英語版のファイナンス&ディベロップメントで人気企画だった「Back to Basics（基本に立ち返る）」シリーズ。2015年末に終了したこのコーナーですが、今号から連載を再開し、読者が日常生活で接する経済用語を解説します。また、ファイナンス&ディベロップメントのホームページからは「Back to Basics」のビデオシリーズもご覧いただけます。

ホームページ: www.fandd.org

暗号通貨とは何か

新しい形の貨幣となりうるものが、利益と同時にリスクをもたらしている

アントワーヌ・ブーヴレ　ヴィクラム・ハクサー

何百という暗号通貨が、プライムコイン、ダッシュ、ヴァージといった想像力に富んだ名前とともに姿を現している。テクノロジーに精通した人々の間では、カルトに近い支持者が増えつつある。暗号通貨の価値は、大きく変動する。謎に包まれたこれらのコンピューターコードの断片が、私たちが知る形の貨幣にいつか取って代わると考える人々もいる。暗号通貨とは正確には何か。暗号通貨に何らかの価値があると思わせる理由は何か。これらの問いに答えるために、まずは貨幣が遂げた進化に目を向けよう。

貨幣の利用

貨幣は、価値の貯蔵、財やサービスの交換手段、そして価値を測る計算単位として用いられる。貨幣のない時代、人類の社会では、財やサービスが直接交換されていた。1ブッシェルの種と1匹の豚を交換する、といった具合だ。これはあまり効率的ではなかった。社会が複雑化するにつれて、商品貨幣が使われるようになり、貝殻から銅、銀、金へと発展を遂げていった。一部の国では不換紙幣が導入された。支払いの約束以上に何の本源的価値も持たない紙幣である。唐王朝期にあった8世紀の中国の紙幣がその例だ。

多くの場合、初期の不換紙幣はあまり安定しておらず、広く受け取られてもいなかった。その紙幣の価値が発行者によって約束どおり保証されると人々が信じていなかったからだ。政府は物品の購入や賃金の引き上げのために、貨幣の発行量を増やそうという気を起こし、インフレを煽ることとなった。この点に関しては、第一次世界大戦後のドイツで、人々が手押し車で現金を運んでいた姿を思い起こして頂きたい。現代の中央銀行は、政府に代わって貨幣の供給を規制し、物価の安定を維持しようとしている。

簿記と台帳

金融システムの規模が拡大し、複雑化するにつれて、信用のある仲介者と信頼できる会計制度の必要性が高まった。ルネッサンス期のイタリアにおける複式簿記の開発という重要な技術革新の結果、民間の大手銀行の役割が強くなった。近代に入ると、中央銀行が決済システムの頂点に姿を現した。銀行台帳の電子化とともに、中央銀行が果たす調整の役割が大きくなった。

このような台帳はどのように機能するのか。金融機関は銀行内部の台帳で各口座の残高を取引に応じて調整し、中央銀行は中央台帳において金融機関同士の取引を有効にする。例えばメルナーズがA銀行にある自分の口座のお金を使って、B銀行に口座を持つメアリーから物を買うとする。A銀行はメルナーズの口座からその代金を引く。中央銀行はA銀行からB銀行へその金額を振り替え、中央台帳に取引を記録する。そしてB銀行はその金額をメアリーの口座に入金する。これから分かるように、このシステムの基盤となっているのは、中央銀行に対する信頼と、中央台帳の整合性を守り、同じお金が二度使われることを確実に防ぐその能力に対する信頼である。

アートワーク: THE NOUN PROJECT / MASSUPA KAEWGAHYA

その一方で多くの暗号通貨については、信頼された中央管理者は必要とされない。その代わりに暗号資産の拠り所となるのは、ブロックチェーンといった分散型台帳技術であり、この技術によってネットワークを通じて維持される台帳（データベース）が構築されている。同一の暗号通貨が二度払い出されることがないように、ネットワークのメンバーがコンピューティングと暗号化技術に基づくテクノロジーを使って取引を確かめ、承認する。ネットワーク内に分散するメンバー間で合意が形成された時点で、取引は台帳に追加され、確定される。この台帳には、特定の暗号通貨に関連する取引の包括的な履歴が永続的に記録されており、何者かが単独でこれを操作することは不可能だ。分散型ネットワーク上で口座間取引を承認し、合意を形成させるこの能力は、根本的な技術的変化である。

取引を確認し、承認するネットワークのメンバーは通常、新規に発行される暗号通貨によって報酬を得る。また多くの暗号通貨が、半匿名性を有している。通貨保有者は二つの鍵を持つ。一つはアカウントナンバーなどの公開鍵である。もう一つは秘密鍵で、取引を完了するために必要となる。先ほど挙げた例の続きで行くと、メルナーズが暗号資産を使ってメアリーから物を買おうとしている。そこで、彼女は自分の秘密鍵を使って取引を開始する。メルナーズはネットワーク上で、彼女の公開鍵「ABC」によって特定され、メアリーは彼女の公開鍵「XYZ」で特定される。ネットワークのメンバーは、ABCが、XYZに送金を希望する額を所有しているかを、暗号パズルを解読して確認する。このパズルが解かれれば、取引は承認され、この取引を表す新たなブロックがブロックチェーンに追加される。そして取引額は、ABCのウォレットからXYZのウォレットへと移転される。

利点とリスク

テクノロジーが理解できたところで、暗号資産の起源へと話を戻そう。最初の暗号資産、ビットコインは、2009年にサトシ・ナカモトという名義を使う一人のプログラマー（またはプログラマー集団）によってリリースされた。coinmarketcap.comによると、2018年4月の時点で1,500以上の暗号通貨の存在が確認された。ビットコインと並んで最も広く利用されているのは、イーサとリップルである。

一世を風靡しているにもかかわらず、暗号通貨はまだ、価値貯蔵、交換手段、価値尺度という貨幣の基本的機能を満たしていない。価値が非常に変動しやすいため、今までのところでは、価値尺度や価値貯蔵の手段としてはほとんど使うことができない。暗号通貨による支払いが受け付けられるケースが限られていることから、交換媒体としての利用も制限されている。法定不換紙幣と異なり、多くの暗号通貨は製造コストが高い。暗号パズルを解くコンピューターの電力として、大量のエネルギーが必要だからだ。さらに、分散型の発行ということは、資産を裏付けるものが誰もいないということを意味し、暗号資産の受け入れは完全に、利用者の信頼に基づくことになる。

分散型台帳技術によって、送金など国際的な資金移動のコストを削減し、金融包摂を促進できる可能性がある

暗号通貨とその基盤にあるテクロジーは、利益をもたらすと同時にリスクも含んでいる。分散型台帳技術によって、送金も含めた国際的資金移動のコストを削減し、金融包摂を促進できる可能性がある。海外への送金を数日間ではなくたった数時間で行える決済サービスも登場している。このテクノロジーは、金融システムの枠を超えて利益をもたらしうる。例えば、診療記録や土地の権利証といった重要な記録を安全に保管するために利用できる。一方で、大半の暗号通貨が持つ半匿名性は、取引の整合性や取引者の身元を確認する仲介機関が存在しないことから、資金洗浄やテロリストへの資金供与に使われるリスクを高めている。暗号通貨が通貨供給の制御に影響を及ぼし、それによって金融政策の実施に影響を与えるようになるとしたら、いずれ中央銀行に対しても課題が突き付けられる可能性がある。 FD

アントワーヌ・ブーヴレはIMF戦略政策審査局の**エコノミスト**、**ヴィクラム・ハクサー**は同局の局長補。