



① ブロックチェーンの基本と発展

高木聡一郎 (国際大学 GLOCOM)

ブロックチェーンとは何か

ブロックチェーンは、ビットコインを実現する過程で生まれた技術であり、最近もその著者が誰であるかが話題となった「サトシ・ナカモト論文」¹⁾で提唱された仕組みである。ビットコインから始まったため、金融あるいはフィンテックの文脈で語られることが多いが、ブロックチェーンは、より汎用的な活用を行える技術であり、最近では台帳管理からモノのインターネット (Internet of Things: IoT) に至るまで、広範囲な活用に期待が高まっている。

インターネットが単なる「情報」を繋ぐネットワークを作ったのに対して、ブロックチェーンはインターネット上で「主体や資産」を繋ぐネットワークを構成する。たとえば誰のコインなのか、どれだけの量なのか、そして誰から誰に譲渡されたのかといった価値の流通管理を得意とする。このような価値流通の側面から、ブロックチェーンを「主体に紐づく取引データが連結・凝縮された一連の電子ファイル」と定義することもできるだろう。まだ初期段階ではあるが、これからブロックチェーンが汎用技術として普及し、重層的に展開されていくことで、インターネットの上に構築されるもう1つの基盤技術になることが期待されている。

ブロックチェーンの3大要素

ブロックチェーンは進化が速く、また多様な側面を持っているが、多くの場合そこには3つの共通する要素が見られる。ここではこの3つの要素について概略を解説する。

第1の要素は、データの連結による偽造防止である。ブロックチェーンは、世界中の取引データを一定時間ごとに集約してブロックと呼ばれるデータのかた

まりを作成する。そして過去に作成されたブロックと連結していくが、そのときに過去のブロックの要素を次のブロックに入れていく。そのため、過去のデータを改ざんすると、新しいブロックまですべて改ざんしなければならない。これによって、過去の取引の改ざんが困難になる仕組みとなっている。

第2の要素は、主体と情報資産の紐付けである。たとえばコインの持ち主は公開鍵のハッシュ値で指定され、その公開鍵に対応する秘密鍵を持っていることを証明できれば、そのコインを使うことができる。ここでの主体とは、人や企業、組織などだが、モノのインターネットの場合は各デバイスにまで拡張することもできるだろう。

第3の要素は、不特定多数のコンピュータによる情報管理である。ブロックチェーンでは、どこか特定のクラウドやサーバに情報を保管しておくのではなく、多数のコンピュータで同じデータを持ち合っており、分散して管理する。そのため、特定の大規模なサーバが不要であり、またどこか1カ所のデータが失われても、ほかの参加者のコンピュータが動いていればシステムを維持することができる。こうした不特定多数によるシステム管理をピアツーピア (P2P) と呼ぶ。

技術的な実現方法

以上で見た3大要素を実現する技術的な特徴を簡単に紹介する (文献2) 等を参考)。

● データの連結

データの連結をもう少し詳しく見ると、図-1のようになる。

世界中でさまざまな取引 (たとえばコインによる支払い) が行われているが、こうした取引データを一定

間隔（ビットコインの場合は約10分）で集約していく。集約の際はハッシュ関数を繰り返し用いることで、その時間取引されたデータを最終的に1つのハッシュ値（ハッシュ木のルート）として集約する。このハッシュ木のルート値はブロックのヘッダに含まれる。

また、ブロックの連結においてもハッシュ関数を用いられる。前のブロックヘッダをハッシュ処理した値を、次のヘッダに含めるのだ。ハッシュ関数は、元のデータが変わると、生成されるハッシュ値も異なるものになる性質がある。

そのため、過去の取引データの一部でも改ざんされれば、ハッシュ木のルートも変更しなければならない。そして、ハッシュ木のルートが変更された場合は、その後連結されているブロックもすべて変更していかなければ、データの整合性が取れず、結局は改ざんしたことが検知されてしまう仕組みである。

● 主体と資産の紐づけ

一方、個々の取引データに着目しても、新しい工夫が見られる(図-2)。新しい取引データを作成するには(たとえば花子から次郎にコインを支払う)、花子はそれがどこから手に入れたコインなのか、そして誰に支

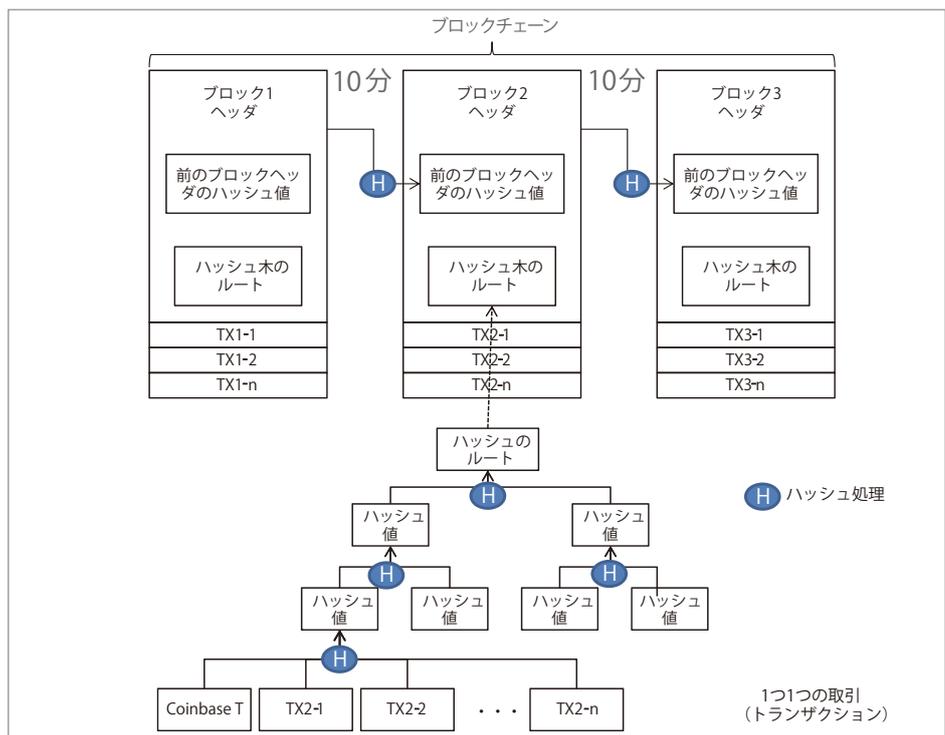


図-1 ブロックチェーンの全体像

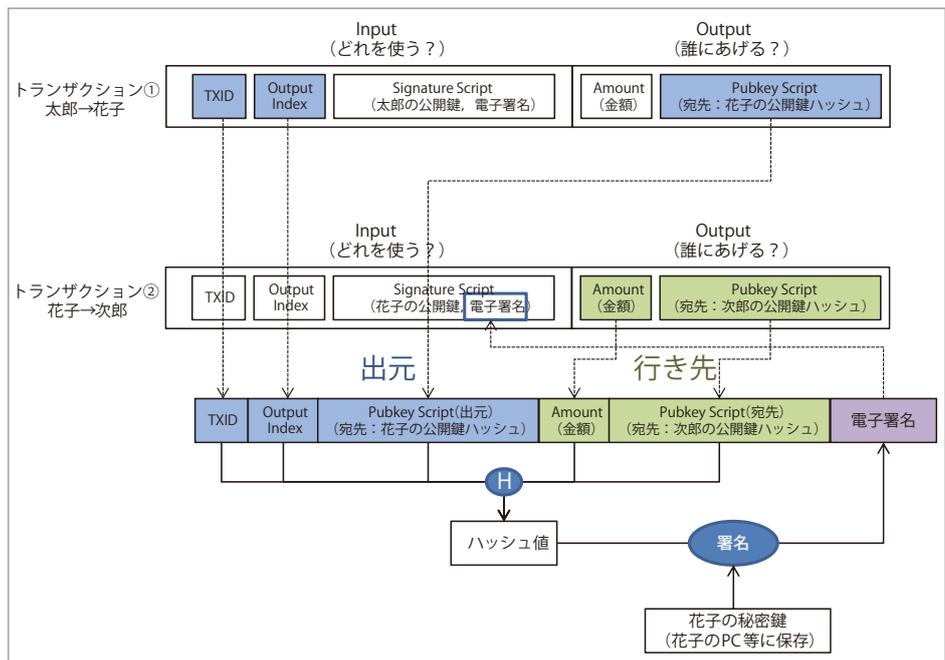


図-2 取引データの構造

払おうとしているのかをまとめて、公開鍵暗号方式を用いた電子署名を付与する。この方法により、コインの2重払いを防止するとともに、確実に資産の移転を行っていく。

● プルーフ・オブ・ワーク

ところで、ブロックチェーンではP2Pでブロック作

成の作業が担われる。世界中のどこでも新しいブロックを作成できるということは、異なるバージョンのブロックチェーンができてしまう可能性がある。これを解決するのが、プルーフ・オブ・ワークという仕組みである(図-3)。

ブロックを作成するコンピュータは、作成されたヘッダ部分のハッシュ処理を行う。その際、あらかじめ決められた閾値よりも小さな値にならない。元のデータからどのようなハッシュ値が生成されるか予測不能であるが、同じデータからは必ず同じハッシュ値が生成されるため、ナンスと呼ばれるランダムな値を付け加えながら、何度も何度もハッシュ処理を繰り返す。ビットコインの場合、この作業が平均10分かかると設定されており、これがブロックの間隔が約10分であることの原因だ。

こうしたブロック作成作業を全世界で競争しており、最も早く作成できたコンピュータが、世界に新しいブロックを提供する。もし、ほぼ同時に2つの異なるブロックができた場合は、その後続くブロックが長くなった方が正統とされる。

このような方式で、不特定多数のコンピュータによるデータ管理でも、どれが正しいブロックチェーンかの合意を取る仕組みとなっている。

ブロックチェーンの発展

●スマート・プロパティ

当初はビットコインの管理に使われたブロックチェーンだが、登場後から間もなく、より汎用的なデジタル資産への応用が検討され始めた。多くの金融商品、たとえば債券、株式、コマーシャル・ペーパーなどはデジタル化が容易なため、ブロックチェーン上での管理もしやすい。最近多くの金融機関で実証実験が行われているのは、こうしたデジタル化された金融資産をブロックチェーン上で管理しようと

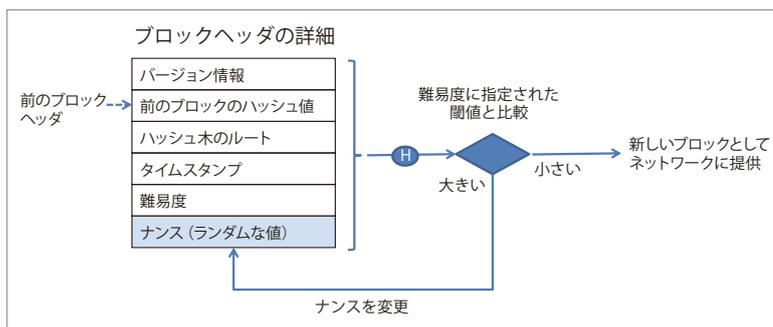


図-3 プルーフ・オブ・ワークの仕組み

種別	例
一般	エスクロー取引、担保付き取引、第三者裁定、複数者取引
金融取引	株、未公開株、クラウドファンディング、債券、投資信託、デリバティブ、年金保険、年金
公的情報	不動産登記、自動車登録、事業者登録、結婚証明、死亡証明
ID	運転免許、IDカード、パスポート、有権者登録
民間	借用証書、ローン、契約、賭け、署名、遺言、信託、エスクロー
各種証明	保険証明、所有証明、公証
有形資産の鍵	家、ホテルの部屋、レンタカー、自動車利用
無形資産	特許、商標、著作権、予約、ドメイン名

表-1 ブロックチェーンで管理できる可能性がある対象の例
出典：文献3)を元に作成(筆者訳)

するものだ。一方、実物資産でもデジタル情報とのリンクをうまく行えば、ブロックチェーンに載せることができる。たとえばエバーレジャー社は、ダイヤモンドの特徴をデジタル化し、ブロックチェーン上で持ち主を管理するサービスを提供している。こうした「管理対象の拡大」がブロックチェーンの進化の第一歩であり、上記以外にもさまざまなものが提案されている(表-1)。

●スマート・コントラクト

ブロックチェーンの原型は情報を載せる台帳のようなものであり、データを操作するのは基本的に外部のアプリケーションの仕事であった。しかし、徐々にブロックチェーン上にコンピュータ・プログラムを格納し、動作させることもできるようになっている。ブロックチェーン上にデータだけでなくプログラムも載せることで、デジタル資産を登録するだけでなく、資産の移転やそれに付随する業務を自動的に実行する「スマート・コントラクト」と呼ばれる仕組みが生まれてきた。

こうした仕組みを発展させ、汎用的にどのようなプログラムでも実行できるようにした仕組みが「イーサリ

アム」である。ここに至って、ブロックチェーンは資産を管理するための「台帳」という役割から、汎用的なネットワーク型コンピュータへと変わりつつある。ビットコインやイーサリアムに加え、現在では、Linux Foundation が主導する「ハイパーレジャー」などもあり、百花繚乱の様相を呈している。なお、ビットコイン、イーサリアム、ハイパーレジャーはいずれもそのソフトウェアのプログラムが公開されており、利用者が独自にブロックチェーンを立ち上げたり、カスタマイズすることが可能である。

ところで、ブロックチェーンは不特定多数のコンピュータにより維持されるオープンなものがその原型であるが、情報が外部に筒抜けになってしまうことや、不特定多数であるがゆえの処理速度の遅さなどに課題があった。そこで、クローズドの環境でブロックチェーンを使おうとする動きも目立ってきている。インターネットに対する社内イントラネットのようなものだ。クローズドにすることで、情報の秘匿性や処理速度を大幅に向上することができる。

多彩な活用可能性

ブロックチェーンの長所は、情報の偽造が困難、情報資産の流通管理を行える、障害が発生しにくい、中央管理者が不要などである。一方で、特にオープン型の場合は、情報の秘匿性が低い、処理速度が遅いといった弱点もある。これらの特徴を総合すると、どのような活用方法があるだろうか。

ブロックチェーンの耐偽造性や公開性を考慮すると、「秘匿性はあまり求められないが、偽造されては困るもの」などが検討の対象になるだろう。たとえば、公的機関が行う登記や事業所登録などがある。また、データの偽造・偽装問題への対策としても有効だろう。契約履行の確認と支払いを自動化するスマート・コントラクトが普及すれば、決算情報の偽装なども難しくなるかもしれない。

情報の流通管理という観点からは、資産の利用者または状態が変化していく際の管理に使えるだろう。たとえば、動画や音楽などデジタルコンテンツの流

通や課金、企業が保有するデータやソフトウェアなどの売買に使用することなどが考えられる。あるいは、電子書籍コンテンツの中古販売などもできるようになるかもしれない。

一方、耐障害性に着目すれば、万が一止まると大きな影響が出るシステムの利用には良いだろう。ただし、一般的なブロックチェーンは超高速の処理には向いていない。金融の基幹システムなど、ミリ秒を争う業務に適用するのは慎重に検討する必要がある。

分散型組織の登場

先に見たように、ブロックチェーンは中央管理者がいなくとも、ネットワークへの参加者が自主的にシステムの維持に貢献する仕組みを実現している。この特性を活かしたまったく新しいサービスも生まれつつある。たとえば、イーサリアムを活用した Colony というサービスは、フリーランスで働く人々が、互いに独立して自律的に仕事を受発注できるような仕組みである。

ブロックチェーンで実現するこのような形態の組織を、DAO (Decentralized Autonomous Organization) と呼ぶ。こうした組織形態は、各個人や参加者がプラットフォーム企業を介さずに、独立してほかの参加者と連携できるような仕組みの登場を示唆しており、今後の動向が注目される。

ビットコインから始まったものの、ブロックチェーンは情報管理の方法のみならず、新しいサービスから組織の作り方にまで、さまざまな応用可能性がある。今後の発展にも注目したい。

参考文献

- 1) Nakamoto, S. (unknown) : Bitcoin : A Peer-to-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf>
- 2) Antonopoulos, A. M. : Mastering Bitcoin, O'Reilly & Associates Inc. (2014).
- 3) Swan, M. : Blockchain : Blueprint for a New Economy, O'Reilly Media (2015) .

(2016年8月31日受付)

高木聡一郎 stakagi@glocom.ac.jp

国際大学グローバル・コミュニケーション・センター 研究部長/准教授/主幹研究員。東京大学大学院学際情報学府博士課程修了。博士(学際情報学)。専門は情報経済学。国際大学 GLOCOM ブロックチェーン経済研究ラボ代表。