特集　デジタルが拓く金融の近未来像

ブロックチェーン技術がもたらすデジタル通貨の未来

西片健郎

CONTENTS

要　約

1　ビットコインをはじめとする暗号通貨、それを支えるブロックチェーン・分散台帳技術への注目が高まる中、デジタル通貨の調査研究や実証実験が世界中で進んでいる。

2　現在、主に利用されている預金通貨を支える決済システムは、①銀行や中央銀行などの単一の信頼できる第三者機関が単一の台帳を管理している点、②複数の異なる台帳が存在する点、③台帳が階層構造となっている点、に特徴がある。

3　ビットコインは、さまざまな課題があるものの、①信頼できる第三者機関なしに複数の主体で単一の台帳を管理している点、②台帳が階層構造を持たない点、③単一の主体の判断では実質的に台帳のデータやプロセスの変更ができない点、を特徴とする新たな決済システム方式の可能性を示した。

4　ビットコインを支える技術の汎用化・標準を目指すさまざまな技術開発が進んでおり、この技術の総称がブロックチェーン・分散台帳技術と呼ばれている。ブロックチェーン・分散台帳技術をベースとする次世代決済システムは、中央集権型の決済システムに比べて、①システム全体の効率化、②決済リスクの削減、③透明性の向上、④金融サービスの多様化といったユニークなメリットをもたらし得る。

5　これらのメリットを活かしながら、ブロックチェーン・分散台帳技術を新たな決済システムとして活用していくためには、ユースケースの模索により活用メリットと要件を洗い出し、制度的･技術的課題に対して国際的かつ中長期的に取り組んでいくことが求められる。

Ⅰ デジタル通貨への関心の高まり

暗号通貨とそれを支える技術であるブロックチェーン・分散台帳技術への関心の高まりとともに、デジタル通貨に関する調査研究、実証実験が世界中のさまざまなレベルで進んでいる。

ビットコインをはじめとする暗号通貨は、さまざまなものが台頭してきており、投機的な取引の増加による価格の乱高下、各国の規制当局の動きのほか、取引所や暗号通貨自体の脆弱性を突く事件、詐欺事件などが世間を騒がせている。世界各国の中央銀行では、英国、カナダ、スウェーデン、シンガポール、中国などをはじめとして、中央銀行自身によるデジタル通貨発行に関する研究が進んでいる。2017年11月に、ウルグアイが一般向けデジタル通貨のテスト運用の開始を発表して世界を驚かせたことは記憶に新しい。民間の金融機関においても、銀行間の決済に用いるデジタル通貨や、銀行が一般向けに発行するデジタル通貨の取り組みが活発である。

このようにさまざまな動きがある一方で、そもそもデジタル通貨とは何なのか、また同時に語られることの多いブロックチェーン・分散台帳技術は、デジタル通貨にどのような影響を与えるのかについて、整理して述べられた文献は少ない。

本稿では、まず通貨および通貨を支える決済システムの歴史と現状を俯瞰した上で、新たな決済システムとしてのブロックチェーン・分散台帳技術の位置づけと革新性を明らかにする。その上で、新たな決済システムが開くデジタル通貨の可能性、新たな決済システムの課題について考察したい。

Ⅱ 通貨の性質と形態

古代メソポタミアでは、ハンムラビ法典に見られるように、さまざまな財の価値の尺度に銀が利用されていたとされる。ミクロネシアにあるヤップ島では、ライと呼ばれる巨大な石が貨幣として用いられてきた。翻って、われわれが日常利用する現代の通貨のほとんどはデジタル化されており、形を持たない。このように通貨は多様な姿を見せるが、通貨とは果たして一体何なのであろうか。

通貨の定義は、①価値の尺度、②価値の交換手段、③価値の保存手段の３つの性質を満たすものという、経済的機能に着目した定義がよく知られており、本稿でもこの定義に従うこととしたい。また、同じ意味で使われる用語に「貨幣」「お金」などの用語もあるが、本稿では「通貨」という用語に統一する。

通貨の形態は、歴史を振り返ると技術革新や時代背景に合わせて進化してきたことが分かる。古くは石や貝殻などに始まり、持ち運びや分割の容易性から次第に金や銀などが用いられるようになり、その後、鋳造技術が発達すると硬貨が利用されるようになったと考えられている。現存する最古の鋳造硬貨は、紀元前7世紀にリディア王国で利用されていたエレクトロン貨であるといわれる。その後、両替商が金属や硬貨を預かる見返りとして預り証を発行するようになり、さらに印刷技術の普及と相まって、金属との交換が保証された紙幣（兌換紙幣）が流通するようになったとされる。

現代では、金属との兌換が保証されない紙幣（不換紙幣）が流通するようになった。そして、金融取引の増加と情報技術の発達によ

り、電子的に集中的に管理された台帳の記録という形態が生まれ、現在に至る。

現在利用される通貨形態は、預金通貨と現金（硬貨、銀行券）であり、預金通貨は電子的に管理された台帳、現金は硬貨、不換紙幣という形態をとっている。また、発行残高で見れば預金通貨が多くの割合を占めていることが分かる。

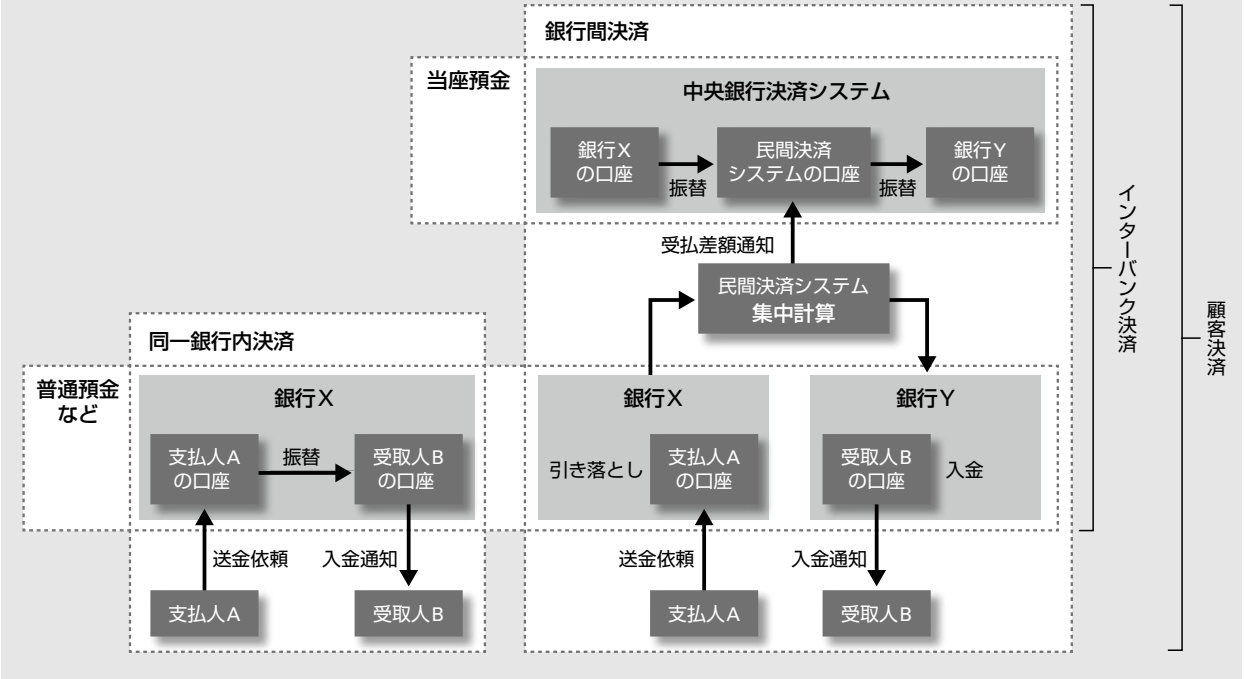
Ⅲ 通貨を支える決済システム

通貨が機能するためには、インフラとなる決済システムが必要である。ここでいう「決済システム」とは、参加者間で資金移動を行うための一連の手続きやルールのことである。

現在、主に利用される預金通貨を支える決済システムは、普通預金などの場合は銀行、銀行の当座預金の場合は中央銀行の保有する台帳上の記録として管理される。預金通貨の決済方法には、国内通貨の取引（内国為替）と、異なる通貨間の取引（外為決済）がある。また、銀行が顧客の依頼を受けて顧客のために行う決済（顧客決済）と、銀行自身のために行う決済（インターバンク決済）がある。

われわれの生活でなじみのある内国為替の顧客決済を見ると、支払人と受取人が同一の銀行内に口座を保有している場合は、支払人が銀行に送金依頼を行い、銀行が台帳上で振替を行うことで決済が行われる。一方、支払人と受取人が別々の銀行に口座を保有している場合は、支払人が自身の口座を保有する銀行に送金依頼を行った後、支払人の銀行は、受取人の銀行に送金依頼の内容を伝えた上で、民間決済システムと中央銀行決済システムを利用して、決済を行う。インターバンク決済では、民間決済システムと中央銀行決済

図1　内国為替取引の流れ



システムによって銀行間決済を行うことになる（図１）。

外為決済では、それぞれの国の決済システムを通じて決済する方法と、CLSと呼ばれる国際的な決済システムを利用する方法がある。

整理すると、現在の預金通貨の決済システム方式には、①銀行や中央銀行などの単一の信頼できる第三者機関が単一の台帳を管理している点、②複数の異なる台帳が存在する点、③台帳が階層構造となっている点、に大きな特徴があるといえる。

Ⅳ 新たな決済システムとしてのブロックチェーン・分散台帳技術

2009年に登場したビットコインは新たな決済システムの方式を提示した。ビットコインはP2P（Peer to Peer）の電子現金システムであり、単一の信頼できる第三者機関を介さず、支払人から受取人に直接的に電子現金の支払いを可能とする仕組みである。電子現金に関する研究はビットコイン以前から存在していたが、二重使用を防止するために信頼できる第三者機関が必要となることが課題であった。ビットコインは、これに対して信頼できる第三者機関を介さずに二重使用や改ざんを防止する方法を提案した。

1 仕組み

ビットコインの仕組みは既に多くの解説がなされているので、ここではポイントのみ解説することとしたい。

ビットコインの前提となるP2Pネットワークには、単一の管理主体が存在せず、不特定多数の利用者が参加するため、悪意のある利用者の参加も想定される。この環境下で参加者が自由に取引を行うためには、どのように参加者間で同一の取引順序を保ちつつ、二重使用や改ざんを防止できるかが課題となる。

ビットコインは、この課題の解決策として、①参加者が共有・保持するデータ構造として、取引をブロックという単位にまとめ、ハッシュ関数（ある入力値から一意な固定値を得る関数）を用いてブロックをチェーン上に連鎖したデータ構造を採用する（ブロックチェーン）、②取引はP2Pネットワーク上で伝播され、すべての参加者が二重使用の有無などをチェックする、③新たなブロックを追加するには、マイナーと呼ばれる参加者に膨大な計算量を要する単純な計算問題を与え、最初に解を見つけたマイナーにブロック追加の権利を与えるとともに、新たなコインを発行する（プルーフオブワーク、マイニング）、という仕組みを導入した。ここではデータ構造としてのブロックチェーンが、台帳としての機能を果たしているといえる。

なお、ビットコインは暗号通貨とも呼ばれるが、通貨の３つの性質である、①価値の尺度、②価値の交換手段、③価値の保存手段のうち、①価値の尺度、③価値の保存手段を実現していないため、現状では通貨とは言い難い。これは、コインの発行スケジュールが固定されており、コインの需要の増減に応じた発行量の調整が効かず、価格が大きく変動するためである。

2 決済システムとしての特徴

ビットコインを決済システムとして捉えると、現状での課題は多々あるものの、既存の

預金通貨の決済システムと比較して、①信頼できる第三者機関なしに複数の主体で単一の台帳を管理している点、②台帳が階層構造を持たない点、③単一の主体の判断では実質的に台帳のデータやプロセスの変更ができない点に特徴があり、これは新たな決済システム方式の可能性を開いたといえるであろう。

3　ブロックチェーン・分散台帳技術へ

こうしたビットコインの技術的な側面に対する評価が高まり、ビットコインを支える技術を汎用化・標準化していく動きが活発化しており、このような技術の総称がビットコインも含めて一般にブロックチェーン・分散台帳技術と呼ばれている。技術の取り組みの方向性は、大きくは、P2Pネットワークの中にさらに小さなネットワークを形成する方式、ネットワーク参加者を限定する方式、アプリケーション機能を拡張する方式などがある。

Ⅴ　新たな決済システムの姿

次世代決済インフラとしてブロックチェーン・分散台帳技術の活用を考えた場合、この技術の特徴を最大限に活用することで、既存の決済システムに比べ、次のようなユニークなメリットが期待できる。

1　システム全体の効率化

台帳を単一化することにより、プロセスや制度が簡素になり、システム全体が効率化される可能性がある。第一に、これまで個々の台帳管理者がそれぞれ行っていたオペレーションが集約化・自動化される。たとえば、取引のチェック、発行量のコントロール機能は、ビットコインがこれらの機能をシステムの中に組み込んでいるように、自動化されることが考えられる。第二に、規制のあり方に変化をもたらす。これまで個々の台帳の管理主体に対する規制として、倒産に備えた預金保護、報告や監査の義務付けなどが求められていたが、単一の台帳を複数の主体で管理する仕組みにおいては、こうした規制のあり方自体が変わる可能性がある。

2　決済リスクの削減

現在の決済システムにはさまざまな決済リスクがある。リスクには、決済の完了までに台帳の管理主体が倒産してしまうリスク（信用リスク）、台帳の管理主体が決済に必要な資金を準備できないリスク（流動性リスク）、台帳の管理主体のオペレーションミスのリスク（オペレーショナルリスク）、これらのリスクがシステム全体を不安定化するリスク（システミックリスク）などがある。複数の主体で単一の台帳を管理し、階層構造をフラット化する仕組みでは、このような決済リスクを削減できる可能性がある。

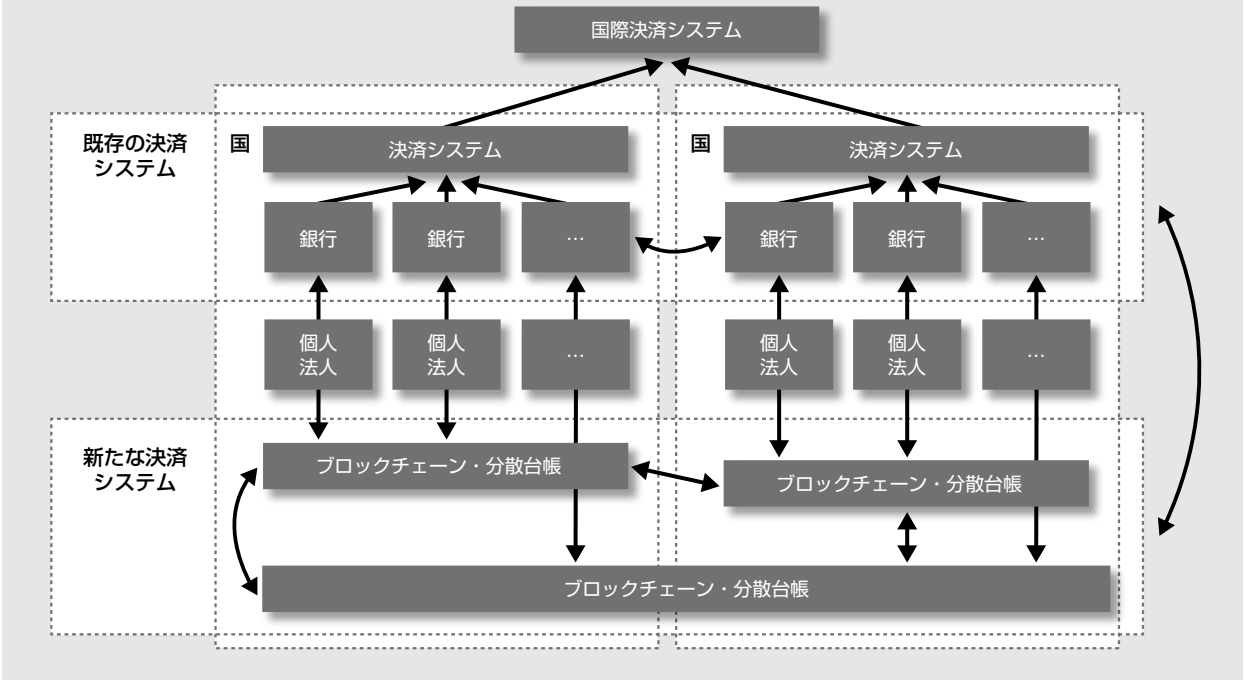
3　透明性の向上

ブロックチェーン・分散台帳上のデータやプロセスは、単一の主体の判断で変更することができないため、透明性を向上させることができる。先に述べた取引のチェックや金融政策オペレーションなどは人手に依存することなく、事前に定めたルールが確実に実行される。

4　金融サービスの多様化

ビットコインをはじめ、さまざまな暗号通

図2　併存する2種類の決済システム



貨が登場しているように、ブロックチェーン・分散台帳技術により、現在の決済システムの外側に、複数の新たな決済システムを作ることが可能となる。それぞれのシステムには、独自のルールを設定することが可能だ。また、台帳の情報へのアクセスに許可を得る必要のないタイプの技術の場合、アクセスの障壁を下げることにより、台帳の情報を活用した新たなサービスが生まれ、金融サービスが多様化することが考えられる。

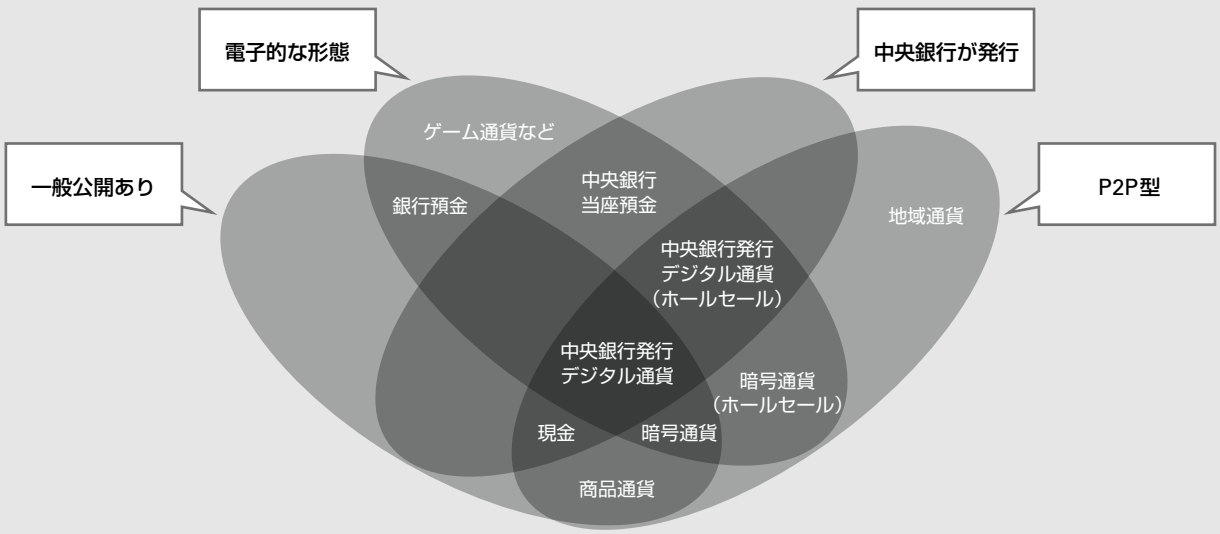
一方で、制約については考慮する必要がある。たとえば、ブロックチェーン・分散台帳技術は、既存のシステムに比べ、大量データの一括処理や実時間を起点とするイベント処理などは不得意とする。また、ブロックチェーン・分散台帳技術は、既存の決済システムの一部のオペレーションや機能を代替し得るが、すべての機能を代替するわけではない。仮に決済インフラとして利用されるとしても、本人確認、秘密鍵の管理、資産の存在証明、システム障害への対処などは、この技術の外側のオペレーションや機能として運用が必要となる。

ブロックチェーン・分散台帳技術は、既存の仕組みと競合する技術と捉えられることも多い。しかし、上記の特徴を踏まえれば、競合というよりもむしろ、双方の特徴やメリットを適材適所で使い分け、併存する姿を描いていくべきではないだろうか（図2）。

Ⅵ　新たな決済システムを活用したデジタル通貨の可能性

ブロックチェーン・分散台帳技術が新たな決済インフラとして普及するとすれば、デジ

図3　マネーの分類



出所）BISの資料を基に作成

タル通貨にどのような影響をもたらすだろうか。

国際決済銀行（BIS）によれば、通貨は、①発行者が中央銀行であるか否か、②形態が電子的か物理的か、③利用が一般公開されているか制限されているか、④交換の仕組みがP2P型か否かの4軸で分類される（図3）[注1]。

この分類に基づけば、ブロックチェーン・分散台帳技術のインフラ上で生まれるデジタル通貨は、②の電子的な形態、④のP2P型の仕組みを満たすものと考えられる。活用領域としては、①の発行者が中央銀行であるか否か、③の利用が一般公開されているか制限されているかの4パターンの可能性が考えられよう。

また、活用を考える上では、現在の決済システムにおいて課題となっている領域、あるいは新たな価値を生み出せる領域で、システムのユニークな特徴を活かしながら、既存技術に対する優位性を発揮できる活用方法を考えるべきであろう。こうした観点から次のような活用例が考えられる。

1　発行者が中央銀行で限定公開

複数の中央銀行が運用する準備通貨のインフラとしての活用可能性が考えられる。現在の国際取引の多くは、基軸通貨ドルで行われており、一国の通貨に依存するリスクがあることは長く指摘されている。国際通貨基金（IMF）が発行する、主要通貨のバスケット通貨SDR（特別引出権）などがあるが、広く普及するには至っておらず、代替手段が模索されている。国際通貨には高い透明性が求められるため、複数の中央銀行が共同で運用するブロックチェーン・分散台帳技術上で、準備通貨を発行するという可能性はあり得る。

2　発行者が中央銀行で一般公開

現金のデジタル化の検討は世界中の中央銀行が進めている。デジタル化のメリットとし

ては、現金のハンドリングコストの低下などによる利用者の利便性の向上、金融政策の有効性の向上といった効果が挙げられる。イングランド銀行は、仮にGDPの30％に相当する額のデジタル通貨を政府債務に対して発行した場合、実質金利、非中立的税率、貨幣取引コストの低下により、継続的に英国のGDPを３％引き上げ得ると分析している[注2]。課題としては、民間銀行預金からデジタル通貨へ資金シフトが起こり、民間の資金仲介が縮小する可能性があることが指摘されている。これは、多くの人が民間銀行の預金をデジタル通貨に移動するということである。また、デジタル化された決済情報の取り扱いも大きな課題の一つである。

実際の運用においては、中央銀行が単体で決済システムを運用することは、ブロックチェーン・分散台帳技術を活用する意義が薄れることから、中央銀行の役割は発行量調整ルールの決定などに限定しつつ、法的に許可された複数の組織がシステムを運用するということが考えられる。

3　発行者が中央銀行以外で限定公開

複数の金融機関の間のクロスボーダー決済としての活用も検討されている。現在の外為決済システムは、決済に時間とコストがかかることが多い。これは、銀行は海外の銀行との間で契約を結び、双方に口座を開設した上でその口座上の資金の振替によって決済を行うことが多いが、直接契約関係を持たない海外銀行と決済を行う場合は、契約関係のある銀行を中継する必要があり、そのたびにコストと時間がかかるためである。これに対して、複数の金融機関でブロックチェーン・分散台帳技術を利用した決済インフラを運用することで、中継プロセスをなくしてプロセス全体を効率化していこうという動きがある。

実際の事例としては、Utility Settlement Coinというものがある。これは複数の金融機関が共同で運用する仕組みで、中央銀行の当座預金を裏づけとして、決済用コインをブロックチェーン上に発行して、金融機関の間の決済に用いるものである。

4　発行者が中央銀行以外で一般公開

ビットコインなどの暗号通貨は、このカテゴリの一つとして考えられる。そのほかの活用例としては、今後、多くのデバイスがインターネットに接続されることを踏まえると、たとえば、自身のデバイスが何らかの計算をするときに、他人のデバイスを用いて並列処理をするようなことが考えられる。その際に、誰のどのマシンに対してどれだけの処理をしてもらったかの債権債務をリアルタイムで記録するような用途として、ブロックチェーン・分散台帳技術を用いることは可能かもしれない。

それでは、決済インフラとしてのブロックチェーン・分散台帳技術の普及の先にはどのようなシナリオが考えられるだろうか。

１つ目のシナリオは、機能の異なる多様な通貨の共存である。日本では江戸時代に金や銀の複数の通貨が同時に流通していたという歴史的事実もあることから、複数の通貨の共存が現代でも起こる可能性は十分に考えられる。

もう一つのシナリオは、金融産業のインターネット化である。インターネットプロトコ

ルの登場は、利用者の情報へのアクセスコストを下げ、クラウドやSNSなど多様なサービスを生み出した。同じように、ブロックチェーン・分散台帳技術は、これまで個々の台帳の管理者に閉じていた決済情報へのアクセス障壁を下げることで、さまざまな金融サービスを生み出す可能性がある。たとえば、ニュース記事や動画などがコンテンツ単位で課金され、即時に決済が可能になるかもしれない。これは、現在のインターネットサービスの広告に依存するビジネスモデルを大きく変える可能性がある。そのほかにも、個人が迅速かつ安全に事業に必要な資金調達を行うサービス、家電を使ってお金を稼ぐというサービスなども可能になるかもしれない。実験的ではあるものの、こうしたサービスは既に暗号通貨の世界で生まれている。

Ⅶ 課題と展望

新たなデジタル通貨の決済インフラとして、ブロックチェーン・分散台帳技術の可能性を引き出すための最大のポイントは、社会インフラとなる制度的・技術的なスタンダードを作れるかどうかという点にあろう。そのためには、次世代の決済インフラとしてのビジョンや目標を描き、技術の活用メリットと要件を明らかにし、要件に対する制度的・技術的課題の解決に取り組んでいく必要がある。また、ブロックチェーン・分散台帳技術がインターネット上で展開されていく可能性のある技術であることを考えれば、中長期的な視野で、国際的な協調の下、官民が連携し、取り組みを進めていくことが求められる。

活用メリットや要件を探る手段としては、ユースケースを明らかにすることが有効であろう。ユースケースを明らかにするとは、利用事例を羅列することではなく、システムにおいて、特定の目的やゴールを達成するために必要な利用者やプロセスを明らかにすることである。さまざまな用途に利用可能と喧伝されるブロックチェーン・分散台帳技術であるが、技術のユニークな特徴を活かしつつ、利用者にどのような価値を提供できるのかについては、現状では十分に見極められているとはいえず、引き続きこうした活動が求められるだろう。

また、さまざまなユースケースとその要件を基に、制度的・技術的な課題を解決していくことが求められる。

制度的な課題については、マネーロンダリングの防止、利用者保護、金融システムの安定性の維持、イノベーションの促進などの影響を見極めながら、こうした政策目標をバランスよく達成する制度設計を目指していく必要がある。

たとえば、暗号通貨の普及とともに明るみに出た課題としては、国際的なマネーロンダリングへの対策がある。日本では、2017年4月から開始された改正資金決済法で、暗号通貨の取引所に対する本人確認を義務付けているが、取引所を経由せずとも暗号通貨の取引は可能である。世界に先駆けて暗号通貨を法的に位置づけた点は評価されている面もあるが、他国との規制ギャップにより、国際的なマネーロンダリングの温床になるリスクも指摘されており、規制の面からも国際的な協調が求められるだろう。

利用者保護の観点からは、システムの運用

ルールや安全対策基準の整備が課題として挙げられる。世界中の暗号通貨取引所で繰り返される暗号通貨の盗難事件の多くは、秘密鍵の管理を含むマネジメントシステムの問題に起因している。また、利用者が暗号通貨の資産価値を適正に評価するための制度の整備も課題である。2017年以降、既に流通している暗号通貨と引き換えに新たな暗号通貨を発行するICO（Initial Coin Offering）と呼ばれるスキームが急速に広がっている。同時にこのスキームを利用した詐欺事件も拡大しており、各国の規制当局は取り締まりや注意喚起を進めている状況である。先にも述べた通り、これらはブロックチェーン・分散台帳技術の外側の運用プロセスとして整備されるべき点であるが、今後、制度をどのように設計・運用していくかは大きな論点になると見られる。

技術的な課題については、通貨供給量の調整メカニズム、性能、セキュリティ、プライバシー、ガバナンス、ファイナリティ、トラストなど、さまざまな課題が指摘されており、課題の解消に向けた提案や実験が世界中で進められている。しかし、要件に照らし合わせて、それが本当に解決すべき課題なのかは見極める必要がある。また、セキュリティと性能など、システム特性の多くがトレードオフの関係にあることが知られており、現状はこうしたトレードオフのバランスを模索している段階にある。信頼できる第三者機関を必要としないという特徴を保ちながら、要件を実現する最適なアーキテクチャーを設計面、実装面、運用面から模索していくことが必要であろう。

冒頭で見たように、通貨や決済システムは、歴史とともに技術革新や時代の状況を反映して進化してきた。ブロックチェーン・分散台帳技術は、この進化の過程における技術革新の一部であると考えられる。新技術は往々にしてこれまでにない新たな効果とリスクをもたらすものであるが、進化の先にある次世代の通貨や決済システムにたどり着けるかは、われわれがこの新技術をどのように導くかにかかっているのではないだろうか。

注

1 Morten Linnemann Bech and Rodney Garratt, “Central bank cryptocurrencies”, BIS Quarterly Review, September 2017

2 John Barrdear and Michael Kumhof, “The macroeconomics of central bank issued digital currencies”, Bank of England Staff Working Paper No. 605, July 2016.

著者

西片健郎（にしかたたけお）
NRIアメリカ主任研究員
専門は金融先端技術の調査研究・国際標準化