「ブロックチェーン」とは何か

ビットバンク株式会社
代表取締役 CEO
廣末　紀之　氏

■ビットコインの概要

ビットコインは、2008 年 10 月 satoshi nakamoto と称する人物が暗号学メーリングリスト上に”A Peer-to-Peer Electronic Cash System”という論文（概念設計図）を発表したことから始まる。2009 年 1 月、ビットコインのソフトウェア「Bitcoin V0.1」がインターネット上に発表され、ビットコインの最初の運用、つまり最初のブロックの採掘が開始され、以来無停止状態が継続している。

ビットコインとは、特定の管理主体に依存することなく、価値のやりとりにおいて不正を排除した形で正しく証明することができる P2P 決済ネットワークであり、その管理台帳がブロックチェーンである。中央機関が管理・承認するのでなく、ネットワークの参加者が承認作業を行う。また、現物の「コイン」のようなものがあるわけではなく、あくまで「データ」である。ビットコインは①電子署名、②ブロックチェーン、③プルーフオブワークという中核技術が存在することによって中央機関が管理しなくても不正を排除し正しく運用できる。

■ビットコインの特徴

ビットコインには以下の特徴がある。

①中央管理者が存在しない

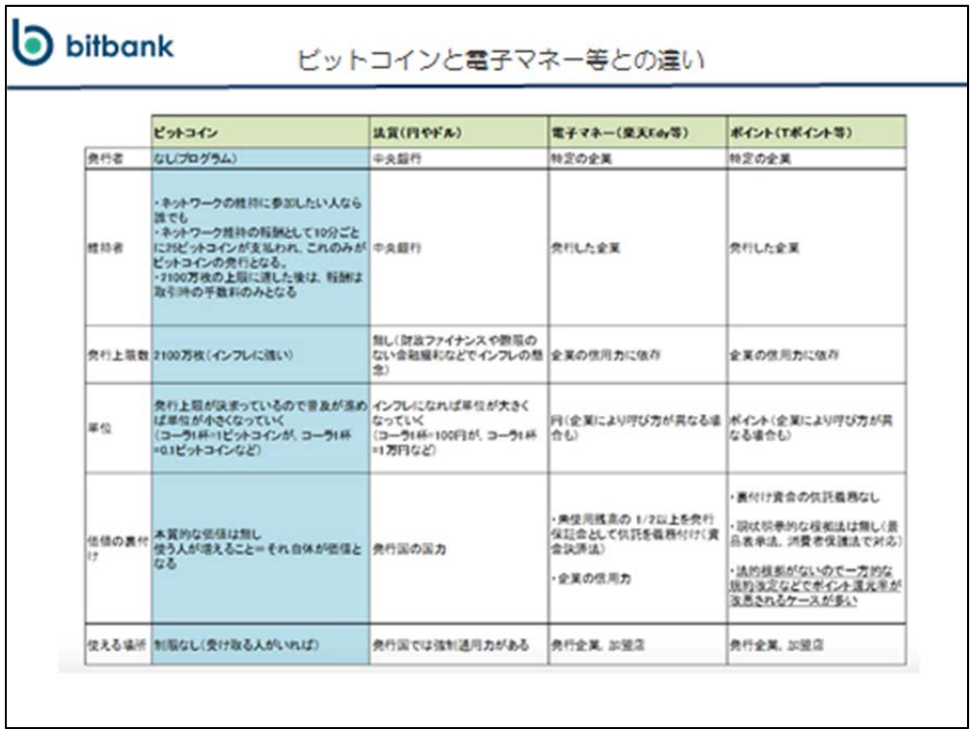
中央管理者が存在しないので、規制は不可能であり、利用者がシステム維持のため費用負担などをする必要がなく、結果としてきわめて安い手数料で利用できる。

②世界中で 24 時間 365 日利用可能

③取引履歴は公開されており、誰でも閲覧可能

④2,100 万枚の発行上限があらかじめプログラムされており、通貨の改悪、ハイパーインフレが起こらない。

ビットコインには発行者はおらず、不特定の参加者が維持しており、発行上限数があらかじめ決められており、本質的な価値の裏付けはなく、使う人が増えること自体が価値となる、という点で法定通貨や従来の電子マネーと大きく異なる。



	ビットコイン	法貨（円やドル）	電子マネー（楽天Edy等）	ポイント（Tポイント等）
発行者	なし（プログラム）	中央銀行	特定の企業	特定の企業
維持者	・ネットワークの維持に参加したい人なら誰でも ・ネットワーク維持の報酬として10分ごとに25ビットコインが支払われ、これのみがビットコインの発行となる。 ・2100万枚の上限に達した後は、報酬は取引時の手数料のみとなる	中央銀行	発行した企業	発行した企業
発行上限数	2100万枚（インフレに強い）	無し（財政ファイナンスや際限のない金融緩和などでインフレの懸念）	企業の信用力に依存	企業の信用力に依存
単位	発行上限が決まっているので普及が進めば単位が小さくなっていく （コーラ1杯=1ビットコインが、コーラ1杯=0.1ビットコインなど）	インフレになれば単位が大きくなっていく （コーラ1杯=100円が、コーラ1杯=1万円など）	円（企業により呼び方が異なる場合も）	ポイント（企業により呼び方が異なる場合も）
信頼の裏付け	本質的な価値は無し 使う人が増えること＝それ自体が価値となる	発行国の国力	・未使用残高の 1/2以上を発行保証金として供託を義務付け（資金決済法） ・企業の信用力	・裏付け資金の供託義務なし ・現状明確的な規制は無し（景品表示法、消費者保護法で対応） ・法的規制がないので一方的な規約改定などでポイント還元率が改悪されるケースが多い
使える場所	制限なし（受け取る人がいれば）	発行国では強制通用力がある	発行企業、加盟店	発行企業、加盟店

■ビットコインの構造

「二重使用」できないことが、お金がお金として信頼されるための大前提であり、従来、中央集権的な方法以外で「二重使用」を回避することは不可能と考えられていた。しかし、ビットコインは例えば A さんから B さんへの通信（送金）が正しいか否かを不特定多数の参加者が監視、承認することにより二重使用を防止している。この承認作業（マイニング）を行うのがマイナー（採掘者）と呼ばれる大量の P2P ノードである。マイナーとは P2P ネットワークにおいてハッシュ計算を行なうものであり、これは、大抵がマイニングのために製造された専用機器（ASIC）である。マイナーは、①取引情報が不正ではないかの確認、②取引履歴データベースへの記録を行っている。

ビットコインは 2009 年 1 月の最初の取引からのすべての取引が記録・公開されており、不正な取引、改ざんを行うには過去の移動記録すべてを書き換える必要があり、きわめて難易度が高い。

■ビットコインの中核技術　①電子署名

ビットコインのブロックチェーン上にはビットコイン所有者の署名が記録されており、署名が一致する場合だけ所有者が内容を書き込める仕組みが採られている。もしも誰かがブロックチェーンにウソの署名を使ってウソの取引内容を記録しようとしても、署名が一致しない場合には内容は書き込めない。そして、取引への署名行為は、秘密鍵を持つ者だけが行うことができる仕組みになっている。つまり、秘密鍵を持つ者だけがブロックチェ

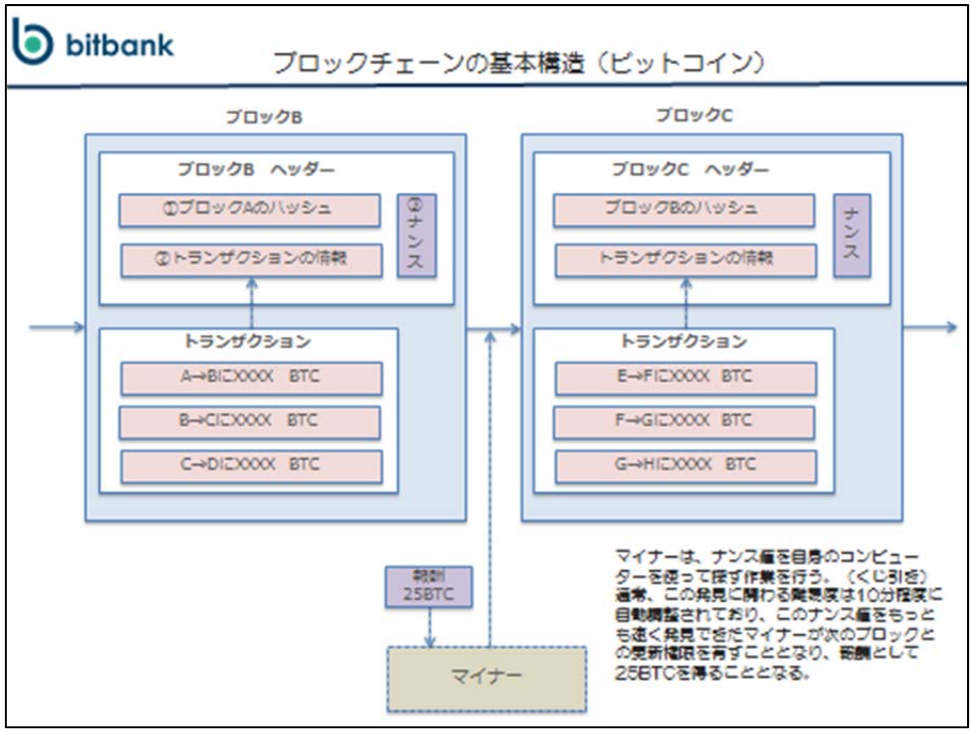
ーンに書き込めるということ、すなわちビットコインを他人に送信可能、つまりビットコインを保有することを意味している。

■ビットコインの中核技術　②全取引データベース（ブロックチェーン）への記録

約 10 分を要する一取引の束（ブロック）を時系列でチェーンのように繋げたデータ構造を持つ取引データベースをブロックチェーンという。全取引履歴データベースは維持管理作業への参加者（マイナー）のコンピュータ内にそれぞれ作成する。つまり世界中に参加者の数だけ全取引履歴データベースが存在する。

全取引履歴データベースの更新権限者は、更新の都度変え、更新権限は維持管理作業者による「くじ引き」で決め、くじで「当たり（ナンス値）」を出した人は、全取引履歴データベースの更新を行い、ビットコインでの報酬を受け取り、更新情報を他の参加者に通知する。

くじ引きの形式は、「特定の問題の答えを、世界で最初に解けた人が当たり」とし、その問題は世界中の参加者が一斉に頑張っても解くまでに 10 分間必要な難しいものとすることで、特定の人が連続して「当たり（ナンス値）」を出して不正を行うことを難しくしている。



■ビットコインの中核技術　③プルーフオブワーク

プルーフオブワークとは、分散型合意形成アルゴリズムの一種で、取引データの改ざんを防止する仕組みである。前述の通り、ネットワーク参加者（マイナー）が膨大な計算を行い”ナンス値”を探す作業（マイニング）を実行することにより、悪意のある参加者の改ざ

んを防止している。

現在、ビットコインのハッシュレート（採掘速度）は 150 万テラハッシュに達している。もはやビットコインのネットワークは世界最大のスーパーコンピューターとなっており、強靭な攻撃耐性があるといえる。また、ビットコインのブロックチェーンは、長いチェーンを正とするルールとなっており、攻撃者とブロックチェーンの伸ばし合い競争をした場合、善意の参加者の持つ計算資源が、攻撃者のそれより少しでも多い限り、攻撃者がブロックチェーンを乗っ取れる可能性はきわめて低いとされている。

■ブロックチェーンの発展

ビットコインはオープンソースなので、誰でもフォーク（分岐）が可能である。現在、ビットコインに類似したシステムは 1,000 を超え、ハッシュアルゴリズムを変更したもの、株式会社のように仮想通貨の保有量によって発言権や承認権を決めるもの、管理者を設置したものなど多岐にわたっている。

ブロックチェーンは、ビットコインや ethereum に代表される管理者不在の形態で誰でも利用可能なパブリック型と、管理者を設定し、利用可能な参加者を限定したプライベート型に大別される。ethereum はチューリング完全、すなわちプログラム可能なものはすべてここに実装可能であり、コントラクトをブロックチェーンに記録することで改ざん不能なコントラクトベースのブロックチェーンを構築するものである。

■産業への応用

ブロックチェーンに関する研究は金融機関を中心に進められており、ゴールドマン・サックスや JP モルガンなど 9 行を束ねる「ブロックチェーン・コンソーシアム」にはみずほ銀行など日本の金融機関も加わっている。また、PC やスマートフォン、家電製品などのあらゆるチップセットにマイニング用 ASIC を組み込み、各デバイスがマイニングしたビットコインを原資に、M2M で少額決済がブロックチェーン上で自動的に行われる IoT 時代を見据えた研究も行われている。さらに guardtime はエストニア政府と提携し、130 万人のエストニア国民の生涯の健康・医療データの記録管理にブロックチェーンの利用試験を開始するなど、ブロックチェーンの産業分野への応用が広まっている。