第２章　ブロックチェーンの概要

第１節．ブロックチェーンの基礎知識

１．ブロックチェーンの定義

ブロックチェーンについては、明確な定義が存在していない。総務省が発表した令和２年版情報通信白書においては、以下のように示されている。

> ブロックチェーン技術とは、情報通信ネットワーク上にある端末同士を直接接続して、暗号技術を用いて取引記録を分散的に処理・記録する**データベースの一種**であり、「ビットコイン」等の暗号資産[2]に用いられている基盤技術である。[3]

上記にある様に、ブロックチェーンはデータを蓄積することができるデータベース[4]であり、データを分散的に保管・記録する手段のひとつである。また、端末同士が直接接続してやり取りを行うことができるため、管理者や仲介事業者などの存在が不要となる。

２．従来のデータベースとブロックチェーンによるデータベースの違い

従来のデータベースでは、各人が業務に必要なデータを取り出すには、それぞれのコンピュータから該当するデータが保存されているファイルサーバ（以下、中央サーバ）にアクセスし、データを取得している。この構造の大きな欠点は、中央サーバに障害が起きた場合、そのサーバが復旧するまで業務が滞ってしまったり、最悪の場合蓄積されたデータが全て喪失してしまったりする可能性があることである。

一方、ブロックチェーンによるデータベースは、中心となるサーバがない。利用する全員が同じデータを持ち、共有・同期するため、誰か１人が情報をなくしてしまったとしても、同じデータを補完できることから、喪失リスクは低減される。

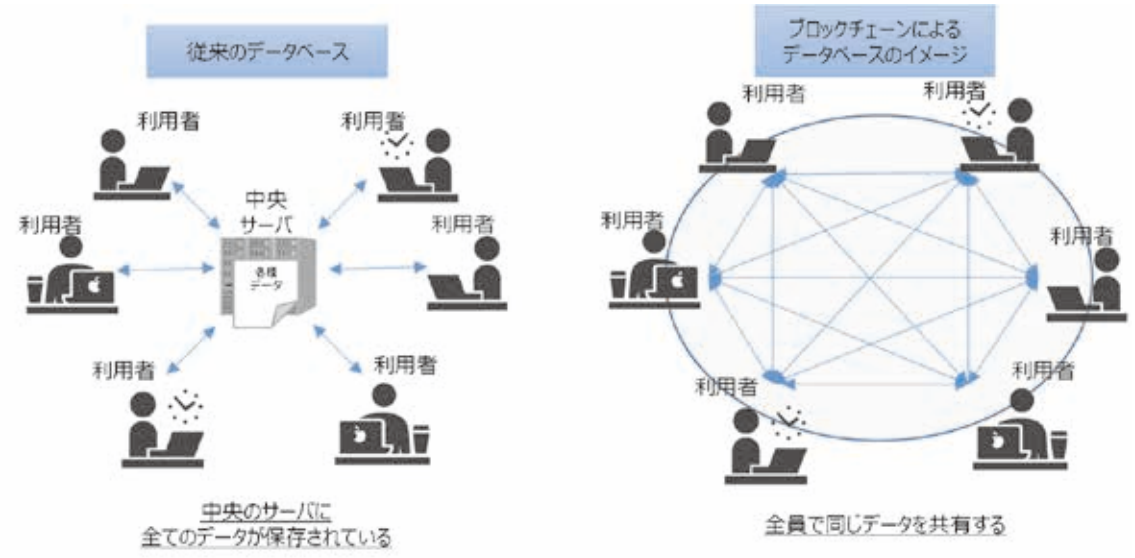
---

[2] 暗号資産…インターネット上でやりとりできる財産的価値のこと。資産決済に関する法律には、次の３つの性質を持つものとして定義されている。
（１）不特定の者に対して、代金の支払い等に使用でき、かつ、法定通貨（日本円や米国ドル等）と相互に交換できる
（２）電子的に記録され、移転できる
（３）法定通貨または法定通貨建ての資産（プリペイドカード等）ではない

[3] 出典：総務省　令和２年版情報通信白書
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/html/nd134620.html（2021 年 11 月 29 日確認）

[4] データベース…ある特定の条件にあてはまる「データ」を複数集めて、ひとつに集積したもの。紙で言うところの台帳（売買や事務上の記録の土台となる帳簿）のイメージである。

図表 2　従来のデータベースとブロックチェーンによるデータベース



出典：各種情報に基づき情報通信総合研究所作成

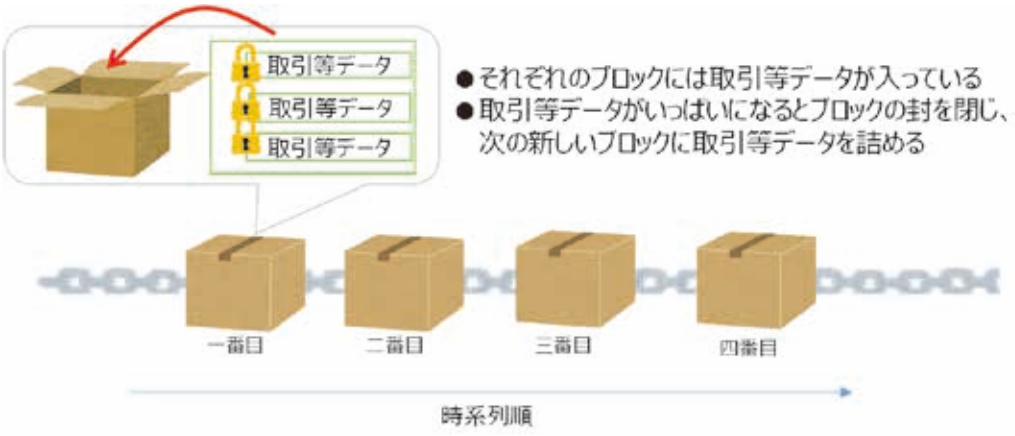
３．ブロックチェーンの仕組み

本項では、ブロックチェーンがどのような流れでデータを蓄積していくのかについて説明する。

ブロックチェーンに記録されるデータは、モノの受け渡しやお金の送金などで発生したやり取りの記録（以下、取引等データ）である。それぞれの取引等データは、１回のやり取りごとに暗号化されており、暗号化されたデータが一定量溜まると１つの「ブロック」にまとめる仕組みとなっている。

ブロックが１つ完成すると、次の新しいブロックにデータを貯めていく。これらのブロックは時系列がわかるように並んでおり、一本の鎖（チェーン）のようにつながっている。

図表 3　ブロックチェーンのイメージ図



出典：各種情報に基づき情報通信総合研究所作成

ブロックを１つ完成させる際、ブロックチェーンでは合意形成を行う。合意形成とはブロックに詰めたデータが正当なものであるか検証することであり、やり方は様々あるが、ブロックチェーンの参加者（ノード[5]）全員に、ブロックに詰めたデータに誤りがないか確認してからブロックを作る方法などがある。この作業によりブロックの信頼性が確保されている。

図表 4　合意形成のイメージ

出典：各種情報に基づき情報通信総合研究所作成

４．ブロックチェーンの特徴

前項の「ブロックチェーンの仕組み」を踏まえ、ブロックチェーンの基本的な考え方となる、大きな特徴３つについて紹介する。

①耐改ざん性に優れている

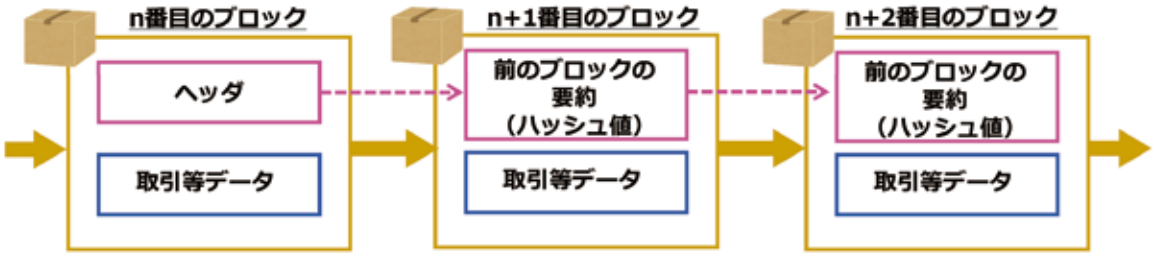
ブロックは時系列順に並ぶ仕組みとなっている。これは、各ブロックに１つ前のブロックの要約を入れることで実現されている。

ブロックの中身について簡単に説明すると、ブロックには「ヘッダ」と「取引等データ」の大きく分けて２つが入っている。ヘッダは前のブロックがどれなのか判別できる役割を持ち、前のブロックの要約（ハッシュ値）（参照：ブロックチェーンの理解を深める①P11）等が入っている。仮に、悪意のある参加者が過去のデータの一部を書き換えた場合、その要約との不一致が起き、他の参加者とデータの整合性がとれなくなり、すぐに不正が発見されてしまう。これによって、ブロックチェーンは事実上データの改ざんが不可能であるといえる。

また、ブロックを１つ完成させる際、合意形成を行う。参加者全員にブロックの正しさを確認してから生成する方法などがあるため、改ざんしたデータを加えることは困難である。

[5] ノード：ブロックチェーンを構成する（参加する）コンピュータのこと。

図表 5　ブロックがつながっていくイメージ



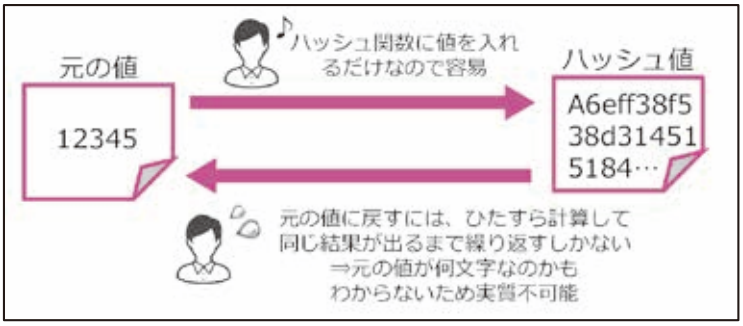
出典：各種情報に基づき情報通信総合研究所作成

【ブロックチェーンの理解を深める①　ハッシュ関数／ハッシュ値】

ブロックチェーンで使われる「ハッシュ関数／ハッシュ値」について説明する。

ハッシュ関数とは、数式（関数）のことであり、一般的には、Web サイトにログインする際のパスワードの暗号などに利用されている。また、ある値についてハッシュ関数を使い計算した値を「ハッシュ値」と呼ぶ。

ハッシュ関数は、ある値からハッシュ値を作り出すのは簡単であるが、そのハッシュ値から元の値を復元するのは難しいという特徴を持つ。また、元の値を一文字だけ変更したとしても、全く異なるハッシュ値が導き出されるため、簡単に値を予想することはできない。



②履歴の追跡ができる

ブロックチェーンには、これまでの「取引等データ」の履歴が時系列順に全て保存されている。そのため、過去にどのようなやり取りがあったのかを、遡って確認することができ、ヒト・モノ・カネなどの移動記録を保存することに向いている。

一方で、すべての取引等データを保存するため、取引等の数に比例してデータ量は増加していく。また、過去のデータを消去することは難しい。（消去する場合、「消去した」という履歴が残る。）

③データを全員で共有できる（透明性が高い）

ブロックチェーンの場合は参加者（ノード）全員が同じデータを共有している。（分散して保存している）そのため、仮に誰かの持つデータが消えたり壊れたりしたとしても、他の人が持つデータで補うことができ、データ喪失の恐れが少ない。また、ネットワークに参加するノードすべてが同時に止まらない限り稼働し続けるため、システム障害などで停止す

ることのなく稼働し続ける仕組みを実現できる。

一方、データを全員で共有できるという特徴から、ブロックチェーンにはプライバシーや個人情報に直結するようなデータを保存しないことが望ましい。

図表 6　ブロックチェーンの特徴のまとめ

出典：各種情報に基づき情報通信総合研究所作成

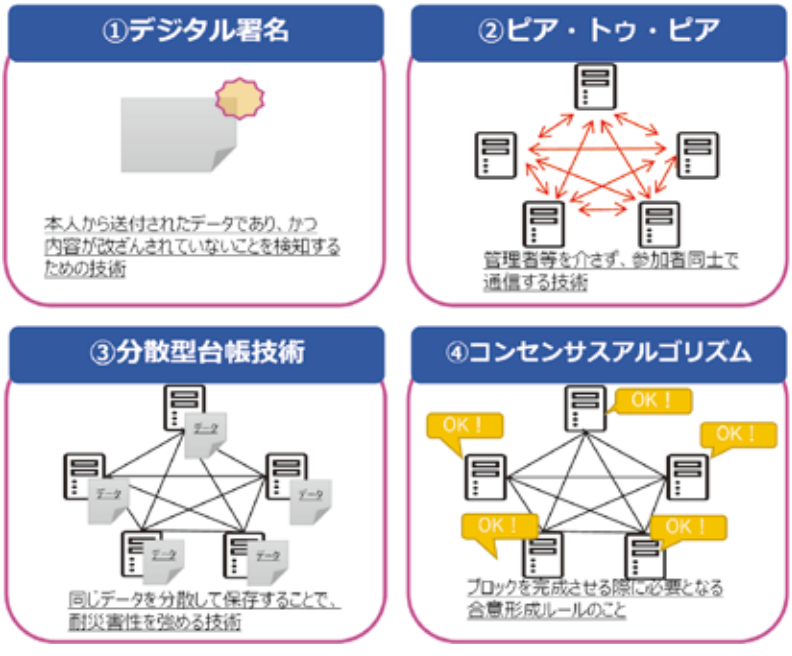
５．ブロックチェーンに使われている技術と技術的課題

（１）ブロックチェーンで使われている技術

ブロックチェーンは、「新しい技術」と考える人は多いが、既存技術の集合体である。

ここではブロックチェーンを理解するうえで必要となる代表的な４つの技術について説明する。

図表 7 ブロックチェーンに使われている代表的な４つの技術



出典：各種情報に基づき情報通信総合研究所作成

①デジタル署名／暗号化技術

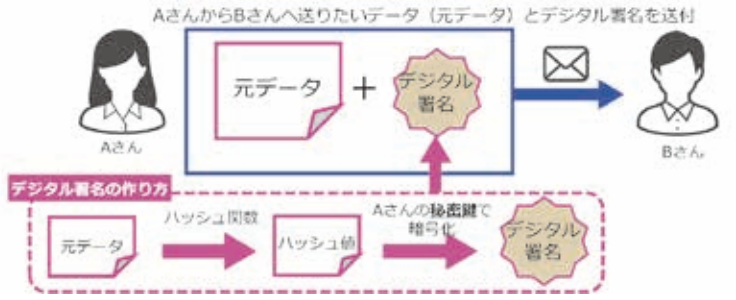
ブロックチェーン上で取引等やり取りする際、デジタル署名を付与する必要がある。デジタル署名とは、デジタル上の「はんこ」のイメージであり、あるデータがその本人によって確実に送られたことを証明する技術である。また、そのデータが作成後に改ざんがされていないことの証明にも利用できる。デジタル署名の仕組みには、暗号化技術（公開鍵暗号[6]）が利用されており、ブロックチェーンのセキュリティを担保する仕組みのひとつとなっている。

【ブロックチェーンの理解を深める②　デジタル署名の仕組み】

デジタル署名は、公開鍵暗号方式と呼ばれる暗号化方式がベースになっており、「公開鍵」と「秘密鍵」の２つの鍵を利用し、暗号化を行う。公開鍵とは、広く一般に公開される鍵であり、秘密鍵は個人など特定のユーザだけが所有している鍵のことである。デジタル署名においては、秘密鍵がデータを暗号化するための鍵として利用されており、それと対になった公開鍵でないと復号することはできない。デジタル署名の２つの工程「（1）署名を作成する工程」と、「（2）（その署名により）データが改ざんされていないか検知する工程」について詳しく説明する。

（1）署名を作成する工程　※A さんから B さんへデータを送付する

A さんは、送りたいデータ（元のデータ）について、ハッシュ関数を利用してハッシュ値を導き、そのハッシュ値を A さんの秘密鍵を利用して暗号化を行う。A さんだけが所有している秘密鍵を利用しているため、A さんであることの証明となり、これがデジタル署名となる。



（2）（その署名により）データが改ざんされていないか検知する工程

B さんは、データを受け取ったら A さんの公開鍵を利用して、検証を行う。まず、元のデータからハッシュ関数を利用し、ハッシュ値を求める。次に、デジタル署名を A さんの公開鍵を利用して復号し、暗号化される前のハッシュ値を求める。導き出した２つのハッシュ値が一致していれば、このデータは改ざんされていないということを確認できる。（仮にどこかで元データが改ざんされていたとすると、ハッシュ値の不一致が起きる。）

[6] 公開鍵暗号…暗号方式のひとつであり、ブロックチェーンだけでなく、一般的なネットワーク通信でも、暗号化を行う際に利用されている。

②ピア・トゥ・ピア（Peer[7] to Peer）

第２項で紹介した、従来のシステム構造は「クライアントサーバ型」と呼ばれており、全ての通信は中心となる「サーバ」を介して行われる。そのため、各人のコンピュータが直接通信することはない。

一方、ブロックチェーンの場合は、中心となる管理者がいない構造である。そのため、各人のコンピュータ間で直接通信をすることができる。

③分散型台帳技術

データを複数箇所で分散して保持する技術のこと。データが分散して格納されるため、単一障害点（システムを構成する機器の中で、１つが故障するとシステム全体が停止すること）のない構造となる。ブロックチェーンは、分散型台帳技術のひとつといえる。

④コンセンサスアルゴリズム

ブロックチェーンでは、ブロックを１つ完成させる際、合意形成が必要であり、様々な合意形成のルールを総称して「コンセンサスアルゴリズム」と呼ぶ。なお、実際この合意形成作業を行うのは、「ノード」と呼ばれるブロックチェーンに参加しているコンピュータのことである。

【ブロックチェーンの理解を深める③ コンセンサスアルゴリズム（合意形成）】

ブロックチェーンでは、ブロックを１つ生成するには、参加者から合意を得る必要がある。この合意形成の方法をコンセンサスアルゴリズムと呼び、これには複数の種類がある。

ビットコインの場合は、PoW（Proof of Work）という方法になる。直訳すると「仕事の証明」であり、このWork（仕事）とは計算競争のことを指す。この計算競争に挑む参加者は、高い計算能力を有する必要があるため、大量の電力費用や機器の初期投資費用がかかる。（参照：ブロックチェーンの理解を深める⑤ P17）

PoW のほかには、通貨の保有量が多い参加者がブロックを生成できる方法や、ブロック生成者をランダムに選ぶ方法などのコンセンサスアルゴリズムが存在する。どの種類のコンセンサスアルゴリズムを利用するかは、構築するブロックチェーンに合わせて設計時に検討する。

コンセンサスアルゴリズムの名称	概要
PoW （Proof of Work）	高度な計算競争に勝った参加者がブロックを生成し、全参加者によって正しさが検証・承認されるとブロックが追加される方法
PoS （Proof of Stake）	通貨の保有量が多い参加者がブロックの生成や承認する権利を得られる方法
PoA （Proof of Activity）	信頼された参加者のみがブロック生成の権利を持つ方法

[7] Peer は「対等」の意味を示す

（２）ブロックチェーンの技術的課題

ブロックチェーンの技術的課題として、代表的なものを２つ紹介する。

１つ目は「量子コンピュータの出現」である。取引等データは、暗号化技術によって守られているが、近年量子コンピュータの出現により、暗号が解かれてしまう可能性があると言われている。

量子コンピュータとは、これまでのコンピュータよりも計算処理能力が桁違いに速いコンピュータのことである。暗号化技術は時間のかかる難しい計算を用いているが、近いうちに解読されてしまう危険性がある。量子コンピュータにも耐えられるよう、一部のブロックチェーンでは量子耐性のある、すなわちより計算難易度を上げた暗号化方式を実装し始めている。

２つ目は、「スケーラビリティ」の問題である。スケーラビリティとは、取引等データを同時に処理できる限界値の拡張性のことであり、参加者（ノード）が増え、取引等データが増えると、ブロックの生成が追い付かなくなり、処理速度が遅くなってしまうというリスクのことである。この問題については、処理の一部をブロックチェーン外側で行う技術等が検討されており、解消に向けた試行が進んでいる。

様々な課題に対し解決策も日々生み出されているが、導入時には懸念点やリスクを改めて確認したうえで検討する必要がある。

第２節．ブロックチェーンの実用化

１．ブロックチェーンの歴史

（１）ブロックチェーンの歩み

ブロックチェーンには様々な種類があり、歴史と共に進化している。

世界で初めて活用されたブロックチェーンはビットコインブロックチェーンである。

2013 年には、現在主流となっている「イーサリアム」が誕生した。イーサリアムは、ブロックチェーンを活用し、開発・実行ができる汎用的なプラットフォームである。それまでは、ビットコインのブロックチェーンをベースに開発を行っていたが、イーサリアムの誕生によって、複雑なアプリケーションの開発・実行ができるようになった。

図表 8　ブロックチェーンの歴史

ブロックチェーンの歴史	ビットコイン ブロックチェーン	イーサリアム
利用開始時期	2009年～	2013年～
概要	・ビットコインが実装されたブロックチェーン ・世界で初めてのブロックチェーン	・ブロックチェーンを活用し、様々なアプリケーションを開発・実行できる**汎用的なプラットフォーム** **・現在主流となっているブロックチェーン**
ブロックチェーンのネットワークモデル	パブリックチェーン	パブリックチェーン・プライベートチェーン

出典：各種情報に基づき情報通信総合研究所作成

【ブロックチェーンの理解を深める④　イーサリアム】

最初に作られたビットコインブロックチェーンは仮想通貨のためだけに作られていたが、さまざまな機能を持たせて他分野にも応用しようという動きの中で出現したのが「イーサリアム」である。現在も世界中のエンジニアによって開発が進められている。

イーサリアムは、ブロックチェーンを構築するための汎用プラットフォーム機能を提供しており、従来にはなかった「スマートコントラクト」（参照：ブロックチェーンの理解を深める⑦P19）など、開発しやすくなる機能が備わっており、イーサリアムによってブロックチェーンを基盤技術として活用したアプリケーションの開発が進んだ。

（２）管理者のいないビットコイン

ブロックチェーンの最も代表的かつ最大の活用事例はビットコインである。ビットコインは暗号資産（仮想通貨）の一種であり、世界中の投資家や一般の人などが口座を開設し、ネットワークに参加すれば、誰でも売り買いすることができる。参加者（ノード）同士が直接やり取りするため、管理者（発行主体）にあたる存在はいない仕組みとなっている。

【ブロックチェーンの理解を深める⑤　管理者がいないビットコインはどのように運用されているのか】

ビットコインは、管理者（発行主体）が存在せず、誰でも参加できるネットワークで、不正のないやり取りができる環境を構築している。これを実現しているのはネットワークの参加者であり、参加者が自ら「取引が正当なものであるか検証し、合意する」作業を担っている。

また、この作業に１番最初に貢献した者には報酬（ビットコイン）が支払われる。作業では、複雑な計算を実施し、決められたルールを満たす値を探す（ハッシュ値を求める）必要があるため、報酬を得たいと考える参加者は、複雑な計算を行うための高性能なコンピュータを準備し計算競争に挑んでいる。このような作業のことを「マイニング（＝複雑な計算を行い、値を採掘する）」と呼び、その計算争いに参加する参加者のことを「マイナー」と呼ぶ。

【ブロックチェーンの理解を深める⑥　ノードの役割】

ノードには４つの役割「①ブロックチェーンデータの保存」「②ウォレット」「③ノード間でのデータの共有」「④マイニング」を持たせることが可能である。なお、ノードにどこまでの役割を持たせるかは、ブロックチェーンをどのように設計・構築するかに依存する。

①ブロックチェーンデータの保存

ブロックチェーンに書き込まれた最初から最後までのデータを保存する役割のことである。なお、実運用では、個人のパソコンやスマートフォン端末ですべてのデータを保存する容量等がないため、ブロックチェーンに記録された情報を web 経由で閲覧できる環境を設ける等の方法がとられている。

②ウォレット

ブロックチェーンでは、電子署名に必要となる個人の秘密鍵を保存する場所のことを「ウォレット」と呼ぶ。ウォレットでは、鍵の管理のほか、電子署名を付与した取引等データを発行する役割を持つ。

③ノード間でのデータの共有

ノード同士でデータを共有・同期させるため、互いに情報を送り合う役割を持つ。

④マイニング

ブロックチェーンのブロックを作りだすために行う計算等の処理をする役割。

（３）ブロックチェーンのネットワークモデル

非金融分野での活用検討が進み、「ビットコイン」のように誰でも参加できる（パブリックな）ブロックチェーンに対し、「プライベートチェーン」と呼ばれるネットワークモデルが登場した。

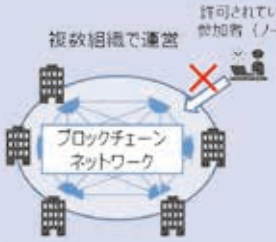
ブロックチェーンのネットワークモデルは大きく分けて２つの種類がある。不特定多数が利用できる「パブリックチェーン」と、利用者が明確になっている「プライベートチェーン」である。後者はさらに、複数の組織（自治体や企業など）で利用する「コンソーシアム型」と、ひとつの組織が利用する「プライベート型」に分けられる。

パブリックチェーンの場合、記録された情報が不特定多数に公開されてしまうため、取り扱う情報の精査を慎重に行う必要があるほか、悪意を持った参加者による攻撃を受ける可能性があるため、脆弱性検査等を事前に行うなどセキュリティリスクを考慮し構築する必要がある。一方、プライベートチェーン（コンソーシアム型・プライベート型）は、記録された情報の公開対象者が明確であるため、セキュリティリスクもパブリックチェーンに比べて抑えられる。

また、プライベートチェーンは、そもそもブロックチェーンを活用したサービス提供を実

施するために登場したネットワークである。サービスは、継続して提供する必要があるため、維持・運用する者が必要となる。このため、プライベートチェーンでは管理者を用意する必要があり、利用者のブロックチェーンへの参加許可なども含め実施する。従って、ブロックチェーンを活用したサービス提供や様々な情報管理に適用し易いネットワークモデルといえる。

図表 9　ブロックチェーンの種類

	ブロックチェーンの種類		
	パブリックチェーン	プライベートチェーン	
		コンソーシアム型	プライベート型
管理者	不在	存在 （複数組織で運営）	存在 （単一組織で運営）
参加者	誰でも自由に参加可能	限定された組織のみ参加可能	単一組織（管理者と同じ）
特徴	・不特定多数がアクセスできる開かれたネットワーク ・悪意を持った参加者による攻撃の可能性があり、セキュリティリスクが高い ・全員に情報が共有されるため、プライベートチェーンよりも取り扱う情報を慎重に精査する必要がある	・限定された人しかアクセスできない閉じたネットワーク ・許可された参加者で構成されているため、パブリックチェーンに比べてセキュリティリスクが低い ・限定された参加者のためのサービス提供や様々な情報管理に適用し易い※	
利用例	暗号資産（仮想通貨）等	トレーサビリティや証明書発行　等	
イメージ図			

※ブロックチェーンに記録するデータについては、公開対象者が明確ではあるが、すべての取引等データを保存しているというブロックチェーンの特徴があるため、データの削除が難しい。したがって、個人情報の格納は避けるべきである。

出典：各種情報に基づき情報通信総合研究所作成

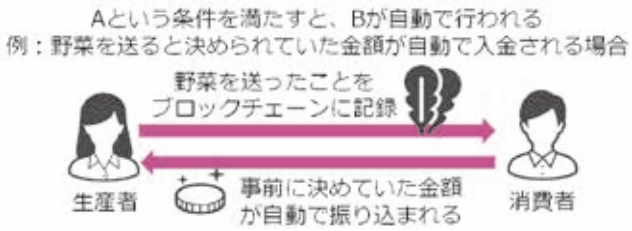
現状、「ビットコイン」で利用されている管理者のいないパブリックチェーンは、中央集権型の社会や組織に馴染まず、非金融分野での活用事例では、基本的に「プライベートチェーン」によってブロックチェーンが構築されている。

なお、世間一般で「ブロックチェーン」について語られる場合、ビットコインのネットワークモデルである「パブリックチェーン」を前提としていることが多い。

【ブロックチェーンの理解を深める⑦　スマートコントラクト】

スマートコントラクトは、イーサリアムのブロックチェーンで初めて実行可能となった機能である。（ビットコインのブロックチェーンにこの機能はない）

スマートコントラクトは直訳すると「賢い契約」という意味である。ブロックチェーン上であらかじめ「A という条件になったら、B の処理をする」と決めておくことで、その条件に合致すると自動で処理が行われる仕組みである。 このような仕組みをブロックチェーンではプログラムに書いておき、自動での契約締結・自動執行を可能にしている。



【ブロックチェーンの理解を深める⑧　トークン】

トークンには様々な意味があるが、ブロックチェーンにおけるトークンとは、定量化できていない価値を定量化するもの（数値情報）である。具体的には、ブロックチェーンで電子投票を実現させる際の「票」に利用されたり、ブロックチェーンで地域通貨等のコインを発行した際の「コイン」として利用される。

２．ブロックチェーンの利用用途

ブロックチェーンの主な利用用途について紹介する。

（１）暗号資産（仮想通貨）

ビットコインをはじめとして、ブロックチェーンを基盤技術とした暗号資産（仮想通貨）は世の中に数多く存在している。暗号資産は、日本円のように国家や銀行から保証されている法定通貨とは異なる、インターネット上でのみ使える通貨のイメージである。そのため、実際に利用する場合は、法定通貨と暗号資産を交換してくれる仲介業者等が必要となる。

また、自治体等が発行する地域通貨を、ブロックチェーンで流通・管理することも可能である。地域内で循環する通貨を作ることで、新しい経済を生み出す可能性もある。

（２）トレーサビリティ

トレーサビリティとは、商品が「いつ」「どこで」「誰によって作られ」「誰によって運ばれた」といった、商品の流通情報を追跡する仕組みのことである。消費者に届くまでに関係するプレイヤー（生産者、加工業者、検査機関、配送業者、小売店）が各段階でその商品の情報をブロックチェーンに記録しておくことで、生産・流通過程の透明性が確保できる。また、商品に不具合があった場合の原因追究にも役立つ。

オーガニック食品やブランド品の生産・流通の記録として、活用が期待されている。

（３）証明書の発行

ブロックチェーンは、証明書の発行にも活用が期待されている。ブロックチェーンを使えば、証明書の発行・更新履歴を全て記録することができ、改ざんがあればすぐに検知されてしまうため、不正の防止にも役立つ。

現在は、紙での証明書発行が主流であるが、デジタル証明書の検討が本格的に進んでくれば、ブロックチェーンを利用して実現することも考えられる。