればよいというのであれば、コンセンサスアルゴリズムはなくても構いません。
その思想で作られたものに DAG と呼ばれる技術があります。

１－２．署名暗号

一度記録されたトランザクションの改ざん不能性についてはハッシュチェーンが守っていると説明しました。
しかしトランザクションを登録する前に一部の内容を書き換えたり、過去のトランザクションを一部書き換えて再送したりされることも改ざんの一種です。

この種の改ざんを防いでいるのは署名暗号技術です。トランザクションは秘密鍵により署名されます。署名をするとサインが作られますが、このサインは元のトランザクションを1ビットでも変えてしまえば正しくなくなります。（ハッシュと同じ性質です）
またサインには公開鍵が紐ついており、誰でもどの公開鍵で署名されたのかがわかります。なので偽物の公開鍵で署名してもすぐに正しくないことがわかってしまいます。

したがってトランザクションは正しい秘密鍵を持っている人によって作られたことが確実となります。なので第三者がトランザクションを改ざんすることはできません。

２．権限を持つものによってトランザクションが作られていること

RDB には様々な権限が存在します。なんでもできる DBA からログを閲覧する権限だとか、テーブルごとにクエリーをする権限を設定することも可能です。

ブロックチェーンにも同じように権限が存在します。例えばあなたのビットコインはあなたにしか操作できません。

このようにブロックチェーンの権限をレイヤを支える仕組みを2つ説明します。

2-1	**公開鍵**
2-2	**コンセンサスアルゴリズム**

２－１．公開鍵、その利点

ビットコインにおいて秘密鍵保持者しかそのコインを動かすことができないのは、そのコインが公開鍵に紐ついているからです。
RDBなど従来のシステムが ユーザーIDとパスワードによって権限を管理しているのに対し、ブロックチェーンでは公開鍵をIDとして署名をパスワードの代わりに使っています。
パスワードの照合のためには照合者が「パスワードを知る」必要があります。これは照合者が管理者的な立場であるのであればあまり問題になりませんが、Web3のような分散環境では難しい要請です。
それに対し、公開鍵暗号の署名のチェックは秘密鍵を外に漏らすことなく行うことができます。ブロックチェーンが分散環境に向いている大きな理由の一つがこの局所性であるといえます。

そして十分な記述能力のなるスマートコントラクトを使えば、コインを移動する権限だけでなく多彩な権限を表現することができます。仮想通貨においてはもっぱら所有権を表すだけの使い方が目立ちますが、Web3という世界では今後もっと多彩な権限が使われることと思います。

スマートコントラクト自身が権限を持つこともできます。例えばスマートコントラクトにコインを預けて条件に合わせて運用する、という DiFi のような使い方ができます。
この能力もWeb3においては重要なものとなるでしょう。スマートコントラクトは契約で、契約に従って何かを実行するときにスマートコントラクト自身がその権利を擁していればスムーズに事が運ぶからです。

２－１．公開鍵、その欠点

公開鍵をユーザーIDとし、秘密鍵をパスワードとするこの方法は前述のように利点だけでなく、大きな欠点もあります。

それは秘密鍵の紛失・盗難の際に原理的にリカバリーできないということです。

中央集権的にサーバでログイン処理をしていればパスワードの再発行も可能ですが、分散環境で局所的に公開鍵暗号で署名のチェックをしている以上、その秘密鍵を変えることができないからです。

もちろんスーパーユーザー公開鍵を設定して、その署名であれば何でもできる、などの対策は可能です。しかしそのようなスーパーユーザーを設定すること自体が分散の思想に反しているのは否めません。

また現在のインフラとして秘密鍵を利便性高く安全に管理するようなデバイスやソフトウェアはまだ充実していません。しかしインフラは技術革新で進化していきます。Web3が広まるにつれて徐々に利便性の高いものが使用可能になるでしょう。将来はスマホに秘密鍵管理モジュールが標準搭載されるかもしれません。

２－２．コンセンサスアルゴリズム

ブロックチェーンには署名鍵とは別の権限体系があります。それとはコンセンサスアルゴリズムのことです。
前節でも説明したようにコンセンサスアルゴリズムはトランザクションの順番を決めるためのアルゴリズムです。これはいいかえれば「順序を決める権限」なのです。

署名鍵は通常個人の権限を表現しますが、トランザクションの順序というのは特定の個人ではなくシステム全体で決めるものです。なのでビットコインなどの PoW ではコンセンサスアルゴリズムには秘密鍵は使いません。（しかし秘密鍵を使うコンセンサスアルゴリズムも存在します）
またパブリックチェーンは不特定多数のノードで実行されます。そのためコンセンサスアルゴリズムにはビザンチン障害耐性というものが求められます。これは一部のノードが悪さをして歴史を変えたりシステムを停止しようとしてもできない、という能力のことです。

権限という視点でコンセンサスアルゴリズムをみると、要は「誰が権限を持っているのか？」ということなのだと見えてくると思います。
PoW であれば計算能力を持っている人が権利を持っている、ということです。なぜそれでうまくいくかというと計算能力を提供してくれる人に対してインセンティブを与えているからだ（マイニング報酬）、ということがわかります。
ほかの PoX もそれぞれ権限を与える方法とそれを正しく運用させるための仕組みを一緒に作っています。ぜひその視点でブロックチェーンを再度確認してみてください。

３．情報ソースが信頼できること

一度ブロックチェーンに登録された情報は、改ざんされることもなく、正しい権限によって伝播していきます。しかし最初にブロックチェーンに乗せるデータはどうやって信頼を得るのでしょうか。

まず思いつくのは外部の権威を使って信頼すること（オラクル）です。

そしてもう一つはコンセンサスアルゴリズムなどによってブロックチェーン単体でデータを信頼することです。

3-1	**オラクル**
3-2	**コンセンサスアルゴリズム**

３－１．オラクル

ブロックチェーンには様々な情報を格納できます。そして一度書き込まれた情報は改ざんされることもなく、適切な秘密鍵を持つ人による署名によりその後の操作がなされます。つまり一度取り込んでしまえば「キレイな」情報になるのです。

しかし当たり前ですが、最初に書き込まれる情報が「キレイ」かどうかについてはブロックチェーンだけでは判定することができません。

食品トレーサビリティにブロックチェーンを応用しているとしたら、書き込まれた情報をあとから書き換えることはできませんが、そもそもその情報が正しいかどうかはわからないのです。

なので最初にブロックチェーンに情報を書き込むときには外部の権威を利用することになります。このときに利用されるのが VC (Verifiable Credentials) という証明書になります。

ブロックチェーンに情報を書き込むとにこの VC を使って署名をして情報を書き込みます。VCは SSL 証明書のようなものなので、ブロックチェーンであらかじめ認めた情報提供者（VCによって認められた人）の情報を信用することが可能になります。

VC は SSL 証明書のようにツリー状にチェーンすることも可能なのでいくつかのルート証明書を登録しておくことで柔軟な運用も可能になります。Web3時代には必須の技術になると思います。

３－２．コンセンサスアルゴリズム

ところで外部の権威に頼るしか「キレイ」な情報を書き込むことはできないのでしょうか？
中央集権でない仮想通貨においてまさに、通貨を発行という行為が「キレイ」であることが求められます。通貨の発行権をだれが持つのか？というのは最も難しい問題だったと言えます。

ビットコインにおいて、その答えはPoWなのですが、これはオラクルのように外部の権威に頼ることなく、純粋に数学と物理を信用する方式と言えます。
PoW において新しいコインを発掘するためには、ある関数を実際に計算してみるしかなく、それにはコストがかかり逃げ道はない、ということが事実であるからこそ成り立っています。
なので PoW においては現実世界で計算資源を持っておりそれを利用していることが、仮想世界であるブロックチェーン上で権利に結びつく、という現実と仮想世界を結ぶ魔法の役割を持っていると言えます。このことはブロックチェーンというテクノロジーが私のような技術者をひきつけてやまない一番の魅力的なところだと思います。

このようにコンセンサスアルゴリズムは全く異なる2つの価値をブロックチェーンにもたらしています。Web3時代には多くの人の投票により「キレイ」を決めるというようなアルゴリズムが現実化するのかもしれません。


bitFlyer