

# 第 1 部

## ブロックチェーン技術の歴史と展望

鎌田 光宣

### 目 次

1. はじめに
2. ブロックチェーンとは
  - 2-1 ブロックチェーンの定義
  - 2-2 ブロックの中身 トランザクション
  - 2-3 マイニング（採掘）
3. ブロックチェーンを支える技術 その1 ハッシュ関数
4. ブロックチェーンを支える技術 その2 暗号技術
  - 4-1 公開鍵暗号
  - 4-2 電子署名
  - 4-3 ウォレット
  - 4-4 送金の流れ
5. ブロックチェーンを支える技術 その3 分散システム
  - 5-1 分散ネットワーク
  - 5-2 合意形成の仕組み
  - 5-3 パブリック型とプライベート型
  - 5-4 フルノードと軽量クライアント
  - 5-5 メモリープールと未承認トランザクション

6. ブロックチェーンの歴史

7. ブロックチェーンの課題

7-1 安全性

7-2 スケーラビリティ

7-3 ハードフォーク

7-4 ダブルスペント（二重送金）問題

7-5 電力消費

8. ブロックチェーンのこれから

## 1. はじめに

ブロックチェーン技術の仕組みを活用したものの代表がビットコインやイーサリアムといった仮想通貨（暗号資産）である。国家が発行した普通のお金を法定通貨と呼ぶのに対し、ブロックチェーンのなかで流通するお金は仮想通貨と呼ばれている。このお金はどこの企業が発行したものではなく、管理している明確な組織がないにもかかわらず、しっかりと信用された取引を行うことができるのである。

「ブロックチェーンの登場は、インターネットの登場と同程度の大きなインパクトがある。」「ブロックチェーンは仮想通貨をはじめ様々な分野に応用でき、新しいビジネスのチャンスと輝かしい未来が待ち受けている。」「この世界的な波に乗り遅れることは国益を損なうことだ。」このような言葉をあちこちで目にする。一方で、ブロックチェーンは大量の電力を消費する、仮想通貨が犯罪に用いられる、サイバー攻撃によって資金が流出した、などの負のイメージもついてまわる。

本稿では入門知識としてブロックチェーンの概要、また、ブロックチェーンを理解するのに必要な知識として、暗号技術、ハッシュ関数、分散システムなどの概略を説明する。最後にブロックチェーンのこれからについて考察する。

## 2. ブロックチェーンとは

### 2-1 ブロックチェーンの定義

ブロックチェーンというものをイメージしやすいように表現したものが図1である。ある大きさのデータの塊（ブロック）がいくつもチェーン状に繋がっている。物理的なチェーンが存在するわけではなく、ブロックのヘッダー部に、直前のブロックがどれかわかるような情報が記載されているだけの繋がりである。ところが、ここに暗号技術や分散システムの技術を取り入れると、一度書き込まれたデータは、たとえシステム管理者であってもあとから改竄することはできないシステムができあがる。

ビザンチン障害耐性とは、分散システムの一部のコンピューターで、故障や動作不良、悪意のある攻撃による誤作動、管理者が悪意を持って行う記録の改ざんなどの障害（ビザンチン障害）が発生しても、分散システムの他の正常なコンピューターでは、記録や動作について正しい結果が得られる性質のことです。

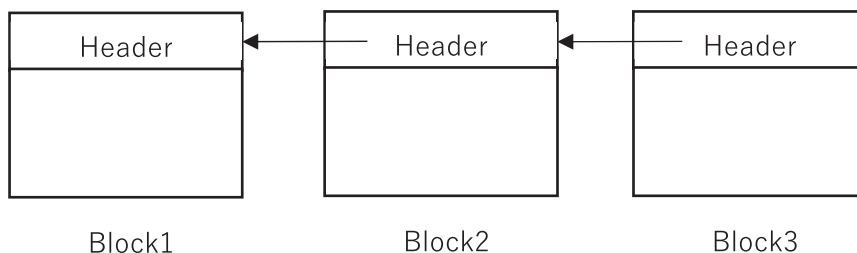


図1 ブロックチェーンのイメージ

日本ブロックチェーン協会によるブロックチェーンの定義は次の通りである。<sup>(1)</sup>

- 1) 「**ビザンチン障害**を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が0へ収束するプロトコル、またはその実装をブロックチェーンと呼ぶ。」
- 2) 「**電子署名とハッシュポインタを使用し改竄検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させること**で、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ。」

広義のブロックチェーンの定義を見ると、電子署名とハッシュというキーワードが出てくる。これについては3章および4章で説明する。ネットワークに参加するコンピューターはノードと呼ばれる。ブロックチェーンでは、多数のノードが同じデータを共有している。つまりデータを冗長化して保存して稼働しているため、どこかのノードやネットワークに障害が発生しても動き続けることができるシステムである。また、**改竄の検出が容易であるという特徴を持つ。**

狭義のブロックチェーンの定義を見ると、ビザンチン障害というキーワードが出てくる。これについては5章で説明する。ブロックチェーンは、時間の経過とともに合意が覆る（記録が変わる）確率が0に近づく仕組みを用いてシステムが設計されている。

ブロックチェーンの特徴を簡単にまとめると、次のようになる。

- － 分散型データベースである
- － **非中央集権型である**
- － 書き込み専用・改ざん困難である

非中央集権型というのは、中央の管理者がいない状態のことを指す。特定役割を持つサーバーが中央にあるわけではなく、**大量のユーザーがブロックチェーンを共有する状態である**。中央集権型とは違い、管理者が独裁的に管理するということができないため、利用者は信頼できない管理者の存在を気にしなくて良い。お互いに信用できない者どうしであっても、不正があることを心配することなく安心して取引を行えるという不思議な世界が登場するのである。

## 2-2 ブロックの中身 トランザクション

ブロックチェーンの中にはどのようなデータが書かれているのだろうか。1つのブロックには多数のトランザクションが含まれており、その中には、どの口座からどの口座にいくら送るか、という情報が書かれている。

**ブロックチェーン自体は残高を管理しておらず、利用者が誰なのか、残高はいくらなのか記載されていない**。利用者が自分の残高を知りたいときは、自分のウォレットアドレスに関する取引データを集めて、**未使用分の残高である UTXO (Unspent Transaction Output) を求める必要がある**。ある金額を相手に送りたいときは、送金するのに十分な残高のある UTXO を入力側に置き、送金したい相手のウォレットアドレスと金額を出力側に置く。入力側、出力側ともに複数の宛先を指定することができ、UTXO と送金額の差額は自分のウォレットアドレス宛に送るよう出力側に配置する。このときのトランザクションの中身は、送る側と受ける側との合計が等しくなっていなければならない<sup>1</sup>。ブロックチェーンには、この取引の記録が延々と綴られているのである。なお、電子署名、公開鍵、ウォレットアドレスについては4章で説明する。

トランザクション			
入力		出力	
自分の電子署名と公開鍵	100	相手のウォレットアドレス	65
		自分のウォレットアドレス	35

図2 トランザクションの中身のイメージ

1 手数料の扱いについては後述する。

## 2-3 マイニング（採掘）

ブロックチェーンでは、マイナー（採掘者）と呼ばれるノードがトランザクションを集めてブロックに詰め、それをブロックチェーンに追加する、マイニングと呼ばれる作業を行っている。マイナーは、ブロック追加の成功報酬と送金の手数料を手に入れることができる。

ビットコインのトランザクションの中身を見ると、必ずしも送る側からの入力と受ける側への出力が一致しておらず、その差額は手数料としてマイナーに支払われる報酬になる。この手数料の金額はトランザクションを作る人、すなわち送金する人が自由に決めて良いことになっている。手数料を0にしたり、安く設定したりすることもできるが、手数料が安いと、トランザクションをブロックチェーンに取り込んでももらえない（いつまでたっても取引が承認されない）可能性が高くなる。


ここで、ある値以下のハッシュ値が見つかる確率を採掘難易度と呼んでおり、これを調整することでマイニングの難易度を調整できるようになっている。ビットコインでは2016ブロック（約2週間に1回）ごとに採掘難易度が調整され、約10分に1つのブロックが生成されるように変更される。

なお、現在のビットコインはブロック追加の成功報酬が高く設定されており、多くのマイナーが競い合ってマイニングを行っている。この成功報酬は段階的に少なくなるよう設計されており、およそ100年後にはビットコインの発行上限に達してゼロになると計算されている。将来は成功報酬よりも取引手数料の割合が高くなり、発行上限に達した後は取引手数料のみがマイニングの動機となる。その際にビットコインを支えるネットワークがどのような振る舞いを見せるかは未知数である。

## 3. ブロックチェーンを支える技術 その1 ハッシュ関数

ブロックチェーン技術では、ハッシュ関数が様々な場面で登場する。ハッシュ関数（正確には一方方向ハッシュ関数）は、ある入力値に対して常に同じ値を返し、長さの異なる入力値を与えても常に一定の桁数が出力され、1ビットでも異なるとまったく関連性のない異なる値が得られるものである。これを「ハッシュ値」と呼ぶ（図3）。別の異なる値（データ）を入力したときに、同じハッシュ値を返すこともあり得るが、出力の桁数をある程度長くしておくと、故意に衝突（同じ値を返す）を起こすことは非常に困難である。このことから、オリジナルのデータのハッシュ値と手元にあるデータのハッシュ値を比べることで、同じものか異なるものかがすぐにわかるようになっている。

もとの値（文字列）	ハッシュ値
こ	B8f0mdh2c09t
こんにちは	Hr6KbKB3d4g7
こんにちは	Hr6KbKB3d4g7
こんにちはわ	vVd38ck2HcEr
こんにちは。今日は良い天気ですね。	1Aj3H1QuTv7y



同じ

図3 ハッシュ値のイメージ

ハッシュアルゴリズムはいくつも提案されており、新しく開発されたものほど別の異なる入力値で同じ値を返す可能性が低く、言い換えるとセキュリティの強度が高くなっている。

ブロックチェーンでは、保存されているデータの耐改竄性を担保する仕組みとしてハッシュ値が用いられている。ブロックの中には多数のトランザクションが格納される。トランザクションの中身には、送信者の電子署名と公開鍵、送金する金額、送金先のウォレットアドレスなどが含まれる。これらのトランザクションに加え、前のブロックのハッシュ値と、さらにノンス（Nonce）と呼ばれる値を加えてハッシュ値を求める。これらはすべてブロックの中に取り込まれ、永久に保管されることになる。途中のデータの改竄を行おうとしても、1ビットでもデータが変わるとそのブロック以降に含まれるハッシュ値がすべて不整合を起こすことになるため、不正を行うことは事実上不可能である。

ビットコインでは、ハッシュ値の先頭が所定数の「0」の並びになるノンスを求める作業を各ノードで行っている。ノンスを変えて、何度も何度もハッシュ値を求め、ハッシュ値の先頭が所定数の「0」の並びになるノンスを発見すると、ブロックを追加し、コインを新規発行することができる仕組みになっている。この作業はマイニング（採掘）と呼ばれ、時間と電力をかけて行っている処理の正体である。

## 4. ブロックチェーンを支える技術 その2 暗号技術

### 4-1 公開鍵暗号

私たちが鍵と言ってイメージしやすいのは、文書を暗号化するための鍵と、暗号文を復

号化する鍵が共通のもので、これは「**共通鍵暗号**」と呼ばれる。暗号化された文書は共通鍵を入手することで誰でも復号化できる。

それとは異なり、ブロックチェーンでよく用いられるのが、「**公開鍵暗号**」である。これは、秘密鍵と公開鍵の2種類の鍵を生成して文書を暗号化する方式で、公開鍵を用いて暗号化した文書は秘密鍵でのみ復号化できるというものである。**あらかじめ公開鍵を通信先の相手に渡す必要があるが**、このとき、公開鍵は誰の手にわたっても安全とされる。共通鍵暗号方式に比べて、公開鍵の共有が容易なことや、相手の数に関係なく公開鍵は1つでよいなど、鍵の管理が容易で安全性が高い。

重要なのは、公開鍵を用いて暗号化した文書は、秘密鍵でのみ復号化でき、公開鍵では復号化できないという点である。この仕組みを利用して文書を送る手順を以下に示す。

- 1) 受信者は、**あらかじめ秘密鍵と公開鍵のペアを作成する**
- 2) 公開鍵を送信者に送る
- 3) 送信者は文書を受信者の公開鍵で暗号化する
- 4) 送信者は文書を受信者に送信する
- 5) 受信者は受信した文書を受信者の秘密鍵で復号化する

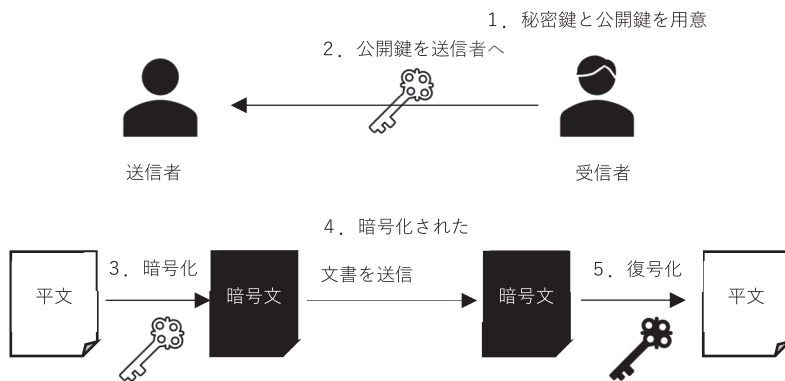


図4 公開鍵暗号

#### 4-2 電子署名

電子署名はデジタル文書の作成者を証明する技術で、公開鍵暗号とハッシュ値の性質を利用して利用している。電子文書を送信する際、送信者の秘密鍵で文書のハッシュ値を暗号化して電子文書に添付する。受信者は、送信者から受け取った電子文書と、添付されてきた電子



署名を組み合わせることで検証する。署名部分が送信者の公開鍵で復号化できなければ別人の署名である可能性がある。また、受け取った電子文書のハッシュ値と比較し、ハッシュ値が異なれば内容が改竄されていることになる。

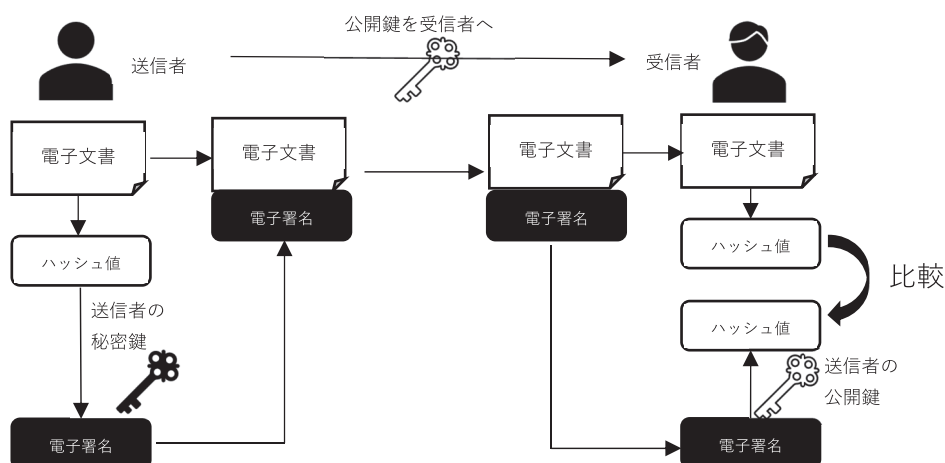


図5 電子署名

### 4-3 ウォレット

「ウォレット」には大きく分けて2つの意味がある。ひとつは、モバイルアプリやウェブサービスが提供する残高照会や送金などの機能のこと。もうひとつは、秘密鍵と公開鍵をもとにして、数学的に導出されたウォレットアドレスのことである。

ウォレットアドレスを使って取引を行うためには、どこからどこへ送金を行うのかを明確にする必要があり、お金を受け取るための（送り先の）アドレスを用意する必要がある。乱数列から秘密鍵が作られ、公開鍵は秘密鍵から生成される。そして、公開鍵からウォレットアドレスが生成される。以前は、1つのウォレットアプリに対して1つのアドレスが割り当てられるような運用が主流だったが、最近では、より安全な取引をするため、1つのウォレットアプリがたくさんのウォレットアドレスを持つという使い方が一般的である。ブロックチェーンに記録されたトランザクション（取引の記録）は、すべて誰でも見られるようになっているため、1つのアドレスだけを使って何度も取引を重ねると、頻繁に取引していることが誰の目にも明らかになってしまい、攻撃の標的になりやすいためである。取引ごとにウォレットアドレスを生成するため、多数のアドレスを管理する必要がある。

なお、ウォレットアドレスの鍵がなんらかの理由で失われたり破損したりしてしまうと、

ウォレットアドレスに二度とアクセスできなくなり、管理している資金が失われてしまう。ウォレットの管理方法として、ホットウォレットとコールドウォレットの2種類がある。ホットウォレットとは、ウォレットアドレスの鍵をインターネットに接続された状態で保管するタイプのウォレットのことをいう。利便性の高い保管方法であるが、不正アクセスなど鍵を失う危険性もある。コールドウォレットとは、ウォレットをインターネットから完全に切り離された場所に保管することで、不正アクセスによって鍵が盗まれる危険性を大幅に下げることができるものである。コールドウォレットの種類としては、紙に印刷して管理する「ペーパー・ウォレット」や、専用デバイスで管理する「ハードウェア・ウォレット」などがある。

#### 4-4 送金の流れ

デジタルの資産はいくらでもコピーできるため、法定通貨とは異なる仕組みが必要となる。まず、公開鍵から生成されるウォレットアドレスに残高があるとする。そのアドレスから支払いをする時は、そのアドレスの秘密鍵を持っている所有者が秘密鍵を用いて電子署名を添付する。他の人は、その電子署名と公開鍵を使い、その電子署名が秘密鍵を持った人が行ったこと、および電子署名された後に本文が改竄されていないことを確認することが出来る。具体的な送金の流れは以下になる。

- 1) 受信側が公開鍵と秘密鍵のペアを生成する
- 2) 受信側が公開鍵からハッシュ値を求め、ウォレットアドレスを生成する
- 3) 送信側が、取引データとして残高やウォレットアドレス等の情報を含めて、秘密鍵を使って署名する
- 4) 送信側が、ネットワークに取引データを流す
- 5) ネットワークの各ノードは、取引内に含まれる公開鍵と署名済みの送金情報を照合して取引が正しいことを検証する

## 5. ブロックチェーンを支える技術 その3 分散システム

### 5-1 分散ネットワーク

ネットワークに接続されたコンピューター（ノード）が1対1で接続して通信を行う方式をP2P（Peer to Peer）という。P2P形式の接続を行うノードがたくさん集まると、

安全で公平な金融システムの実現に資する FinTech フレームワークの提案

それぞれが P2P 方式で接続された状態の P2P 分散ネットワークが形成される。中心となるサーバーが存在せず、一部のノードが特別な役割を持つことがないため、一部のノードが故障や停止しただけでは全体に影響を受けることは少ない。すなわち、「単一障害点」を持たない。また、規模が大きくなればなるほど耐障害性に優れていく。

ブロックチェーンのネットワークでは、参加しているノードのすべてが同じデータを保持しているため冗長性が高い。あるノードが初めてブロックチェーンのネットワークに参加する際には、他のノードからデータをコピーする。同じデータを参照していることを保証・検証するため、データのハッシュ関数の値を確認しながら、1つ1つのブロックをコピーしてゆく。

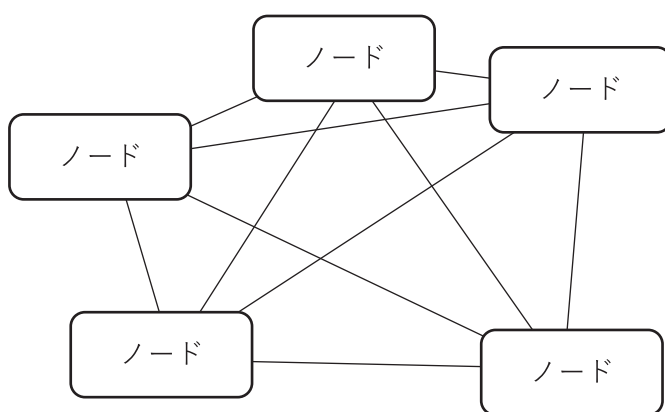


図6 分散ネットワーク

## 5-2 合意形成の仕組み

ブロックチェーンでは、正しいブロックやトランザクションを検証し、1つのブロックに対して全ノードで合意（承認）したうえでチェーンに加えることが必要になる。ブロックチェーンでは、原則としてすべてのノードがいっせいに同じ仕事を行うが、一部のノードが異なる結果を出すことがある。その際、多数決をとれば良いが、パブリックチェーンの場合は総ノード数が不明であることが多い。

さて、コンピューターネットワークの世界には「ビザンチン将軍問題」という問題がある。これは、中世の東ローマ帝国から取った名前である。ビザンチン帝国群には複数の将軍がいて、彼らの合議によって作戦が決定されるのだが、将軍の中に反逆者が存在する可能性があり、どのような対策を講じれば良いのかを考えるという問題である。ビザンチン将軍問題に帰結される故障や障害をビザンチン障害という。また、ビザンチン将軍問題が

発生しても全体として正しく動作するシステムをビザンチン・フォールトトレラント性 (Byzantine Fault Tolerance) があるという。

参加者の母数があらかじめわかっているブロックチェーンでは、リーダーを決めて合意を行うパターンが合理的である。分散型のシステムにおいては、いったんリーダーが回答の提案をして、それに対しての是非を問う多数決型の合意形成がとられる。

ところが、参加者の母数があらかじめわからないブロックチェーンでは、多数決型の合意形成をとることが難しい。このような、不特定多数の参加者による合意形成を実現するための仕組みとして、正しい選択をした者が経済インセンティブの行使権を獲得できる仕組みが生み出された。このような合意形成の仕組みを「PoW (Proof of Work)」や「PoS (Proof of Stake)」と呼ぶ。また、この方法を「ビザンチン・フォールト・トレランス (BFT) アルゴリズム」と呼ぶ。

ブロックチェーンで用いられている PoW (Proof of Work) は、元々はスパムメール対策として、メールに計算の証明を付与するという形で考えられたものである。ブロックチェーンには、複数の異なる処理結果が同時並行的に出されることがある。そうすると、チェーンが複数に分かれ、ブロックチェーンが分岐してしまう。このとき、各ノードが自分の計算結果に照らし合わせ、正解だと思う方のブロックチェーンを伸ばしていく。新規生成されたブロックを PoW の結果も含め各ノードで検証し、有効なブロックであれば、各ノードが自分のメインチェーンに追加する。分岐したうち、よりはやく伸びた方が正しい結果のチェーンであるとされ、仮想通貨の新規発行権や手数料が得られ、逆に、もう片方に分岐したチェーンは無効化される。すると、ノード全体がインセンティブに導かれ、自然と正しい結果に収束してゆくというものである。正しい計算結果にも拘わらず、ブロックチェーンに反映されない場合もあるが、悪意を持って結果を書き込もうとする者を結果的に排除できる。

PoW では、一度短くなったブロックチェーンの合意を取り戻す作業は容易ではない。ブロックが承認されてから時間がたてばたつほど、攻撃が難しくなる。ビットコインでは、一般的に6回以上のブロックが承認されるまで待つことが推奨されている。

なお、PoW は次の3つの問題を抱えている。

- 1) 悪意のある攻撃に弱い
- 2) マイニングによる電力消費・コストが高い
- 3) 取引にかかる時間が長い

このような PoW の課題を改善するための仕組みとして PoS が生まれた。PoS は、保有している通貨の量に比例して、新たにブロックを生成・承認する権利を得られる仕組みである。PoS のブロックチェーンを攻撃するには、過半数のコインを保有する必要がある、これを手に入れようとするコストが高くなるため悪意のある攻撃に強いとされる。また、マイナーが大量の計算をしなくて済むため、消費電力が抑えられる。さらに、PoW に比べて計算に割かれる時間が少なく済むため、ブロック生成速度を速めることができる。その結果、1 秒当たりのトランザクションが増える。

しかしながら、新たな問題点も存在している。コインの保有量が多いほどブロック生成に成功しやすくなるという性質から、多くの人がコインを使用せずに溜め込んで保有量を増やそうとする。そうすると、コインの流動性が低下してしまう。また、コインを保有しているだけでブロックが生成できるため、リスクなく、フォーク(分岐)したブロックチェーンに対してブロック生成ができてしまう。

この対策として、イーサリアムでは、間違ったブロックに投票した場合にデポジットを没収する仕組みで、正しいと思う 1 つのフォークのみを承認する仕組みを導入した。また、NEM では PoI (Proof of Importance) というアルゴリズムが用いられている。これは、コインの保有量、取引量、取引回数などから総合的にスコアを出し、スコアの高い人にブロック生成権が付与される仕組みになっている。

### 5-3 パブリック型とプライベート型

ビットコインはパブリック型ブロックチェーンのひとつである。パブリック型ブロックチェーンは、誰でも好きなようにノードを立てることができ、参加も離脱も自由である。ノードの数が増えるほど、システムが停止する可能性が低くなり、不正・改竄に対して強くなる。しかしながら、ネットワークの維持にはインセンティブが必要であり、マイニングに成功した人に使用权を与えることにしている。これが仮想通貨(暗号資産)である。

一方、プライベート型ブロックチェーンは、ネットワークの参加者が限られている状態で、一般には、全体で何台のノードがあるかもわかっているシステムを指す。ノードの数が少なく、全体の動作が早い、中央集権的な部分が残るため、ブロックチェーンを使う意義が薄れるともいわれる。

### 5-4 フルノードと軽量クライアント

ブロックチェーンでは、フルノードと呼ばれていたものが現在では「アーカイブノード」と「剪定ノード」の2種類に分類されるようになった。アーカイブノードは完全なブロッ

クチェーンのコピーを持つノードで、本来の意味でのフルノードにあたるものである。

アーカイブノードは一番先頭のブロック（Genesis Block）以降、最新のものまで、すべてのブロックとトランザクションを持つノードである。アーカイブノードはすべてのトランザクションを保持しているので、ほかのノードに頼ることなく単独でトランザクションの検証を行うことができる。有効なトランザクションのみを転送し、無効なものはその時点で破棄することで、ネットワークの維持に貢献する。アーカイブノードを運用するには、フルサイズのブロックチェーンのコピーを保存するだけのディスク容量と処理能力が必要になる。

アーカイブノード以外のノードは、すべてのブロックをダウンロードしたいときや手元がないトランザクションを確認したいときなど、フルブロックチェーンを持つアーカイブノードに問い合わせデータを送信してもらうことになる。

剪定ノードは、立ち上げの際に始めはいったんフルサイズのブロックチェーンを保持するが、過去の不要なトランザクションやブロックは捨て、UTXO と直近のブロックのみを保持する。剪定ノードは過去全てのトランザクションを検証することはできないが、二重支払いの検証は単独で行うことができる。

軽量クライアントは、ブロックチェーンの一部のみを保持するノードである。SPV（Simplified Payment Verification）という簡易的な方法でトランザクションの検証を行うため、SPV ノードと呼ばれることもある。軽量クライアントでは、ブロックヘッダのみを保持しておき、UTXO の集計の際やトランザクションの検証時などには、必要に応じてほかのノードに足りない情報を問い合わせ処理を行う。

アーカイブノードは他のノードに頼ることなく、単独でトランザクションの検証を行うことができるため、アドレスなどを他のノードに漏えいすることなく運用できる。また、どのトランザクションがアーカイブノード自身に関わるものか特定される可能性が低くなるため、プライバシーが守られやすい。しかしながら、ブロックチェーンの完全コピーをダウンロードするために数百 GB のストレージが必要になり、またブロックチェーンを同期させるため常時ネットワークにつながっている環境を用意するなど、大きなコストがかかる。

## 5-5 メモリープールと未承認トランザクション

フルノードはブロックに追加されていない未承認トランザクションを保存している。この未承認トランザクションを一時的に保管しておく領域を「メモリープール」と呼ぶ。メモリープールの容量はノードによって変わる。



マイナーは、メモリープールに溜まっている未承認トランザクションからブロックに追加するものを選び、マイニングして新たにブロックを生成する。マイナーにとっては手数料が高額に設定されているトランザクションから優先的にマイニングする方が儲かるので、手数料が高いトランザクションが優先的にプールから取り出され、マイニング対象となる。手数料だけを基準にしてしまうと、手数料が低いトランザクションはいつまでたっても処理されないことになってしまうため、トランザクションの年齢も加味して判定されている。ただし、確実に自身のトランザクションをマイナーに処理してもらうためには、トランザクション手数料を高めに設定する必要がある。

## 6. ブロックチェーンの歴史

ブロックチェーンの元となったアイデアは、1991 年の Stuart Haber と W. Scott Stornetta の研究<sup>(10)</sup>に遡る。デジタル文書にタイムスタンプを付けることによって、日付が遡ったり、改竄されたりを防ぐというものである。このシステムでは、暗号化され、鎖のように繋がったブロックを使用してタイムスタンプの付いた文書を保存し、複数の文書を 1 つのブロックにまとめることが行われた。

PoW (Proof of Work) という言葉は 1999 年の Markus Jakobsson と Ari Juels の論文に登場した<sup>(11)</sup>。サービスを受ける側に、コンピューターによる処理時間を要求することで、DoS 攻撃や迷惑メールの送信を抑えようとする仕組みである。2004 年には Hal Finney がリユースブル Proof of Work (RPoW) と呼ばれるシステムを発表した。Web サイトのユーザーが使用した PoW トークンを、新しい未使用の RPoW トークンと交換でき、その後同様に RPoW トークンの受け入れ態勢が整っている第三者のウェブサイトで使用できるというものである。

ビットコインの始まりは 2008 年に Satoshi Nakamoto と名乗る人物が発表した論文<sup>(12)</sup>である。最大の特徴は、中心となる運営者が存在しないということである。2009 年 1 月にビットコインの最初のブロックが採掘された。そして、ビットコインのブロックチェーンをもとに、アルトコイン (Altcoin) と呼ばれるコインが登場した。当初はビットコインのソフトウェアをベースにして、アルゴリズムやブロックサイズなどのパラメータを変更しただけのものが多く作られたが、のちにはより複雑な仕組みで、ビットコインのチェーン上にデータを乗せる形で運用されるコインが作られた。

その後、ブロックチェーンにさまざまな機能を持たせて仮想通貨以外の分野にも応用し

ようとする動きが起こる。イーサリアムは、ループ処理などを含む複雑なアプリケーションを開発し、実行できる機能を実現した。イーサリアムのチェーン上で実行されるプログラムはコントラクトと呼ばれ、金融以外の分野のアプリケーションも開発が進められている。このようなブロックチェーン上で稼働するアプリケーションを、分散型アプリケーション(DApps)と呼ぶ。さらに、イーサリアムの機能を利用することで、イーサリアムのブロックチェーン上でオリジナルの仮想通貨を簡単に作成・発行できるようになった。これにより、新たな仮想通貨が爆発的に増えることになった。

ビットコインやイーサリアムは、誰でも参加可能な、パブリックなブロックチェーンである。その後、プライベートチェーンと呼ばれる、参加者が許可制のブロックチェーンが登場した。なお、プライベートチェーンは、ブロックチェーンの特徴に含まれる「非中央集権型である」という要素がないため、ブロックチェーンではなく分散台帳技術と呼ばれることがある。

## 7. ブロックチェーンの課題

### 7-1 安全性

暗号資産はウォレットの秘密鍵がなければ勝手に使われることはない。しかしながら、秘密鍵が盗難されると全て犯罪者の手に渡ってしまう。ウェブウォレットや取引所のウォレットを利用している場合、秘密鍵がサービス事業者側に知られていることになるため、自分がいくら気を付けていても事業者側で盗難される可能性がゼロではない。実際に、2014年に起こったマウントゴックス事件では、利用者に落ち度がなく、事業者の内部でビットコインが盗まれた。

巨大なマイニングプールの存在も安全性に影を落としている。ビットコインをはじめメジャーなブロックチェーンにおいて、個人がマイニング競争に勝つことは事実上不可能である。どこかのマイニングプールに参加して、チームの一員として報酬を得るしかない。マイニングプールとは、マイナーを集めた巨大なマイナー集団で、マイニングが成功して報酬が得られると、その貢献度に応じて各マイナーに報酬が分配される仕組みになっている。このマイニングプールが巨大になったため、現在のビットコインではいくつかのマイニングプールが談合すれば、不正なブロックを故意に追加することも不可能ではない状態になっている。



## 7-2 スケーラビリティ

多数のユーザーが一度にブロックチェーンを利用すると、ブロックチェーンの処理能力が追いつかなくなることがある。クレジットカードの場合は世界で1秒あたり1700件の決済が行われている一方、ビットコインの処理能力は1秒あたり約5～10件、イーサリアムの処理能力は1秒あたり約15件とされる。トランザクションの遅延が発生すると、ユーザーはより早くトランザクションを処理してもらうために手数料を高く設定するという状況が起こり、手数料が高騰してゆく。また、ブロックチェーン上で動く分散アプリケーション (DApps) の増加もブロックチェーンの負担になっている。ブロックチェーンでは、システムの処理量が増加したときにノードを増やしても、1つのノードが処理するタスク量は減らないため、システム全体の処理能力は変わらないままである。

ブロックチェーンのスケーラビリティ問題を解消するための技術として、大きく分けてオフチェーン型とオンチェーン型がある。オフチェーン型では、システムが処理すべきタスクの一部をブロックチェーンの外側 (オフチェーン) で処理し、どうしてもブロックチェーンで行わなければならない処理やその結果だけをブロックチェーン上で行うことで、システム全体の処理能力を向上させる。オンチェーン型の例としては、イーサリアムで用いられる Plasma がある。これは、ブロックチェーン本体と接続する別のブロックチェーンを作成し、処理をほかのチェーンに分担させることによって、ブロックチェーンの処理性能を向上させている。

もうひとつ、ブロックという単位の問題もある。ブロックチェーンのようなデータ構造の考え方には必ずしもブロックが必要ではなく、ブロック構造を持たない分散型台帳の方が効率よく処理できる可能性がある。

## 7-3 ハードフォーク

ブロックチェーンは一時的な合意の不一致が起きた際、分岐 (フォーク) をすることがある。せいぜい数ブロックのうちにどちらかのチェーンが長くなり、自然に解消するため普段はこれを意識する必要はない。これをソフトフォーク (一時的分岐) という。

ところが、ブロックチェーンの約束事そのものを変更しようとしたときに意見が対立すると、互換性のないブロックを作るハードフォーク (恒久的分岐) が起きることがある。たとえばビットコインのブロックは、スケーラビリティの問題を解決する手段として、ブロックのサイズを大きくするか、ブロックの外にデータを保存するかで意見が分かれた。その際、もとの名を継ぐ「ビットコイン」(BTC) と「ビットコイン・キャッシュ」(BCC) に分離された経緯がある。

#### 7-4 ダブルスペント（二重送金）問題

ビットコインのブロック追加速度はおおよそ10分間隔で、さらに確定するには6ブロックほど待つ必要がある。しかしながら、そこまで顧客を店舗で待たせるわけにはいかず、トランザクションが承認されていないことを承知で顧客にモノを売ることになる。この運用を「ゼロ・コンファメーション（0-comfirmation）」と呼ぶ。

ビットコインでは、手数料が低く設定されたトランザクションは、いつまでたってもブロックチェーンに取り込まれない、という事態が起こる。そのような事態への救済措置として、「RBF」（Replace by Fee）という仕組みが導入された。後から手数料を高く設定しなおしたトランザクションを送ることで、先に送ったトランザクションを取り消せる、というものである。しかし、このRBFを導入したせいで、ビットコインは意図的なダブルスペント（二重送金）ができてしまう状況になってしまった。

あとから別のトランザクションを上書きすることができると、例えば悪意を持った顧客がモノを購入する後、そのトランザクションがブロックチェーンに取り込まれる前に、トランザクションをコピーして違う宛先に送金することで、店舗に支払うことなくモノを手手出来てしまうのである。

Cordaなどの分散型台帳技術では、この二重送金問題を解決する仕組みを取り入れている。

#### 7-5 電力消費

PoWの仕組みを取り入れているブロックチェーンでは、マイナーはチェーンに新しいブロックを追加して報酬を得るため、無意味ともいえる計算で莫大な電力を浪費している。

ビットコインのマイニングに使われる消費電力が、世界の電力消費の0.25%に達するというデータもある。SDGsの面でも、例えばPoWをPoSに変えて消費電力を減らすなどの対策が求められる。

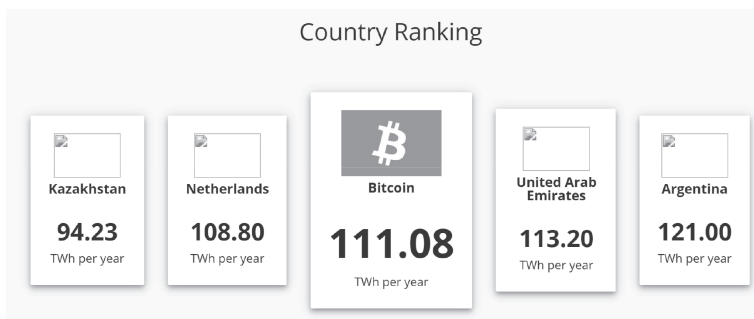


図7 ビットコインと各国の消費電力

(<https://cbeci.org/cbeci/comparisons>)

## 8. ブロックチェーンのこれから

6章で説明したように、ブロックチェーンは新しい技術や仕組みが取り入れられ日進月歩で進化を続けているが、万能ではない。ブロックチェーンが得意とする分野とそうでない分野をしっかりと把握した上で、活用方法を模索していく必要がある。

即応が必要なものは、いまのところブロックチェーンに向いていない。ブロックチェーン上で動く分散アプリケーション（DApps）は、いちどブロックチェーンに載せてしまうと変更ができないため、頻繁にシステムに変更を加える用途には向かない。また、秘匿性の高い情報については、たとえそれを暗号化したとしても、パブリックに流すというのは不要なリスクを生むことになる。容量の大きなものの流通にも向いていない。

ブロックチェーンの優れたところは、非中央集権型であり、データの改竄ができず、参加者がみんなで検証できるというものである。信頼していない者同士で構成されたネットワークで、不正があることを心配することなく安心して取引を行えるのである。

法定通貨の信用度が低い地域、例えば偽札が多く出回っていたり、通貨の価値が乱高下したりするようなところでは、ブロックチェーンによる暗号資産の評価が高い。しかしながら、現状では日常の決済に向いているとは言い難く、決済の高速化を図る仕組みの開発が期待される。

電子投票システムには、ブロックチェーンの耐改竄性がぴったりと当てはまる。いつ、誰が、何に投票したのかをブロックチェーンに記録することで、不正の余地をゼロに近づけることができる。ただし、本人確認をバイオメトリクス認証などを用いて厳格に行う必要があり、また、「誰が、何に」の情報は、個人のプライバシーとして保護されるべきものであるため、記録を検証できる人物や団体は限定される可能性がある。

電子データ化された証憑書類の保存の用途にもブロックチェーンは有効である。現在利用されている電子署名や電子証明書は、それを認証する認証局自体の信頼性や安全性が問われるが、例えばハッシュ値や電子署名をブロックチェーンに記録しておけば、書類自体はブロックチェーンの外にあっても改竄の有無を確認することができる。

### 参考文献

[1]「ブロックチェーンの定義」を公開しました、<https://jba-web.jp/news/642>, 日本ブロックチェーン協会（2021年1月5日参照）

[2] 杉井靖典, “いちばんやさしいブロックチェーンの教本 人気講師が教えるビットコ

- インを支える仕組み”, 株式会社インプレス,2017
- [3] 岡嶋裕史, “ブルーバックス B-2083 ブロックチェーン 相互不信が実現する新しいセキュリティ”, 株式会社国宝社,2019
- [4] コンセンサス・ベイス株式会社, “図解即戦力 ブロックチェーンのしくみと開発がこれ1冊でしっかりわかる教科書”, 株式会社技術評論社,2019
- [5] 伊藤穰一, アンドレー・ウール, “NHK 新書 545 教養としてのテクノロジー AI、仮想通貨、ブロックチェーン”, NHK 出版,2018
- [6] Daniel Drescher (著), 株式会社クイープ (訳), “徹底理解ブロックチェーン ゼロから着実にわかる次世代技術の原則”, 株式会社インプレス,2018
- [7] アンドレアス・M・アントノプロス (著), 今井崇也 (訳), 鳩貝淳一郎 (約), “ビットコインとブロックチェーン 暗号通貨を支える技術”, NTT 出版株式会社,2016
- [8] 岡田仁志, “決定版 ビットコイン&ブロックチェーン”, 東洋経済新報社,2018
- [9] ビットバンク株式会社&『ブロックチェーンの衝撃』編集委員会, “ブロックチェーンの衝撃 ～ビットコイン、FinTech から IoT まで社会構造を覆す破壊的技術～, 日経 BP 社,2016
- [10] Stuart Haber & W. Scott Stornetta, “How to time-stamp a digital document” , Journal of Cryptology volume 3, pages99-111 (1991)
- [11] Jakobsson, Markus; Juels, Ari. "Proofs of Work and Bread Pudding Protocols". Secure Information Networks: Communications and Multimedia Security. Kluwer Academic Publishers: 258-272. (1999)
- [12] Nakamoto, Satoshi (24 May 2009) , Bitcoin: A Peer-to-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf> (2021 年 1 月 10 日閲覧)