

ブロックチェーンの将来性とインパクト

中島 真志 麗澤大学 経済学部 教授



はじめに

ビットコインをはじめとする仮想通貨については、2017 年末にかけての価格急騰のあと価格が下落に転じる中で、「夢の通貨」としての期待感や斬新な仕組みに対する一時的な高揚感が後退してきている。一方で、ビットコインを支えるための技術として開発された「ブロックチェーン」については、「インターネット以来の最大の発明」ともされており、幅広い分野で活用できる技術としての期待が高まっている。

本稿では、ブロックチェーンの今後の将来性とそれがもたらす影響について考察することとした。

ブロックチェーンとは

ブロックチェーンは、もともと世界初の仮想通貨である「ビットコイン」を支えるための中核技術として開発されたものであり、「ブロック」と呼ばれる取引データの固まりを一定時間ごとに生成し、時系列的に鎖（チェーン）のようにつなげていくことにより、データを保管するデータベースの技術である。ブロック（データの集まり）をつなげていく形態がチェーンのように見えることから、「ブロックチェーン」と呼ばれている【図表 1】。

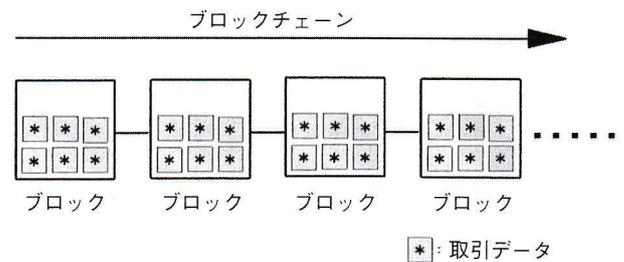
当初は、ビットコインのために開発されたブロックチェーンであるが、これは、ブロックチェーンの最初の実用例がたまたまビットコインであっただけであり、また、かなり特殊な適用例であったものとみられるようになっている。

つまり、ブロックチェーンは、データを管理するための「帳簿の技術」であるため、対象とするデータは、必ずしも仮想通貨のデータに限られることはなく、さ

まざまなデータの管理に应用が可能であることに多くの人が気が付き始めている。すなわち、「ビットコインが中心の世界」から「ブロックチェーンが主役の世界」へと移行してきているのである【図表 2】。

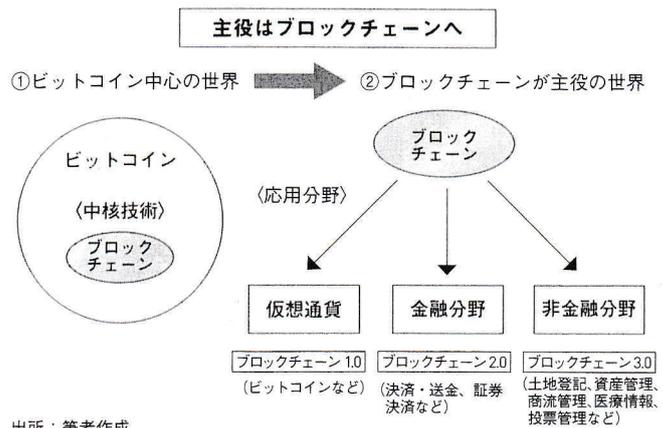
ブロックチェーンの应用分野については、①仮想通貨に应用する場合を「ブロックチェーン 1.0」と呼ぶのに対して、②金融分野（仮想通貨以外）に应用する場合を「ブロックチェーン 2.0」、③非金融分野（土地登記、商流管理、医療情報など）に应用する場合を「ブロックチェーン 3.0」と分類するようになっている。

図表 1 ブロックチェーンの概念図



出所：筆者作成

図表 2 ビットコインとブロックチェーンの関係



ブロックチェーンから分散型台帳技術へ

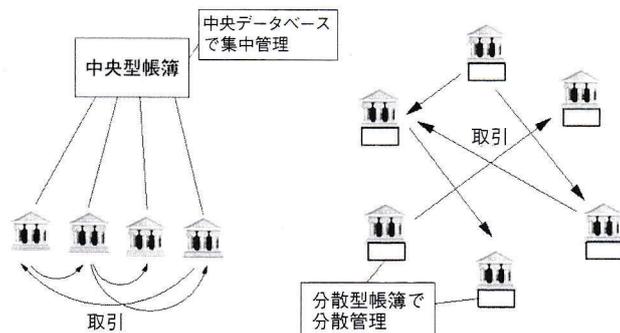
ブロックチェーンは、取引記録を鎖のようにつなげて管理する仕組みであるため、すべての取引履歴が記録された、いわば巨大な帳簿となっている。そして、ネットワーク内の参加者が各自の持っている帳簿を同時に書き換えていくかたちで、取引の記録（所有権の移転）が行われる。これは、ネットワーク内の参加者が、所有権の記録を分散して管理できるようになることを意味する。つまり、ブロックチェーンを使うと、各種のデータをネットワーク上の分散されたデータベースで、分散的に管理することが可能となる。

このため、最近では、ブロックチェーン技術のことを「分散型台帳技術」(DLT: Distributed Ledger Technology)と呼ぶことが多くなっている。「ブロックチェーン」というのが、技術的な面からみたネーミングであるのに対して、「DLT」というのは、この技術の利用方法からみた名称であり、この方がユーザーからみたメリットが分かりやすいものと言えるだろう。

従来は、取引などの記録を「信頼できる第三者」が中央型帳簿（中央データベース）を使って集中的に管理するというのが一般的な方法であった【図表3の①】。これを、分散型台帳を使って、各ユーザーが分散して管理できるようになれば、さまざまな取引をリアルタイムに、しかも劇的に低いコストで行うことができるようになるものと期待されている【図表3の②】。

図表3 ブロックチェーンから分散型台帳技術へ

①中央型帳簿による集中管理 ②ブロックチェーンを使った分散的な管理



出所：筆者作成

つまり、「中央型帳簿」（セントラル・レジャラー）から「分散型帳簿」（ディストリビューテッド・レジャラー）に移行することにより、データの管理手法に画期的なイノベーションが起きるのではないかとみられるようになっているのである。

ブロックチェーンのメリット

ブロックチェーン（DLT）のメリットとしては、大きく以下の3点を挙げることができる。

①不正取引・データの改ざんができない

ブロックチェーンでは、新しいブロックを作るときには、1つ前のブロックの「ハッシュ値」（ブロック内のデータを圧縮した値）を含めるという仕組みをとっている。このため、過去に作ったデータを改ざんしたとすると、そのブロックのハッシュ値が変わってしまい、それによってその次のブロックのハッシュ値も、そしてその次のブロックのハッシュ値も、という形で次々に変わってしまうことになる。こうしたブロック間のデータの連携（シンクロナイズ）により、ブロックチェーンでは、過去の取引データを改ざんすることが極めて困難となっている。

②システムダウンに強い

ブロックチェーンでは、ネットワーク上の多くのコンピュータが同じデータを分散して管理している。このため、どこか1カ所のコンピュータが壊れたとしても、他の参加者のコンピュータが動いているため、システム全体が障害になることはない。このため、障害に強く、ダウンしにくいシステムとなる。

③運用コストが安い

ブロックチェーンが注目される最大の理由は、それが劇的なコストの削減につながる可能性があるためである。中央集中型のシステムでは、巨大なコンピュータ・センターが必要であり、またそれをバックアップするために同等なシステムも保有する必要があり、こうした大規模なデータ・センターの構築・運用のために巨額のコストがかかっている。これが、分散型台帳に移行することになれば、より小規模な

分散型のコンピュータで済むことになり、低コストでの取引が可能になるものとみられる。

ブロックチェーンの2つのタイプ

ブロックチェーンには、大きく「オープン型」と「クローズド型」という2つのタイプがある。実用化を考える上では、この2つを明確に区別しておくことが非常に重要である。

①誰でも参加できる「オープン型」

「オープン型」のブロックチェーンは、参加者を限定せずに、誰でもネットワークに参加できるようにしているものである。参加者は匿名でネットワークに参加することができ、取引の承認作業についても、誰もが自由に行うことができる。スキーム全体を管理する中央管理者はおらず、プログラムがコントロールを行う。

こうした仕組みは、まさにビットコインで採用されているスキームであり、一般に開放されているという意味で「パブリック型」とも呼ばれる。

②特定の参加者のみの「クローズド型」

これに対して、特定の参加者のみが参加できるようにしたものを「クローズド型」のブロックチェーンと呼ぶ。クローズド型では、参加者の身元はすべて明らかになっており（匿名性はない）、取引の承認も特定範囲の参加者のみが行うことができる。さらに、スキーム全体をコントロールする中央の管理主体が存在しており、この中央管理者が参加者の範

図表4 ブロックチェーンの2つのタイプ

	オープン型	クローズド型
取引参加者の制限	なし (自由に参加可)	あり (特定の範囲の参加者のみ)
取引承認への参加の制限	なし (自由に参加可)	あり (特定の範囲の参加者のみ)
中央管理者の存在	なし (プログラムが規定)	あり (全体をコントロール)
ネットワークへの参加	自由	承認が必要
別の呼び方	パブリック型 許可不要型	プライベート型 許可型
利用例	仮想通貨 (ビットコインなど)	金融界での実証実験

出所：筆者作成

囲を決めるなど、全体の仕組みを管理し、運営を行う。こうした仕組みは「プライベート型」とも呼ばれる。

③オープン型とクローズド型の区別はなぜ重要か

オープン型とクローズド型の区別が重要なのは、その選択が、採用する「コンセンサス・アルゴリズム」と密接に関係しているためである。コンセンサス・アルゴリズムとは、取引が行われたあとで、ネットワーク上に分散した多数の台帳でデータの変更を承認し、全員で共有するためのプロセスである。

ビットコインのようなオープン型では、誰でもネットワークに参加できるため、取引データを改ざんして不正なブロックを作成しようとする「悪意の参加者」が入ってくる可能性がある。このため、取引の承認には時間を要する厳格な手続きが必要となる。

一方、クローズド型であれば、許可を受けた信頼できる主体のみが参加者となるため、悪意の参加者の可能性は少なく、より迅速で簡便な方法によって取引の承認を行っていくことが可能となる。

現在、金融界では、数多くのブロックチェーンの実証実験が行われているが、その殆どは、参加者を限定したクローズド型によって行われている。クローズド型は、信頼できる者同士のネットワークであるため、①取引の承認に膨大な手間をかける必要がなく、短期間に大量の処理を行うことができる、②ファイナリティ（決済完了性）を確定させることができる、などのメリットがある。

このため、今後のブロックチェーンの実用化にあたっては、クローズド型が主流になっていくものとみられる。ブロックチェーンについて検討する際には、どうしてもビットコインのイメージに引きずられて、オープン型を前提とした議論になりがちであるため、両者の区別については十分な注意を払っていく必要がある。

金融分野における ブロックチェーン活用の動き

ブロックチェーンは、初めに仮想通貨において利用されたこともあり、現在、最も活発にブロックチェーンの利用を模索しているのが金融業界であ

る。さまざまな金融分野への応用が考えられているが、ここでは、その事例を2つ挙げることにしよう。

①ブロックチェーンによる国際送金革命

まず、1つ目が「国際送金」である。国際送金については、これまで利用者から、「遅い」（相手に着金するまでに時間がかかる）、「高い」（少額の送金にも高い手数料がかかる）、「分かりにくい」（手数料の体系が不透明）といった不満の声があった。

これには理由がある。国境をまたいだクロスボーダーの資金移動には、国内決済における中央銀行のような、中央で資金の流れをすべてコントロールする統一的な中央機関が存在していない。このため、各銀行は、海外の「コルレス銀行」との間で個別に契約を結んで、送金を1件ごとに個別で処理している。こうしたコルレス銀行間の送金メッセージの通信には、「SWIFT」という国際的なネットワークが使われている。

こうした国際送金の非効率性をブロックチェーンの技術を使って解決しようとしているのが、「リップル」というプロジェクトである。リップルでは、参加行同士がネットワークで直接つながり、分散型台帳で情報を共有しつつ、送金を行うというモデルを構築している【図表5】。

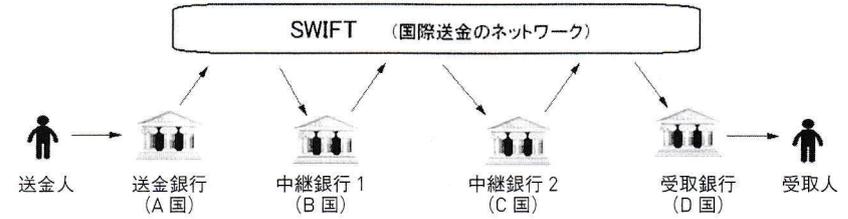
スペインの銀行による実証実験では、リップルの仕組みを使うことにより、これまで4日間を要していたスペインからメキシコへの送金がわずか数秒で着金し、送金コストも40%以下に削減できたという結果が得られている。こうした国際送金を効率化しようとするリップルのプロジェクトには、世界の大手銀行を中心に、160行以上が参加の意向を表明しており、わが国からもメガ3行が参加の予定である。今後、リップルのネットワーク上で稼働する銀行が増えれば、国際送金の世界が大きく変わっていく可能性がある。

②貿易金融へのブロックチェーンの活用

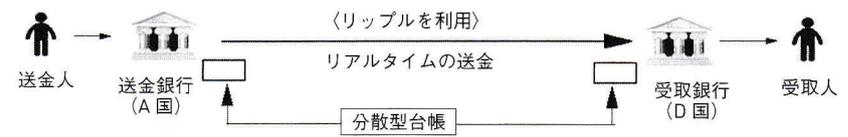
これまで、非効率性が残っていたもう1つの金融

図表5 リップルの送金モデル

①従来のコルレス銀行を使ったモデル（2～4日）



②リップルのモデル（リアルタイム）



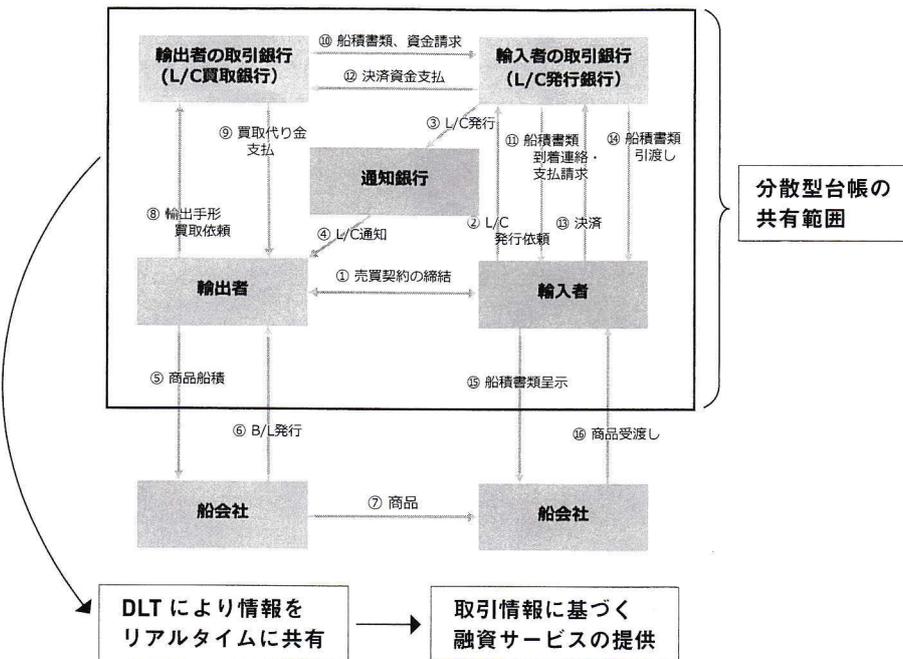
出所：筆者作成

分野として「貿易金融」（トレード・ファイナンス）を挙げることができる。貿易金融においては、輸出者と輸入者、そして輸出者の取引銀行と輸入者の取引銀行という複数の当事者が必要となる。そして、こうした当事者間で、信用状(L/C)や船荷証券、パッキングリストなど各種の紙の書類を受け渡しすることが必要となっている。こうした各種の書類の授受は、受け取る都度に人手によるチェックが必要なことや、遠隔地間の郵送に日数を要することなどから、2～3週間といったかなりの日数と高い処理コストが必要な非効率なプロセスとなっている【図表6】。

こうした非効率性を、ブロックチェーンを使って効率化しようとするプロジェクトが、北米やアジア、欧州などで数多く立ち上がっている。これらのプロジェクトでは、関係者をブロックチェーンのネットワークでつなぎ、それぞれの関係者が書類の作成や手続きを行う都度に、更新した情報を分散型台帳に記録して同時に共有化していく。これによって、必要なデータをリアルタイムに共有しつつ、各関係者が同時並行的に作業を進めていくことができ、処理時間の短縮化とペーパーレス化を実現することが可能となっている。

多くのプロジェクトは実証実験の段階にあるが、ドイツ銀行、HSBC銀行など欧州の9つの大手銀行が進めている「ウィ・トレード」というプロジェクトでは、2018年7月に、5カ国間で実際の貿易取引を成功させており、一足先に実用化のフェーズへと進んでいる。

図表 6 貿易金融へのブロックチェーンの利用



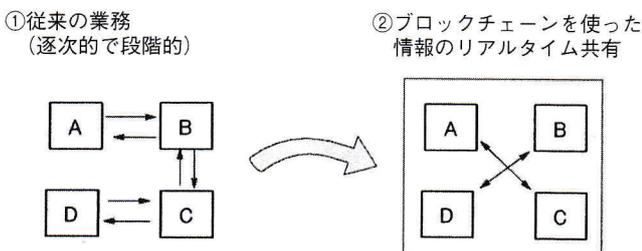
出所：SMBC 資料に加筆修正

ブロックチェーンに適した業務とは

ここで金融業界を離れて、より幅広い観点から、どのような業務がブロックチェーンに向いているのかについて考察してみたい。

まず第1に、複数の当事者が同じ情報をリアルタイムで共有することによって、効率化を図ることができる業務である。従来の業務においては、複数の当事者間で情報の伝達が逐次的に行われ、情報が伝えられるごとに段階的に業務が進められるといった業務フローが多数存在している。ブロックチェーンでは、分散的なデータベースの管理により、関係者がリアルタイムに同じ情報を共有できるため、こうした業務における効率性が飛躍的に向上することになる【図表7】。上述した貿易金融は、業務が逐次

図表 7 ブロックチェーンによるリアルタイムの情報共有



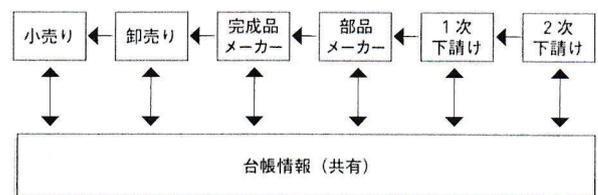
出所：筆者作成

的で段階的に進められている典型的な事例である。この他にも、こうした複数の当事者による逐次的な業務は、身近に多く見つかるのではないだろうか。

第2に、取引履歴を改ざんされない形で、長期間保存していくことが必要な業務である。これは、「追跡可能性」(トレーサビリティ)の確保が必要な業務と言い換えることもできる。すでに、エバーレジャー社という企業が、ダイヤモンドの取引履歴を管理する業務を開始している。また、不動産の登記についても応用が考えられており、スウェーデン、ウクライナなどで実証実験が行われている。この

のほかに、食品の流通経路への応用が考えられている。ここにブロックチェーンを導入すれば、生産段階から加工段階、流通段階まで、いつ、どこで誰が生産や加工を行ったかをデータベースに記録して関係者で共有し、必要な場合には瞬時のうちにトレースすることが可能となる。また、これを製造業で行えば、「サプライチェーン・マネジメント」になり、原材料、部品から完成品に至るまでのプロセスや、受発注、在庫管理、配送などの一連の流れを関係者間で共有しながら、統合して管理することが可能となる【図表8】。すでに、自動車メーカー(アウディ、フォードなど)、家電メーカー(サムスン電子など)において、各種の実証実験が行われており、物流コストの削減などにつながる事が確認されている。

図表 8 サプライチェーン・マネジメントにおけるブロックチェーンの利用

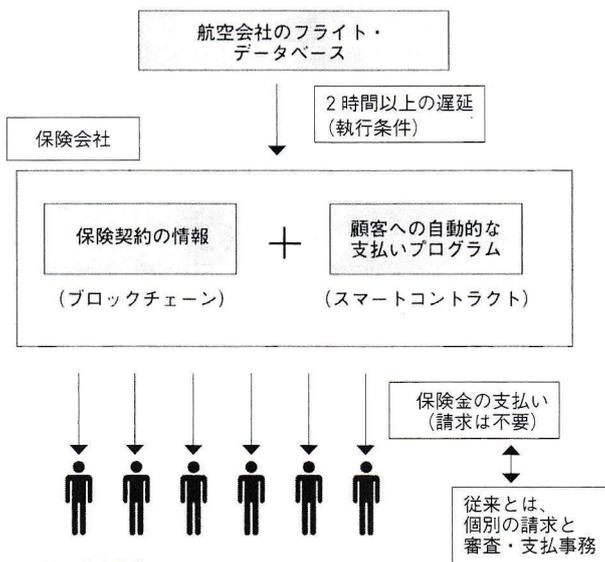


出所：筆者作成

第3に、「スマートコントラクト」が利用できる業務を挙げることができる。スマートコントラクトとは、「プログラム化して自動的に実行できる契約のこと」であり、ブロックチェーン技術と組み合わせて利用することができる。スマートコントラクトでは、①「執行条件」と「契約の内容」を、あらかじめ定義してプログラム化しておき、②執行条件に合致したイベントが発生した場合には、契約が自動的に執行される。これを利用した仕組みとして「フライトの遅延保険」がある【図表9】。この保険では、航空会社のフライト・データベースと保険会社のシステムをつないでおき、保険の支払条件（たとえば2時間以上の遅延）が発生した場合には、スマートコントラクトにより、顧客に対して自動的に支払いが行われる。そこでは、顧客がいちいち保険金の支払請求を行ったり、保険会社で請求の1件ごとに審査を行ったりという手間が不要であり、顧客と保険会社の双方で大幅な合理化が図られることになる。この保険は、すでにフランスの大手保険会社であるAXA（アクサ）が実用化している。

このようにデータの数値に基づいて自動的に支払いを行う保険のことを「パラメトリック保険」というが、今後、スマートコントラクトの普及により、こうした保険が拡大していく可能性があるものとみられる。

図表9 フライト遅延保険におけるスマートコントラクトの利用



出所：筆者作成

おわりに

ブロックチェーンの利用を考える場合には、「技術主導」の考え方ではうまくいかないものとみられる。新しい技術が出てきたから何かに使えないか、ブームに乗ってどこかに使えないか、といった発想ではプロジェクトの成功はおぼつかない。新技術の利用は、あくまでも「課題の解決」(ソリューション)のためでなくてはならない。そのためには、「ニーズ主導」の考え方が必要であり、「手間がかかっていて、非効率な業務は何か」ということを考え抜いた上で、現状の課題をブロックチェーンによって解決できないかを検討していく必要がある。金融分野において、国際送金や貿易金融など、いずれも非効率で高コストであった業務に、ブロックチェーンの応用が考えられているのは、こうしたアプローチの典型的な事例である。

あくまでも、「必要性が主であり」、「技術は従である」ということを念頭に置いた上で、自社の関係する業務において、ブロックチェーンを利用できないかを考えていく必要があるだろう。

金融に関する「ブロックチェーン2.0」が進めば、今後、金融業務が大きく変わっていくことは、まず間違いないものとみられる。また、金融の枠を超えて「ブロックチェーン3.0」が普及していけば、不動産、医療、物流、行政、食の安全性、選挙など広範囲にわたって、人々の生活を大きく変えていく可能性が高いものとみられる。ブロックチェーンの広がりや速度と、それがもたらすインパクトには、今後とも注目していく必要があるだろう。

中島 真志 [なかじま まさし]

1958年生まれ。1981年一橋大学を卒業。同年に日本銀行に入行。調査統計局、金融研究所、国際局、金融機構局、国際決済銀行(BIS)などを経て現職。博士(経済学)。早稲田大学非常勤講師。単著として、『SWIFTのすべて』『外為決済とCLS銀行』『入門 企業金融論』、共著として、『決済システムのすべて』『証券決済システムのすべて』『金融読本』などがある。決済分野を代表する有識者として、金融庁や全銀ネットの審議会などにも数多く参加している。最新刊の『アフター・ビットコイン』(新潮社)は、ビットコインとブロックチェーンを扱った1冊として注目され、約5万部のベストセラーとなっている。