# ブロックチェーン技術概要 ★1

**高木聡一郎**（たかぎ・そういちろう）

**国際大学 GLOCOM 主幹研究員 / 准教授**

## ブロックチェーン技術とは

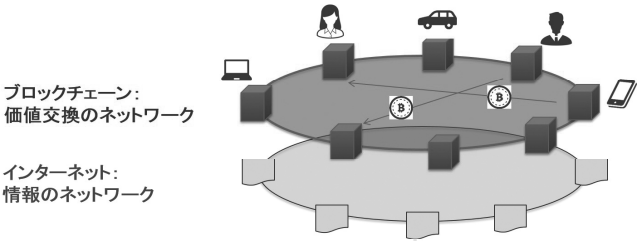
ブロックチェーンは，ビットコインを実現する過程で生まれた技術であり，その著者が誰であるかが現在も明らかになっていない「サトシ・ナカモト（Satoshi Nakamoto）論文」★2 で提唱された仕組みである．ビットコインから始まったため，金融あるいはフィンテックの文脈で語られることが多いが，ブロックチェーンは，情報管理に関する汎用的な技術でもあり，最近は台帳管理からモノのインターネット（IoT：Internet of Things）に至るまで，広範囲な活用に期待が高まっている．

まず，ブロックチェーン技術がどのようなものかを概観していこう．ブロックチェーンはまだ進化の過程にあるため，定義も定まったものはなく，様々なものが乱立している．その多くはブロックチェーン技術の仕組みに着目したものだが，ユーザーの視点からこの技術が実現することに着目すれば，筆者は以下のように捉えることができると考えている．

「ブロックチェーンとは，インターネット技術の上に構築される価値交換のための分散型インフラ技術である」（図 1）

ここには二つのポイントがある．一つは「価値交換」という点であるが，価値を交換するためには主体と主体の関係（誰から誰に価値が交換されるのか），そして主体と価値の関係（誰が持っている，どのような価値なのか）を定義する必要がある．ブロックチェーンは，こうした二つの関係性を定義することで，価値

図 1　ブロックチェーンの位置づけ




出所：筆者作成

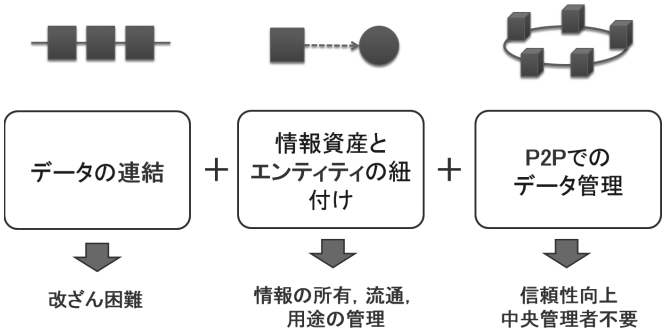
を交換することを可能にする．

もう一つのポイントは，「分散型のインフラ技術」という点である．上記の価値交換の仕組みが，特定の事業者（たとえば銀行や取引所）ではなく，不特定多数により運営されるインフラ技術として実現されるということである．インターネットが，世界中の様々な主体の連携により，世界規模での情報の交換を可能にしたのと同じように，ブロックチェーン技術は不特定多数の運営者の連携により，世界規模での価値の交換を可能にするものである．

## ブロックチェーンの 3 大要素と仕組み

ブロックチェーンには様々なバリエーションがあるが，多くの場合は三つの共通する要素が見られる．ここではビットコインを例に，この三つの要素について概観する（図 2）．

図 2　ブロックチェーンの 3 大要素

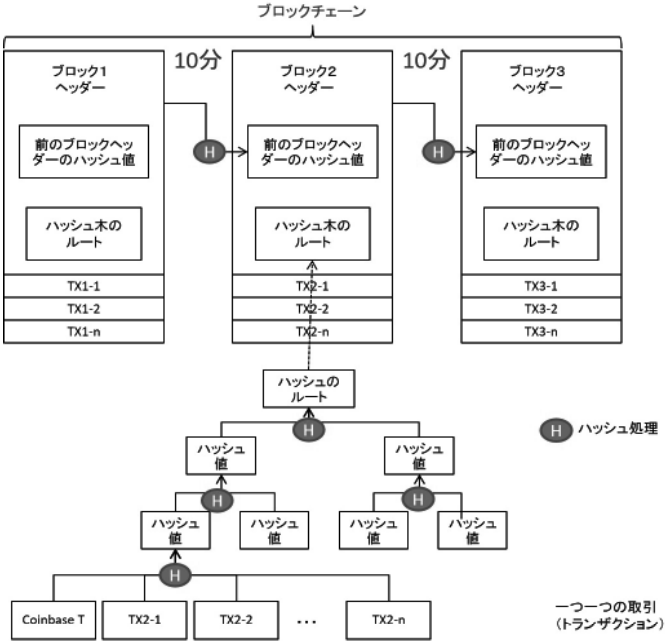



出所：筆者作成

第一の要素は，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，その時に過去のブロックの要素を，ハッシュ処理を活用して，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，過去の取引が改ざんできない仕組みとなっている．

もう少し具体的にブロックチェーンのデータ構造を示したものが図３である．ビットコインの場合は平均 10 分ごとにブロックを作成していくが，ブロックに取り入れる個々の取引データは，ツリー構造を伴うハッシュ処理を用いて集約される．ここで最終的に得られた「ハッシュ木のルート」と呼ばれる小さな値が，ブロックのヘッダー部分に組み込まれる．これによって，取引データのごく一部でも改ざんしようとすると,「ハッシュ木のルート」が変わってしまうことになる．

図３　ブロックチェーンの構造




出所：筆者作成

ハッシュ木のルートが変わると，それを含んだブロックヘッダーが変わってしまうため，それに続く後のブロックのヘッダーも変更しなければならないという仕組みである．このようにして，ブロックチェーンでは誰もが変更できるにもかかわらず，改ざんすると，そのことが他の利用者に見えてしまうという仕掛けになっている．

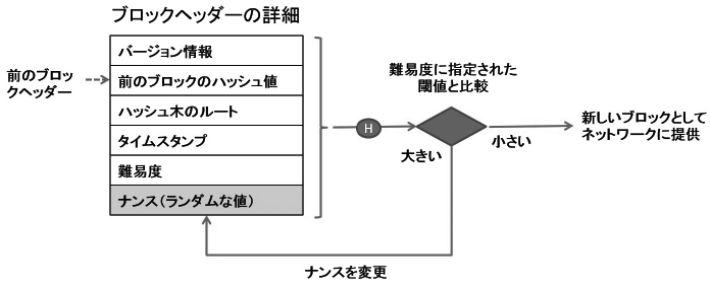
第二の要素は，主体と情報資産の紐付けである．たとえばコインの持ち主は公開鍵のハッシュ値で指定され，その公開鍵に対応する秘密鍵を持っていることを証明できれば，そのコインを使うことができる．ここでの主体とは，人や企業，組織などだが，モノのインターネットの場合は各デバイスにまで拡張することもできるだろう．新しい取引データを作成するには（たとえば花子から次郎にコインで支払う），花子はそれがどこから手に入れたコインなのか，そして誰に支払おうとしているのかをまとめて，公開鍵暗号方式を用いた電子署名を付与する．この方法により，コインの二重払いを防止するとともに，確実に資産の移転を行っていく．ちなみに，ここでの公開鍵には認証局による公開鍵証明書などは付与されない．あくまでも当事者が相手の公開鍵のハッシュ値を知ってさえいれば，送金できる仕組みとなっている（この公開鍵のハッシュ値がアドレスの役割を果たしている）．

第三の要素は，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き，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，他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：Peer to Peer）と呼ぶ．

この P2P システムで最も重要なのは，ブロック作成の作業である．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，場所によって異なるバージョンのブロックチェーンが出来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 4）．

ブロックを作成するコンピュータは，新たに作成されたヘッダー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ければならない．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

図 4　プルーフ・オブ・ワークの仕組み

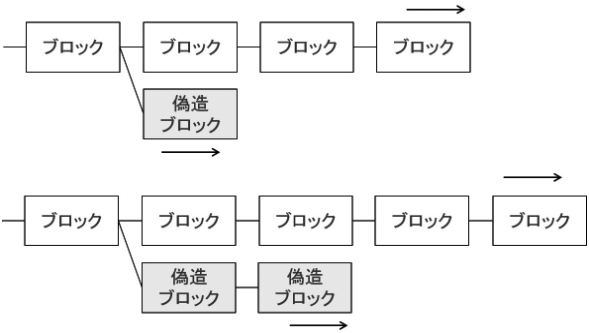



出所：筆者作成

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 分かかるように設定されており，これがブロックの間隔が約 10 分であることの理由だ．

こうしたブロック作成作業は，全世界で競争されており，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，ほぼ同時に二つの異なるブロックができた場合は，その後に続くブロックが結果的に長くなった方が正統とされる．また，仮に過去のブロックを改ざんして，ブロックチェーンを分岐させることがあっても，前述のプルーフ・オブ・ワークと呼ばれる処理を行わなければならないため，最新のブロックチェーンより長くなることは難しい（図 5）．これがプルーフ・オブ・ワークを行う理由であるが，電気代をはじめとするリソースの無駄遣いとの批判もあり，最近ではプルーフ・オブ・ステークなど

図 5　ブロックのフォーク




出所：筆者作成

他の方式も検討・採用されている．

なお，新しいブロックを作成できた人には，まったく新規のビットコインが発行される．このコインの新規発行が，ブロック作成作業を通じてブロックチェーンの維持・管理に参加しようとするインセンティブとなる．

## ブロックチェーンの基本的な長所と短所

ここまで見てくると，ブロックチェーンの基本的な長所と短所が浮かび上がってくるだろう．ブロックチェーンにも様々なバリエーションがあり，その技術も日進月歩で進化を続けているため，一概には言えない面もあるが，ブロックチェーンの基本的な仕組みから，その長所と短所は図６のように整理できる．

図６　ブロックチェーンの基本的な長所と課題

**公開されているデータでも偽造しにくい**
情報の共有に有効
**主体と情報資産の関係を論理的にリンク可能**
情報資産の管理に有効
**分散型ネットワークでデータを管理**
単一ポイントの脆弱性回避，インセンティブ

**取引の認証に時間がかかる**
ブロック間隔，10分など
**スケーラビリティの問題**
7tps / 単調増加 / 修正不可能
**情報の秘匿性・セキュリティ**
秘匿性，鍵の管理，異常時の処理

出所：筆者作成

長所から見ると，まずブロックチェーンは誰もが見たり更新したりできる「公開された」システムであっても，情報の改ざん・偽造が極めて難しいということだ．そのため，多数の関係者で情報を共有したり，多くの組織が連携して処理を行う際の基盤として使いやすいという面がある．また，先に見たように，情報資産と主体の関係を公開鍵方式でリンクしていくため，仮想通貨に限らず様々なデジタル化された資産の流通管理に使える．また，分散型のネットワークで処理を行うため，どこか一つのサーバがダウンしても運用を継続できることや，信頼できる第三者組織などがなくても，コインの発行を通じて不特定多数の関係者によ

りシステムを維持管理できるインセンティブが内在しているのも特徴である．

一方，どうしても一定間隔ごとにブロックを作成するため，データが確定するのに時間がかかってしまう．ビットコインの場合はおよそ 10 分であるが，後述するイーサリアムだと 15 秒弱と短縮されている．また，不特定多数のコンピュータで最新状況を共有しながら処理を行うため，どうしても大量のデータを処理しにくいという面がある．ビットコインの場合は 1 秒間あたり 7 取引が限界とされる．また，公開されたブロックチェーンでは，どのようなアドレスにいくら分のコインが送金されたかといった情報が他の参加者に見えてしまうほか，秘密鍵をどのように管理するか，秘密鍵を紛失した場合にどのように処理するか等，異常時の処理にも課題が残っている．ただし，こうした課題に対する解決策も急ピッチで検討されており，それ自体が一つのビジネスとなりつつある．

## 進化する技術と広がる応用可能性

以上で見た長所や短所は，基本的なブロックチェーンの仕組みに基づいているが，ビットコインの登場後，急速な進化を続けている．当初は仮想通貨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れば，ブロックチェーンに載せることができる．たとえばエバーレッジャー（Everledger）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，上記以外にも様々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

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

| 種別 | 例 |
|---|---|
| 一般 | エスクロー取引，担保付取引，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 |

出所：Melanie Swan [2015], *Blockchain*, O'Reilly を元に作成（筆者訳）

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，リナックス・ファウンデーション（Linux Foundation）が主導する「ハイパーレッジャー」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，ハイパーレッ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故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．こうした使い方は，「パーミッションド」や「許可型」とも呼ばれる．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．

## ブロックチェーンとビジネスモデル

先に見たように，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，公的に行う各種登録業務や，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課題も多い．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だろう．

註

★ 1――より詳細な技術概要については，高木聡一郎［2017］『ブロックチェーン・エコノミクス―分散と自動化による新しい経済のかたち』（翔泳社）を参照．

★ 2――Nakamoto, Satoshi [unknown], “Bitcoin: A Peer-to-Peer Electronic Cash System.” <https://bitcoin.org/bitcoin.pdf>（2017 年 6 月 15 日アクセス）