ブロックチェーンの仕組みとその可能性

ビットコインなどの暗号通貨の要素技術であるブロックチェーンは、欧米を中心とした多くの金融機関から新たな取引インフラとして注目されている。また、金融分野にとどまらず、広範な取引・契約管理インフラとしての試みも始まっている。

ブロックチェーンとは

ブロックチェーンはビットコインなどの分散型暗号通貨を支えるコアの技術である。その名の通り「取引の記録」をまとめた「ブロック」を「チェーン（鎖）」のように順次追加していく仕組みである。このブロックチェーンは「取引のすべてを記録した公開取引簿の作成・維持」を、低コストかつ金融機関や取引所といった中央集権的な機関を用いずにネットワーク上で実現するための極めて巧妙なアイデアだ。

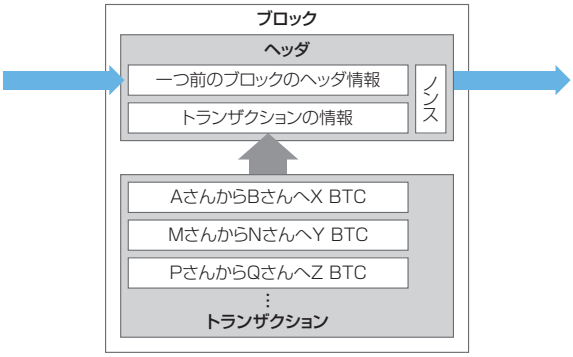
ブロックチェーンを構成するそれぞれの「ブロック」は、「そのブロックと一つ前のブロックに関する情報」を含む【ヘッダ】と、「ある時間内に行われたすべての取引のリスト」を記録した【トランザクション】という二つのパーツで構成されている。ブロックチェーンの仕組みを、ビットコインを例にして簡単に説明してみたい。

ブロックチェーンの仕組み（ビットコインでの例）

ビットコインではブロックチェーンは次のように利用されている。各ブロックの【トランザクション】には、ある時間内に行われたすべての取引が記録されている（平均でおおよそ10分ごとに1,000件程度の取引記録）。このリストに記録される取引記録は、「Aさんの口座からBさんの口座へXビットコインが支払われた」という個々の取引の情報である。

そして【ヘッダ】には、3つの情報が記録される。最初に直前のブロックの【ヘッダ】を圧縮した情報、ついで今回の取引リストを圧縮した【トランザクション】情報[1)]、そして最後に「ノンス」と呼ばれる「次のブロックを作るため」の情報、の3つである。

図表　ブロックと含まれる情報の概念図



（出所）Bitcoin.org等を参考に野村総合研究所作成

新たに生じる取引を記録するためには新たなブロックを作る必要がある。ビットコインでは新たなブロックを作るためには、ある特定の条件を満たす数値（この数値が「ノンス」である）を見つけなければならない。そして、この「ノンス」を見つけるためには膨大な計算が必要とされる[2)]。この「ノンス」を探しだす行為が金鉱を見つけ出す採掘作業に似ているため、「マイニング（採掘）」とも呼ばれている。

このマイニングの大変さをイメージしてもらうために以下のような例を考えてみたい。

> 例：「20,151,001」をn乗し、それを「4307」で割った余りが「1」になる最小のnを求めよ[3)]

試しに「20,151,001」を2乗すると、「406兆628億4,130万2,001」となり、それを「4307」で割った余りは「2,855」である。ついで3乗すると「81垓8,257京2,721兆1,394億6,345万3,001」という22桁の数になる。「4307」で割った余りは「3,140」だ。さて、実際に余りが「1」になるま

NOTE

1) 実際のビットコインの各ブロックの詳細はBlockchain.infoで見ることができる。（https://blockchain.info/ja）
2) 「ある条件」とは、【ヘッダ】と【トランザクション】に【ノンス】を加えた値でSHA256によってハッシュ値を計算した際に、頭に「ゼロ」が規定以上の個数並ぶという条件である。このような条件を満たす付加的な【ノンス】を見つけるための効率的な方法は見つかっておらず、総当りで計算する必要があると言われている。
3) 「20,151,001」は「2015年10月1日」、「4307」はNRIの証券コードである。
4) 20,151,001の174乗は10の後にゼロが1,270個並ぶくらいの大きさである。ちなみに全宇宙に存在する原子の数は10の80乗（10の後にゼロが80個）と推計されている。

で計算してみると、174乗したときに初めて余りは「1」になった[4)]。この時のnつまり「174」が「ノンス」に当たる数字である。

この「ノンス」を見つけて新たなブロックを作ってくれた人にはビットコインが付与される。2015年9月現在ではその額は25ビットコインとなっている（日本円に換算すると70万円程度）。これがビットコインを維持・拡大していくインセンティブの仕組みである。

ブロックチェーンには過去からのすべての取引記録が記録されているため、仮に不正を行おうとした場合、過去のすべてのブロックを書き換える必要がある。しかし、そのような書き換えを行なうには、ブロックチェーンの参加者全体に匹敵する規模の計算パワーが必要となる。そのため現実的にはブロックチェーンの改ざんはほぼ不可能である。この「改ざんが難しい」という性質がブロックチェーンの信頼を生み出している。

金融機関が注目するブロックチェーン

調査会社グリニッジアソシエイツが2015年7月に金融機関のエキスパート102名に行ったアンケート調査結果によると、回答者の約半数が「ビットコインやブロックチェーン技術に関するリサーチや事業への検討を行っている」と回答している。

またドイチェバンクは、ブロックチェーン技術は「有価証券の発行および移管」「有価証券の決済および清算」「有価証券の利回りや配当などの自動化」といったコアの金融業務への適用が可能との意見を公表した。

さらにもう一歩踏み込んで、ブロックチェーンの活用が金融業務に劇的な効率化をもたらすとする意見もある。サンタンデール・イノベンチャーズは、ブロックチェーンのアイデアに基づく分散型元帳管理を銀行業務に適用した場合、2022年までに銀行業務のコストを年間150億ドルから200億ドル削減できる可能性があるとのレポートを発表している。

取引所でもブロックチェーンの活用が検討されている。NASDAQはブロックチェーンを利用した未公開株式市場向けの分散型取引プラットフォームを構築するプロジェクトに着手しており、ブロックチェーンのスタートアップ企業であるChain.comと提携して年内の取引所開設を目指している。

ブロックチェーンの可能性：スマートコントラクト

ブロックチェーンをより広範囲の取引・契約管理インフラとして活用する試み（「スマートコントラクト」とも呼ばれる）も始まっている。英国Ethereum社は、金融以外でも活用できるブロックチェーンのプラットフォームの提供を開始した。同社のプラットフォーム上では、オンラインブックメーカーや、IBMなどが実験的にサービスを始めている。

ブロックチェーンは金融にとどまらず社会に大きな変革をもたらすことになるだろう。

Writer's Profile

柏木 亮二 Ryoji Kashiwagi
金融ITナビゲーション推進部
上級研究員
専門はIT事業戦略分析
focus@nri.co.jp