**新ビジネスの可能性広げるブロックチェーンの仕組み**

2017/11/22

**日本総合研究所副理事長　翁百合氏、東京大学大学院教授　柳川範之氏、京都大学公共政策大学院教授　岩下直行氏**

　仮想通貨ビットコインには、ブロックチェーンという画期的な技術が用いられている。その適用範囲は仮想通貨にとどまらず、世界のさまざまな企業や金融機関・政府が、この技術による多様なサービスの実証実験を行っている。この連載では、3回にわたってブロックチェーン技術の仕組みや主な種類、用途をまとめよう。第1回はブロックチェーン技術の仕組みについて説明する。

**新たなビジネスやデジタルガバメントの可能性が広がる**

|  |  |
| --- | --- |
| ・ | 日本国内でも使えるお店が増えてきた仮想通貨ビットコイン。この通貨を使えば、銀行を介さなくても、個人と個人との間で、低コストで直接送金ができる。国境や為替レートを気にする必要もない。 |
| ・ | ダイヤモンド取引の履歴情報がデジタルで管理される新しいビジネスモデルを作り出した英国ベンチャー企業のエバーレッジャー社。ダイヤモンドの透明で信頼できるマーケット形成に役立っている。 |

　これらには、実はブロックチェーンとよばれる画期的な技術が用いられている。ブロックチェーンは「帳簿のイノベーション」ともいわれる。これまで紙で記録していた取引の履歴情報などがすべて電子的に保管されるようになり、それを関係者が合意の上、分散して保有することが可能となった。その技術は仮想通貨だけにとどまらない。世界のさまざまな企業や金融機関、政府が、この技術を使った多様なサービスの実証実験を行っているのも、新たなビジネスやデジタルガバメントの可能性が広がると考えているからにほかならない。

|  |
| --- |
| http://bizgate.nikkei.co.jp/article/photo/brkchn2017-0103.jpg |

　たとえば、民間ビジネスでは、電子的に契約を記述した取引情報を取引参加者が分散して持ち合うことにより、付加価値の高いサービスを低コストで提供できる可能性が広がる。また行政においては、公共サービスの手続きがネット上で瞬時に完結することで、私たちの生活が飛躍的に便利になるかもしれない。現在の予想をはるかに超えた、これまでのビジネスの仕組みを大きく変えていく社会インフラとして機能することが期待できる。

　他方、ブロックチェーンの仕組みは複雑で技術的に未熟な部分もあり、慎重論が多く聞かれるのも事実であり、その解決に向け多様な取り組みが世界各国で行われている。

**●ブロックチェーンの仕組み：  
重要なコンセプトとフィロソフィー**

　ブロックチェーンという呼び名は、カネやモノの取引の履歴情報を電子的に記録しながら、そのデータをブロックとして集約、さらに連鎖（チェーン）して組成することに由来している（図表1）。

|  |
| --- |
| [**図表1　ブロックチェーンのイメージ**[http://bizgate.nikkei.co.jp/article/photo/brkchn2017-0101.png](javascript:void(0);)](javascript:void(0);) |

　ブロックチェーンの利用者は、パソコンや携帯端末などを使い、ブロックチェーンネットワークにアクセスする。幅広く活用されているブロックチェーンネットワークの多くはインターネットが使われている。ブロックチェーンを一言でいうと「取引の履歴情報をブロックチェーンネットワークに参加する全員が相互に分散して保管維持し、参加者がお互い合意をすることで、そのデータの正当性を保証する分散型台帳（Distributed Ledger）」となる。

　以下、もう少し詳しく説明していく。

#### 分散型台帳技術（DLT：Distributed Ledger Technology）： 取引のデータを複数の参加者が分散して管理する

　ブロックチェーンは、今までの帳簿または台帳の発想やコンセプトと何が異なるのだろうか。かつての台帳は、紙に取引内容を書き込むことによって管理されていた。近年では、紙に代わり、情報が電子化（デジタル化）されているものの、特定の組織や人が集中管理を行うという構造は同じである。たとえば、証券取引所などの中央機関が一箇所で管理する、いわば中央集権的な管理だ。

　実は、こうした管理によって引き起こされる問題がある。例にあげた取引所の場合、取引履歴データなどを記帳するためのシステムなどにコストや時間がかかり非効率なだけではなく、サイバー攻撃により情報が失われるというリスクがある。このため、システムダウンを想定したデータバックアップやBCP（ビジネス・コンティンジェンシー・プラン：事業継続計画）対策に多大なコストをかけているのが現状である。

　これに対して、ブロックチェーンの発想は、取引履歴を記録するデータベースをネットワーク参加者で分散して保有し、管理を行うというものだ（図表2）。複数のネットワーク上の参加者のコンピューター同士をPeer-to-Peer（※1）で直接接続し、モノやカネなどの取引情報を互いにやりとりして確認し、その履歴情報を共有し続ける（以下では、コンピューターをブロックチェーンの参加者という意味で、ノードという）。

|  |
| --- |
| [**図表2　集中処理と分散処理の違い**[http://bizgate.nikkei.co.jp/article/photo/brkchn2017-0102.png](javascript:void(0);)](javascript:void(0);) |

（※1）Peer-to-Peerとは、中央サーバーを用意せず、個々の端末（Peer）がお互いに接続し合うことで成立するネットワークのこと。

#### 参加者間の合意： 取引のデータの整合性について参加者はどう合意するのか

　カネやモノの取引データの整合性について、ネットワーク参加者間でどのように合意するのか。ブロックチェーンで使われている、合意を得るためのメカニズムをコンセンサス・アルゴリズム（合意形成のための計算方法）というが、合意にはさまざまな手法が存在する。

　仮想通貨ビットコインの場合、マイナー（採掘者）（※2）とよばれる人々が、自発的に電気代を大量に費消してコンピューターに計算をさせて答えを出す「マイニング（採掘）」競争をする。その計算競争の勝利者は、その答えとともに、ビットコインによる送金データの塊をブロックとして承認し、参加者へ伝播する。こうした競争によって承認された取引であることを証明する仕組みをプルーフ・オブ・ワーク（PoW：Proof of Work）という。

（※2）マイニングビジネスに投資をしている人は世界各国におり、手がけている会社は多いが、10社程度がその大半を占めており、電気代が安いため、マイニング作業の多くは中国で行われている。

　承認された内容は、それぞれの端末に記録として保存されていく。こうした承認行為には、マイナーが正当な承認を行うと手数料を得られることで計算競争への参加意欲を持つと同時に、その競争下では不正を働くためのコストが膨大なものとなるという経済インセンティブを内包させることで不正も抑止している。ビットコインタイプのブロックチェーンは、この参加者間の競争的なチェックという革新的なメカニズムによって、悪意のある参加者が存在しうる環境下においても不正を許さない仮想通貨を生み出した。

　そして、承認されたすべての記録が、台帳として整合性を保った状態で存在し共有されている。整合性について最終的に合意する具体的な仕組みは以下の通りである。

　マイニング競争の勝利者が承認したブロックを受信した各端末ではこれを検証し、不整合がなければ承認されたものとして取り込む。ただし、不整合がある場合にはこれをはじく。まれに（複数のマイナーにより）答えがほぼ同時に見つかり、各端末が複数のブロックを受信することがある。

　こうした場合にはチェーンが分岐して、どちらも正しく承認された正当なチェーンといえる状況となってしまう。だが、ビットコインでは「最も長く連なったチェーンを正しいチェーンとみなす」というルールを決めてあるため、しばらく（※3）待てば、最長のチェーンが適正であると判断することができる。分岐が起きると、いわば二重支払いといえる状況になるが、結果として長いチェーンを採用すれば、一方の支払いのみを採用する判断が可能だ。

（※3）通常1承認あたり平均10分かかるが、確定するためには、確率的に6回の承認（6ブロック、約60分）以上待つことが求められている。

#### ブロックチェーンネットワーク上での取引： 国境を越えてカネ、モノの取引を展開

　ブロックチェーンがこのように透明で、かつフラットなネットワークの仕組みを基盤としているのは、その根底に草の根的・民主主義的なコンセプトがあるからだ。そもそもブロックチェーンはビットコインを起源とした技術であり、中央集権的な組織や国に依存しない取引の実現を目指して生まれたものなのである。

　ブロックチェーンの特徴の一つに、参加する全員が安全かつ平等に、分散的に情報を共有化しながら「つながり」を実現でき、グローバルにネットワーク展開できるインフラとして機能する、というものがある。誰でも参加できるタイプのブロックチェーンの場合、ノードである構成員は、カネ、モノの取引を、国境を越えて自由に展開でき、世界中どこにいても参加することができる。

　さらにノードが増え、ブロックチェーンのネットワークが拡大すればするほど、影響力が指数関数的に拡大していくという、いわゆるネットワーク効果を発揮することが可能となる。

#### ブロックチェーンと分散型台帳技術（DLT）

　なお、本書では、ブロックチェーン技術を「分散型台帳技術」として紹介しているが、ブロックチェーン技術と分散型台帳技術（DLT）を分けて解説している文献などもあるので、この点について若干敷衍（ふえん）しておきたい。

　仮想通貨ビットコインが注目され、さまざまな仮想通貨が開発されるようになり、その技術面が着目されるようになったが、その技術がブロックチェーンと総称され、注目を浴びるようになった。その基礎的な特徴の一つに分散型台帳があることはすでに述べた通りである。しかし、現在は仮想通貨以外にもブロックチェーン技術は使われるようになった。ブロックチェーン＝仮想通貨という認識が強かったため、仮想通貨以外に使われている同様の技術については、ブロックチェーン技術という用語を使わずに、汎用性のある分散型台帳技術という用語が使われていることがある。

　すなわち、ブロックチェーンという用語は比較的仮想通貨に使われるケースが多く、その応用としてさまざまな場面（金融機関、企業、政府など）で使われる技術として分散型台帳技術という用語が用いられている。

　たとえば、英国政府科学局から2016年1月に公表された報告書（"Distributed Ledger Technology: beyond block chain"）（※4）でも、ビットコインを中心とする技術を狭義のブロックチェーンとよび、仮想通貨から広く一般的な適用が拡大している技術として、分散型台帳技術を位置づけている。

　しかし、この定義の違いについては広く合意されたものがあるわけではない（※5）。ここでも、分散型台帳技術も含めてブロックチェーン技術と総称している。

（※4）NIRA 総研ホームページより日本語訳が入手できる。

（※5）たとえば、日本ブロックチェーン協会（JBA）は、以下のような狭義、広義のブロックチェーンの定義を提唱している。

「・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 に収束するプロトコル、またはその実装をブロックチェーンと呼ぶ。  
・電子署名とハッシュポインタを使用し、改竄検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ」。

##### ブロックチェーンの未来 金融・産業・社会はどう変わるのか

翁 百合・柳川範之・岩下直行 編著  
出版：日本経済新聞出版社  
価格：2,160円(税込)