

中学生にも分かる「ブロックチェーン」の仕組み

仮想通貨をめぐるニュースがよく見かける専門用語に「ブロックチェーン」がある。仮想通貨を支える中核的な仕組みだが、雑誌や本を読んでもコンピューター用語が難しく、なかなか理解が深まらない。インターネット以来の発明とさえ言われるが、一体どんな仕組みなのか。中学生にも分かるように専門家に解説してもらった。【井田純】

いきなり驚かすつもりはないが、この一文を読んでほしい。
△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

これが、関連企業などをつくる一般社団法人「日本ブロックチェーン協会」による「ブロックチェーン」の定義だ。この文章の意味が分かる人がどれくらいいるだろうか。昨年出版された「ブロックチェーンの未来」(日本経済新聞出版)の筆者の一人で、シンクタンク「NIRA総合研究開発機構」の林祐司主任研究員を訪ねた。

冒頭の定義について、林さんは苦笑交じりに説明する。「表現の仕方はいろいろあり、この通りに理解している人はかりではないと思います。私なりに言うと、ブロックチェーンとは「帳簿のイノベーション」(革新)です」

林さんは一般的な銀行を例に解説してくれた。「銀行の仕組みを突き詰めると「帳簿の管理」です。銀行では、メインコンピューターに全ての口座のあらゆる取引記録が収められている。「そこから個々の入出金記録などをアウトプットし、それぞれの通帳に記録しているだけです。ブロックチェーンでは、特定の誰かが情報を管理するのではなく、コンピューターのネットワークを通じて、過去の取引情報全てが書かれた帳簿を全ての参加者が持っている、というイメージです」

多くの利用者がデータを共有して互いに監視、改ざんや偽造などを防ぐという発想だ。銀行はメインコンピューターのデータを破壊されれば事実上おしまいなので、莫大なコストをかけて外部からの攻撃に備えています。ところが、ブロックチェーンは帳簿を分散し、偽造された記録と真正な記録を見分ける仕組みも備えているの

インターネット以来の大発明?

で、そのコストが必要ありません。一定の取引データをまとめた「ブロック」をコンピューター技術で「チェーン」状につなげたのがブロックチェーンだ。時間の経過とともにチェーンは延びていく。途中で改ざんしようとしても、ブロックをまとめてチェーンをつなげる作業には大量の計算を要するため、悪意ある一部の人間だけでつくるブロックチェーンを本物より長くすることはできない。容易

取引公開「仮想通貨」の信頼確保

そもそも通貨とは何か。貨幣経済が確立された古代ギリシャにさかのぼると、アリストテレスは主著「政治学」の中で、物々交換時代の後に必要なものを得る媒介として硬貨が発明された、と論じている。近代経済学の父とされるアダム・スミスも「国富論」の「貨幣の起源と使用について」の章で、自身の生産物以外の交換可能な商品を手もとにもっている「目的から貨幣が生まれた」と説く。

だが、「最近の研究では、物々交換から貨幣が生まれた、という理解は誤りだったという説が有力です」と指摘するのは、工学博士で金融コンサルタント会社を経営する尹熙元さんだ。

「ギリシャ時代に先立つメソポタミア文明では今でいう貨幣は存在せず、財の交換は、王の權威の

に見分けがつくのだ。

この技術は仮想通貨に限らず、さまざまな分野に応用されている。よく知られるようになったが、バルト3国の一つ、エストニアはブロックチェーンと同様の改ざん防止の仕組みを利用して「電子政府」を構築し、税金の申告や住民登録など多くの行政サービスに活用している。女性の地位向上を目指す国連機関「UNウィメン」も、国境を越えた移動を強いられる避

もと官僚制度に従って帳簿に記載される形で行われていました。これに対し、王や政府などの權威によらずに、個人の間に価値をやり取りしよう、というのが貨幣の始まり。通貨を「民主化」した仮想通貨は、むしろ貨幣本来の趣旨にかなっていると言えます。だが、法定通貨のように国家という確かな裏付けがないという点が何だか頼りない。「本当にそうでしょうか。戦争などの非常時には国家が通貨についての約束を簡単にほごにし、お金が紙くずになってしまふのは歴史を見ても明らかです」

では、仮想通貨の安全性をどこまで担保できる仕組みになっているのか。仮想通貨交換業者「コインチェック」から約580億円相当の仮想通貨「NEM(ネム)」が流出した問題では、同社のさ

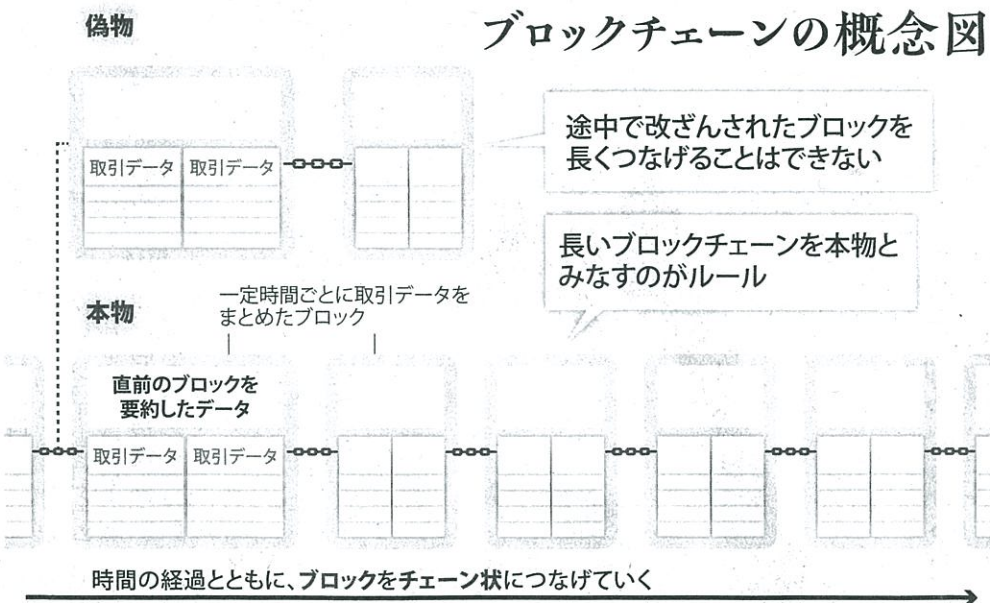
難民の医療記録・資産情報などの管理に、この技術が応用できないか検討を始めている。一部の専門家の間では、選挙の投票システムなどに活用できるとの声もある。そもそも、この技術を生んだのが、ビットコインという仮想通貨の仕組みだ。言うまでもなく、通貨の「実物」がどこかに存在するわけではない。形もなく、国が価値を保証してないもの、が、なぜ通貨として流通できるのか。

「円やドルなどのいわゆる法定通貨の価値を担保しているのは、国が発行しているという裏付けに

加えて、今手にしているこのお札が明日もあっても間違いなくお金として受け取ってもらえる、という確信です。一方、ビットコインの場合は、国の代わりにシステム自体で安全性を担保しようという発想。同時に、現在これだけビットコインが世界中で使われている、という偶然とした事実そのものが信頼を支えている、ということになります」(林さん)

22日時点で、ビットコインの時価総額は円に換算して約20兆円、仮想通貨約1500種の合計で約50兆円に上っている。

ブロックチェーンの概念図



※NIRA総合研究開発機構の資料を基に作成

「ダイヤモンドを預けていた宝石商に強盗が入ったから「ダイヤモンド」は危ない」と言うようなもの。国際法務を専門とする石角完爾弁護士は、仮想通貨に対する不信感には根拠がないとの立場だ。今回の流出問題では、取扱業者のセキュリティと仮想通貨の信頼性の問題が「ごっちゃ」にされてしまっている、と言う。「そもそも「仮想通貨」という訳自体、実体がないというイメージを与えるので不適切です。海外で使われている「クリプトカレンシー」(cryptocurrency)という単語は「暗号通貨」という意味です」

石角さんは昨年、「ビットコインは『金貨』になる」(朝日新聞出版)を刊行。現在の法定通貨の安定性に疑問を呈する一人だ。「こ

仮想通貨が何かを理解しないまま、一攫千金を狙って大丈夫なのか。前出の林さんは、ブロックチェーンが社会にもたらす恩恵について研究してきた立場からこう言う。「現在の投機的な動きについては懸念を覚えています。日本は今、仮想通貨に関する規制が世界で一番緩いと思われています。英国では政府がはるかに慎重ですし、米国ではAI(人工知能)などに比べるとシリコンバレーも盛り上がっていません」

林さん自身、現時点で仮想通貨取引を始めていないそうだ。有用性をよく知る専門家も慎重に見ているのが現状だということ、知

*この記事は毎日新聞社の許諾を得て転載しています。

毎日新聞社に無断で転載することは禁止されています。