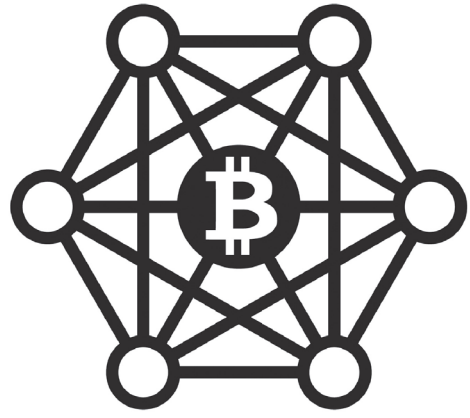
初めの一歩
ブロックチェーン講座

①基礎編

執筆 / 髙橋弘至



株式会社 コガク

講座のねらい

ブロックチェーンといえば、ビットコインなどの暗号資産を支える技術として知られていますが、機能を拡張しながら進化を続けて応用範囲が格段に広まり、金融 (フィンテック) にとどまらずサプライチェーン、ロジスティクス、トレーサビリティと、実証実験の段階から社会実装段階へと移行しつつあります。この流れは近年 Web3 として話題になっています。改ざんが不可能かつ透明性、安定性が高い分散型台帳といわれ、インターネットの登場と同様に、あらゆる産業分野の既存のビジネスを変革していくことが期待されています。

本講座は、ブロックチェーンの始まりと発展、ビットコインの概要、セキュリティのための暗号技術、分散型を特徴とするネットワーク、取引の仕組み、資産の保管場所、イーサリアムによる契約の自動化など、多様な技術が集積して機能するブロックチェーンのシステムをプログラムの解説は用いず技術畑以外の方にも理解できるようにわかりやすく解説し、基本的な仕組みを概観して理解できる内容となっています。ビジネス事例を紹介するだけではなく、“ なぜそうなるのか ” の原理を理解できるよう解説します。

本講座の学習を通じて、ブロックチェーンにはどのような特徴があり何ができるのかを理解し、ソリューションやサービスに変革をもたらすはじめの一歩となるように指南します。

目　次

学習のねらい

本文冊ではブロックチェーンについて基礎的な理解を得るための、基本的な考え方とその技術的概要について解説します。

第 1 週では、新たな通貨である暗号通貨を生み出したブロックチェーンという技術が生まれた背景について、情報とその信頼性の歴史と共に解説します。

第 2 週では、ブロックチェーンの誕生、発展と大きく関係しているビットコインについて、その概要と特徴について解説します。

第 3 週では、データの信頼性を担保している、ハッシュ関数、公開鍵暗号、電子署名などについて解説します。

第 4 週では、ビットコインが展開している分散型ネットワークについて、他のネットワーク形態との比較をし、その概要と特徴について解説します。また、分散型ネットワークがどのように一つのシステムとして機能しているのかコンセンサスのメカニズムについても解説します。

■ 第１章 ■

ブロックチェーンの歴史

【学習のポイント】

どのような技術にもそれが誕生した歴史・背景があり、これを理解することは新たな技術を素早く理解し、効率的に使用するために効果的です。

ブロックチェーンが生まれた背景について、情報とその信頼性の歴史とあわせて解説します。

1.1　ブロックチェーンの歴史

近年、分散型台帳技術 (DLT: Distributed Ledger Technology) の一つとして広く知られるようになったブロックチェーン (Blockchain) の発展は、ビットコイン (Bitcoin) の誕生と深く関わっています。

分散型台帳技術とは、複数の場所や組織をまたがって複製・共有・同期されるように設計された台帳 (データベース) を取り扱う技術です。また、分散型台帳には従来型のデータベース技術である中央集権型台帳と異なり、中央管理者が存在しません。

ビットコインは 2008 年 10 月 31 日に Satoshi Nakamoto とよばれる人物によって、暗号理論に関するオンラインコミュニティにおいて論文という形式で提案されました。この Satoshi Nakamoto という名前は、一見すると日本人の名前のように思われますが、オンラインコミュニティにおけるハンドルネームであるため、実際に誰がこの論文を発表したのかについては諸説があり、いまだに不明です。

Satoshi Nakamoto は同年 9 月に発生した、アメリカの大手投資銀行リーマン・ブラザーズの経営破綻を発端にした世界金融危機、いわゆる “ リーマンショック ” を背景に既存の金融システムへのアンチテーゼとしてビットコインを提案したといわれています。このような金融危機が発生したことは過去にもあり、結果として政府や大企業に依存していた金融システムに対する信用を大きく損ねることになりました。ビットコインが提案された論文のタイトルは、“Bitcoin: A Peer-to-Peer Electronic Cash System”(ビットコイン : ピアツーピア電子決済システム) でした。その内容は、ブロックチェーンとよばれている分散型台帳技術を提唱しながら、それを利用したピアツーピア (Peer-to-Peer: コンピュータ同士がサーバを介さずに、直接相互通信をしてデータを共有する通信モデル) の電子決済システムとしてビットコインを提唱するというものでした。既存の金融システムは、政府や企業に自らの資産と個人情報を委託し、取引を代行してもらうというものですが、ビットコインでは資産の保有者自らが取引を作成、実施するということを提唱し、実現するというものでした。

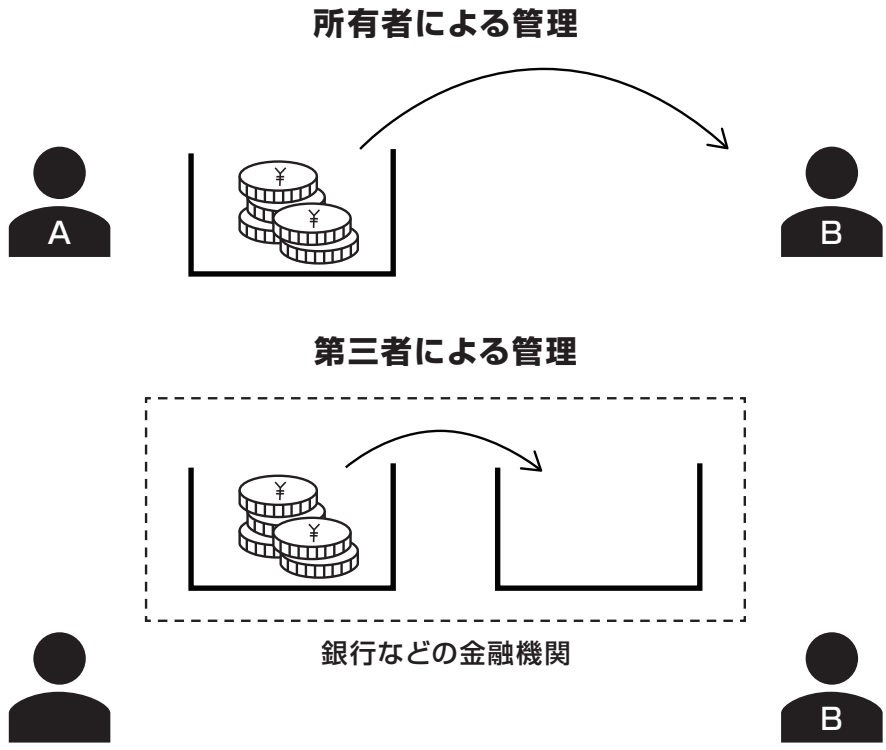


図1.1　資産の第三者管理と所有者管理の違い

1.1.1 情報の信頼性とは

現代は IT(Information Technology) が普及した高度情報化社会となり、インターネットを介して膨大な“情報”が流通しています。さらには IoT(Internet of Things) や AI(Artificial Intelligence) などにビッグデータなどが活用され、“情報”がますます価値を持つようになりました。ところで、そもそも“情報”とは何を意味するのでしょうか？

その定義は広辞苑によると、

(1) あることがらについてのしらせ

(2) 判断を下したり行動を起こしたりするために必要な、種々の媒体を介しての知識

とあります。

通常であれば人間生活において判断を下したり、行動を起こすための情報には、信頼性が求められます。情報が誤っていたり、偏っていたりした場合、その判断や行動は失敗に終わってしまう確率が高いからです。

まいました。すると両替商を中心に、現金取引や口頭取引ではなく、高い専門性を持った公証人によって記録された為替手形 (Bill of Exchange) をベースとした取引が見られるようになりました。

為替手形とは、手形の振出人 (発行者) に代わって、ある一定の期日において支払いを委託された第三者 (支払人) が指定の金額を受取人へ支払する義務を負うということを記した証書のことをいいます。この為替手形を利用した決済の登場はまさに情報の介在しない現金・口頭決済から、為替手形という情報そのものを介した決済への変化を意味しています。金や銀によって作られた貨幣と異なり、為替手形は紙などの素材で作られており、物理的な価値は低く、その情報自体に価値があると認められた場合にのみ取引が成立します。したがって当然のことながら為替手形の信頼性は高いことが求められます。新しいビジネスパートナーと新たな取引をする際に、お互いが公証人によって認められていない為替手形を提示したとしても受け入れることはできないでしょう。為替手形という情報は、信用性、専門性が高い公証人によって仲介されて、初めて信頼性がある情報としてそれぞれ受け入れられるのです。また取引当事者たちは、お互いを直接信頼することがなくとも、仲介人としての公証人をそれぞれが信頼していれば為替手形を介して取引をすることができるのです。この公証人の信頼はしばし、係争が発生した場合、最終的には証書通りの執行を強制できる、政府、裁判所、警察や軍隊などの暴力が伴う仲裁に裏付けられていたといわれています。

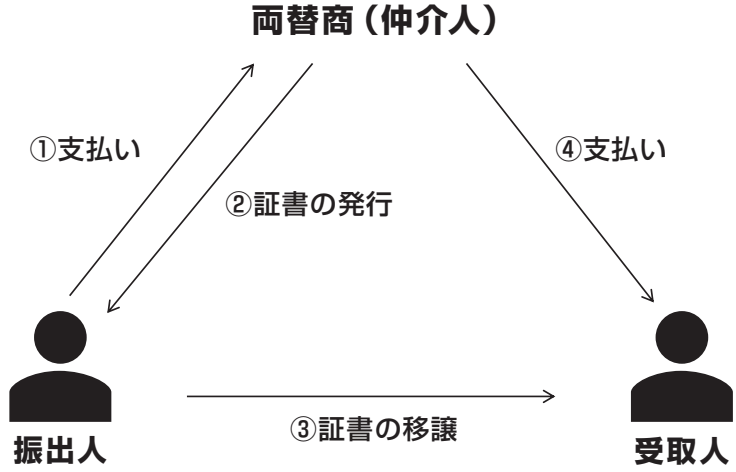


図1.2　信頼性を持った仲介による為替手形