

金融・資本市場とブロックチェーン

京都大学公共政策大学院教授 岩下直行

暗号資産とデジタル通貨

2017年に高騰して世間の耳目を集めたビットコインを始めとする暗号資産は、相場の乱高下を繰り返しながら、現在も数10兆円の流通総額を維持している。2019年には、フェイスブックのリブラ構想や中国のデジタル人民元といったデジタル通貨が世界中で注目された。ここ2、3年の間に、お金に関する常識を揺るがすような事件が相次ぎ、人々の認識も変わってきた。お金といえば当然現金を意味していた日本も大きく変化し、キャッシュレス決済が様々な局面で利用されるようになった。現金という物理媒体から電子決済へ、一国に閉じた法定通貨から国際的に利用可能なデジタル通貨へ、人々のお金に対するイメージは大きく変化している。

とはいえ、落ち着いて考えてみると、こうした変化はやや先走りした虚像のようにも思える。人々は、相変わらず昔ながらの銀行預金で給料を受け取っている。「未来のお金」と騒がれたビットコインは、未だに一般の商店の店頭で使われていない。国際的な資金決済に利用できるデジタル通貨は、まだ登場すらしていないのだ。

これらが全て虚像だと言いたいわけではない。むしろ、こうした現象の裏側には、大きな技術革新や、後戻りのできない社会の変貌が存在するのだろう。これらの新しい技術は、未来の金融・資本市場をどのように変えていくのだろうか。

ブロックチェーン技術

ブロックチェーンは、ビットコインなどの暗号資産の基盤となっている技術である。2008年、ナカモト・サトシを名乗る正体不明の人物が、インターネット上で利用可能な電子現金の論文を公表し、2009年には実際に稼働するプログ

ラムを公開して実験を開始した。ビットコインは、電子情報にデジタル署名を付与して権利者の意思を確認しながら、個人間における匿名での送金を実現しようという実験プロジェクトであった。会社を立ち上げるのではなく、インターネット上で実験への参加を募集し、コミュニティが自然に拡大していった。

ビットコインは、システム全体を「中央システムを持たない」形とし、中央組織による情報の独占を防ぐという思想に基づいて設計されている。金融業界においては、電子化された預金や有価証券の情報は、専用の中央システムに格納し、情報を厳格に保護するのが当たり前である。銀行の勘定系システムや証券保管振替機構がその役割を果たしている。しかし、ビットコインは、インターネットに接続された約一万台のパソコンで構築され、同じデータが共有されることで安定性を実現している。残高を専用システムで管理しないので、特別な保護は必要ない。これは革命的なアイデアであり、もしこの技術が既存の金融システムを代替すれば、金融・資本市場の常識が大きく変わることになるだろう。

とはいえ、中央システムを持たないシステムは、資産の二重譲渡を有効に防ぐことが難しい。特定の誰かが二重譲渡をチェックする仕組みとすると、「中央システムを持たない」という理念に反するし、チェックのためのシステムを安全に維持するコストも掛かる。そこでビットコインでは、利用者取引内容の検証を委ねることにした。ただし、その場合、二重譲渡した利用者自身が検証者を買って出て、自らの不正な取引を承認してしまうリスクがある。

その対策として、約10分に一度、取引の検証をしようとする者に大量の計算を必要とする課題を競争で解かせ、最初に正解した者に検証を担わせることにした。そのような負荷を担うような参加者であれば、検証者として信頼できるという考え方である。競争の勝者は、直前の検証者が作成したブロックに連鎖する新しいブロックを生成し、一定額の新しいビットコイン

を手に入れることができる。この一連の手順を「競争的マイニング」と呼ぶ。

会社組織でもなく、中心人物も不明のビットコインが、どこからも支援を受けず、10年以上稼働し続けてきたのは、こうした仕組みがあったことなのだ。

こうした技術の中身を見れば、ビットコインが採用したブロックチェーン技術が、どんな用途にでも使える魔法の杖ではないことが分かる。競争的マイニングを行わない、参加者を限定したブロックチェーンも提案されているが、それでは既存の中央システムを持つシステムと大差ない。

中央システムを持たないが故に、ビットコインは、規制や政治体制の違いを乗り越えて、世界中の人々に直接交換されるようになった。しかし、形だけビットコインに似せても、中央システムを持つデジタル通貨の場合、国境を越えて信頼されるとは限らない。これが、ビットコインと法定通貨の中間的なものを作り出すことが難しい理由の一つである。

ICOの光と影

ビットコインの高騰をながめて、世界中から何千もの暗号資産プロジェクトが提案された。それらの新しい暗号資産の中からも、高騰するものが相次いだ。特に、イーサリアムという流通総額第2位の暗号資産は、トークンと呼ばれるデジタル資産を発行するプラットフォームとして活用された。

このトークンを発行して資金調達を行う手法がICO (Initial Coin Offering) と呼ばれる。トークンは、株式のように配当を受け取る権利や経営参加権を持つものでもなく、社債のように期日が来れば償還されるものでもない。価値の有無も不明な、暗号資産の一種である。しかし、流通市場では発行価格の数倍で売買される事例が相次いだ。「トークンを発行市場で買って流通市場で売れば儲かる」という噂が暗号資産投資家の間に広まり、2017~18年には、全世界で2兆円とも3兆円ともいわれる資金がICOに流入した。

ICOという言葉はIPOをもじったもので、一見、両者は似ている。しかし、IPOには金融商品取引法の規制や上場審査の枠組みがあるのに対し、ICOにはそういった規制や枠組みは存在しない。ホワイトペーパーと呼ばれる事業

計画書を公表すれば、実体のないプロジェクトでも資金が調達できる。

首尾よくICOで資金調達に成功した発行体が、優れた製品・サービスを開発したのであれば、ICOにも存在意義はあるが、実際はそうではなかった。ホワイトペーパーを書いただけで大金を手に入れてしまった発行体の多くは、苦勞して事業を完遂しようとはしなかった。投資家も、流通市場でトークンを高く転売することばかりを考え、事業が最終的に成功するかどうかに関心はない。その結果、多くのICOプロジェクトは何も開発せず、そのまま自然消滅してしまった。結局、1年ほどでICOブームは去り、2019年以降、世界的に見てもICOはほとんど成功していない。

ICOに対する規制とSTO

このように様々な問題をはらむICOに対して、各国の規制当局が規制に乗り出した。米国では、SECがICOの一部は米国証券法上の有価証券の募集に該当するとの見解を表明した。明らかに詐欺と思われるICOを行った者を告発するといった対応も進めている。これを受けて、トークン発行者側が積極的に有価証券であることを認め、SECに対しRegulation Dなどによる証券募集の登録免除を申請する動きが出てきている。このようなトークン発行を、STO (Security Token Offering) と呼ぶ。

日本でも、ICO規制を織り込んだ改正金融商品取引法が2020年5月から施行されている。改正法では、暗号資産による出資など、収益分配を約して暗号資産の調達を行う「投資性を有するICO」について、金融商品取引法の規制対象となることを明確化した。これを、日本版STOと呼ぶ向きもある。なお、トークンの仲介業者には、発行者の事業、財務状況の審査が義務付けられている。

今回の法改正は、ICOの問題を証券規制で解決することが目的だったが、結果として、伝統的な証券市場にブロックチェーンという新しい基盤技術を導入可能にしたという側面もある。とはいえ、この領域においても、ブロックチェーン技術が魔法の杖である訳ではない。新しい技術が、規制回避のためではなく、真の利便性や効率性に繋がるのか、慎重に検討していくことが必要であろう。