[特集]**フィンテックの進展とその将来像…❷**

ブロックチェーン・仮想通貨市場の現状と将来像

株式会社日本政策投資銀行　産業調査部　産業調査ソリューション室　調査役　石村 尚也

はじめに

2009年1月に最初に「採掘」されたビットコインは、2018年2月末現在ではおよそ1,700万BTC（ビットコインの通貨単位）が採掘されている。当初、モノとの交換価値を持っていなかったビットコインだが、2010年にピザ2枚と1万BTCが交換されたのを端緒に、徐々にビットコインとモノ、あるいはビットコインと法定通貨との取引が活発化してきた。現在では米ドルや日本円などの法定通貨でビットコインなどの仮想通貨が購入されている[1)]ほか、日本国内でも一部店舗では決済にビットコインを使う動きも出始めている。

ビットコインの価格は、振幅しつつ短期間に大きく上昇したあと、2018年初からは大きく下落した。ビットコイン以外の仮想通貨は全体で1,000種類以上に増加し[2)]、仮想通貨全体の時価総額は40兆円を超えている。価格の急上昇やボラティリティの大きさから、マネーゲーム的な側面が取り上げられることの多い仮想通貨だが、本稿ではそういった話題よりもむしろ、今後の社会・経済にどのような影響を与えうるかについて、基礎知識の整理から始め、論点を絞って考察を試みたい。

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仮想通貨を構成する技術であり、一言で言えば新しい「帳簿」の仕組みといえる。従来のシステムでは、帳簿はネットワークの中の管理者が一元管理している。参加者は送金情報などを管理者に送信し、管理者はこの情報を帳簿に反映する、という流れで帳簿の更新が行われている。

一方、ブロックチェーンでは、ネットワークの参加者各自が同一内容の帳簿を持つ。参加者はネットワーク全体の過去から現在まで同一内容の情報を保持しており、データのやりとりが行われるたびに情報がある一定のまとまり毎にネットワーク参加者全員に送信され、保存される。この一定のまとまりのことを「ブロック」と言い、個々のブロックには「前のブロックがどのようなブロックだったか」というデータも埋め込まれ、あたかも鎖のように絡み合いながら情報が保存される。このような特徴から、この帳簿のことを「ブロックチェーン」という名前で呼ぶ。

一つの送金情報を改竄しようとすると、その情報が含まれるブロックの次以降のブロックについても変更して辻褄を合わせなければならないため、膨大な計算能力を必要とする（かつ、その間にも次以降のブロックは生成され続ける）。結果的に、保存された情報の改竄が非常に困難な仕組みとなっている。

ブロックチェーンの有用性

このように、ブロックチェーンは①ダウンしないシステム、②改竄困難な帳簿（データベース）、③電子的に記録可能な帳簿を、中央管理者の信頼性によらない形で実現するこ

1）法定通貨で仮想通貨を購入、または保有する仮想通貨を売却し法定通貨を受け取ることができるインターネット上のプラットフォームを、本稿では「仮想通貨取引所」または単に「取引所」と呼称する。
2）電子的に発行された証票は「仮想通貨」ではなく「トークン（代用貨幣、引換券などの意）」と通称されることもある。

とが可能とされる。

ブロックチェーンの有用性は、仮想通貨以外の領域にも利用することができるため、各事業者とも活用可能性を検討する段階に入っている。例えば、米R3社は、ブロックチェーンの特徴を部分的に取り出した分散型台帳技術（DLT）によって、貿易金融やシンジケートローンなどの分野において実用化に向けた検討を進めており、日本を含む国内外の金融機関等と実証実験を行っている。

非常に多くのブロックチェーン活用プロジェクトがスタートアップや大企業中心に立ち上がっている。また、送金や決済など金融分野だけではなく、ITサービス分野においても活発な動きが見られる。例えば、Filecoinは分散型ファイルストレージに関するプロジェクトである。ユーザーが普段余らせているファイルを保存する容量（ストレージ）をブロックチェーン上で貸し借りし、ストレージを提供するユーザーにはインセンティブを付与する仕組みを目指している。他にも、SNSや住宅の賃貸、民泊などあらゆるサービスでブロックチェーンの導入を目指す動きがある。

スマートコントラクトとは

中でも特徴的な動きといえるのが、「スマートコントラクト」である。スマートコントラクトとは、プログラムを用いて契約を自動かつ強制的に執行する仕組みであり、広義には自動販売機のようなものも指す。概念自体は1990年代頃から提唱されていたが、ブロックチェーンによって改めて注目されるようになった。現代的なスマートコントラクトの核は「プログラムをブロックチェーンに書き込む事によって、改竄が困難で、ダウンもしないプログラムを動かすことができる」ということにある。ブロックチェーンに登録されたプログラムであるスマートコントラクトの仕組みを走らせることで、契約が自動的に執行されるようになれば、契約執行を確認するコストの削減などを含めて有用性があり、様々な利用が考えられる。

イーサリアムは、スマートコントラクトを動かすためのブロックチェーンプラットフォームであり、2013年に当時19歳のヴィタリック・ブテリンによって構想が示され、2015年に最初のベータ版がリリースされた。イーサリアムを用いることで、ブロックチェーン上で動く分散型のアプリケーションであるDApps（Decentralized Applications）を開発することができる。なお、開発者がイーサリアム上にプログラムを登録するためには、イーサ(ETH)という仮想通貨を支払う必要がある。イーサの時価総額は2018年2月現在、8兆円を超えている。イーサリアムのように、プラットフォームとして機能するブロックチェーンプロジェクトには、中国発のプロジェクト「NEO」などがある。

イーサリアム上で動いているDAppsの例は枚挙に暇がない。例えばAugur（オーガー）は予測市場の形成を目指しているイーサリアムベースのDAppsである。予測市場とは、将来のイベントを賭けの対象とすることで、将来を確率論的に予測することを目指す試みである。Augurの仕組みでは、ある参加者が「サッカーのA国対B国の結果はどうなるのか」「選挙の結果はどうなるのか」といった、予測したいテーマを掲載する。このテーマに合わせて予測参加者は自分の予測と共にAugurが発行しているトークン(REP)を賭けることができる。予測結果の審判もトークンの保有者が報告し、多数側が採用されるが、多数側の報告をしたトークン保有者には手数料が支払われ、少数側の報告をしたトークン保有者は虚偽報告をしたペナルティとしてトークンを没収されるため、正しい結果を報告するインセンティブが働く。ブックメーカーのような中央管理者なしでも、公正に賭けの精算が支払われる仕組みから、単にギャンブルだけではなく、保険やデリバティブなどの分野にも展開が期待されている。

今後多くのDAppsが世に出てくることが予想される。Apple iOSの黎明期に、多数のiOS向けアプリケーションがApp storeに登場し、しのぎを削った時期を経て、App storeはスマートフォンアプリ市場における巨大なプラットフォームとしての地位を得た。今後、イーサリアムがそのよ

うなプラットフォームとして覇権を握るのかどうかは、開発されるDAppsのユーザーから見た利便性にかかっていると言えよう。

ブロックチェーンの課題

ここまでブロックチェーンの有用性について述べてきたが、課題も存在する。例えば、スケーラビリティに関する問題がある。ビットコインは、およそ10分に1回ブロックを発行し、取引情報を保存しているが、1ブロックに埋め込まれる取引の数は4,000件ほどであり、理論上、秒間7件程度の取引しか処理することができない。これを超えた場合、通常は取引毎に取引の当事者が付与している取引手数料が高いものから処理されていくため、多くの取引がなかなか確定されない状況が生じている。同様に、イーサリアムでも、2017年末、『CryptoKitties』というデジタル上の子猫を育成し取引するゲームが流行した際、イーサリアムのネットワークが混雑し、ビットコインと同様の問題が顕在化した（「猫詰まり問題」と呼ばれた）。

ただし、こうしたスケーラビリティ問題は、当初からいくつかの解決策が提示されている。例えば、1ブロックあたりのサイズを大きくする方法や、逆に1取引の情報量を小さくすることで、1ブロックに埋め込まれる取引量を多くし、時間当たりの処理件数を改善することができる。また、複数回の取引の処理を主たるブロックチェーンの外で行い、取引が終了した時点で初めて主たるブロックチェーンに書き込むことで、ブロックチェーン上での取引件数を減らす「オフチェーン」と呼ばれる手法も提案されている。

仮想通貨取引所の不正アクセス問題

また、昨今、仮想通貨取引所への不正アクセスが話題となっている。2018年1月26日、国内の仮想通貨取引所への不正アクセスにより、580億円相当の仮想通貨が流出したとの発表がなされた。海外の他の取引所でも、不正アクセスによる仮想通貨流出が報道されている。それぞれ詳しい状況はまだ明らかになっていない部分はあるが、いずれもブロックチェーン技術自体に問題があったものではないと考えられる。ブロックチェーンは、改竄が困難な形で取引情報を記録することができる。これは例えるならば、「破ったり、燃やしたり、偽造したりするのが困難なおカネを作ることができる」ということであるが、一方、それをオンライン上の金庫に入れておいた場合、金庫の鍵が空けられておカネを盗まれてしまうことはある、ということになる。ブロックチェーンの特性としての改竄困難性と、取引所のセキュリティ問題は分けて考える必要があろう。

仮想通貨の「通貨性」

ここまでブロックチェーンについて整理を行った。仮想通貨は、ブロックチェーン技術の応用例の一つにすぎないが、話題になることが多い。「仮想通貨」という名称から誤解されやすいが、正式な法定通貨として各国当局から認められた経緯はない。とはいえ、仮想通貨、特にビットコインが通貨としての性質を備えているかどうかはしばしば議論になる。

一般に、通貨には①交換・決済手段、②価値の尺度、③価値の貯蔵手段、の三つがあるとされる[3)]。ビットコインについてそれぞれ検討してみると、まず①交換・決済手段については、国内外でビットコインを複数の事業者が決済手段として導入しており、モノとの交換がビットコイン単独でされているようにも見える。ただし、ある製品をビットコインと交換するとき、製品自体の法定通貨建ての価格は変わらず、ビットコイン建ての価格が変動する形での決済となる。この点を考えると、ビットコインがモノと交換できるのは、ビットコインが独立した通貨としての機能を持つからではなく、ビットコインが市場で法定通貨と交換できるか

3) もっとも、こうした通貨の性質は、現実的には、「備えているか、備えていないか」の2つに単純に分けられるものではない。本稿ではどの程度通貨の性質を備えているのかということについて議論を進める。また、ここで言う通貨の「価値」とは、ビットコインが何円で購入できるかという「価格」あるいは「為替レート」とは異なる概念であることは注意が必要である。

らであり、ビットコインの交換・決済手段としての機能は、実質的には既存の法定通貨に依存している。②価値の尺度としてのビットコインについても同様に、まず何らかの法定通貨建ての価格表示を経由して、それをビットコイン建ての価格で表したものであり、独立してビットコインが価値の尺度となっているものではない。

①交換・決済手段及び②価値の尺度について検討してみると、ビットコインが通貨たる性質を持っているように見えるのは、現状のところ、ビットコインが法定通貨と交換できることが前提となっているように見える。ブロックチェーン上で発行されたビットコインはデジタルな性質を持ち、腐ったり劣化したりせず、ブロックチェーン上で突如消滅することもないことから、③価値の貯蔵手段としての機能は一定程度存在すると考えられるが、現時点では価格が短期間に大きく下落する危険性もあり、先進国の法定通貨と比べるとその機能は劣っている。ビットコインが安定した価値の貯蔵手段となるには価格の安定化が必要であろう。

仮に今後、ビットコインが通貨としての価値を持ちうるとすれば、そこには「ビットコイン経済圏」ができている必要があるのではないだろうか。モノの値段が一定価格のビットコインで表示され、顧客はビットコインで支払いを行い、ビットコインで受け取った店は給与を一定量のビットコインで支払うというように、法定通貨に依拠せず経済圏が回っているならば、上述の通貨の三機能を、法定通貨に頼らず達成でき、ビットコインが通貨としての機能を持っていると言える可能性はある。ただ、そうした状況を先進国で実現することに、どのような有益性があるかは明確ではない。なお、一部の海外取引所では、他の仮想通貨・トークンを購入するには法定通貨ではなくビットコインを支払う必要がある。そうしたビットコイン以外に支払の手段がないような状況においては、上述の「ビットコイン経済圏」が部分的に成立している可能性はある。

なお、ここまで通貨の機能について、主に先進国の法定通貨と仮想通貨との優劣を念頭に置いて議論してきた。しかし、途上国の法定通貨と仮想通貨を比較した時には状況は大きく違ってくる可能性がある。例えば、ハイパーインフレが起こっている国の法定通貨よりも、ビットコインのほうが、価値の貯蔵手段として利用しやすいのではないかとの指摘もある[4)]。なお、そもそも仮想通貨の「通貨性」が話題になることは徐々に少なくなってきているとの指摘もある。その意味で、ビットコインはDAppsのコンセプトを決済アプリケーションとして実装した一例にすぎない、との整理もある。

ICO の仕組みとメリット

ICO（Initial Coin Offering）は、プロジェクトの資金調達のため、まだ発行していないトークンの予約販売（トークン・セール）を行う事で開発や宣伝に必要な資金を調達する、クラウドファンディングに似た手法である。

ICOを行う事業者は、発行条件や発行したトークンを今後どのように利用していくか等が書かれた「ホワイトペーパー」と呼ばれる書類をWEB上に載せ、購入者を募る。発行されるトークンは、サービスの支払手段として使えるよう設計される。サービス内での支払量が増えれば、トークンの需要が高まり、発行量の上限が予め決められたトークンの価格は上昇する可能性がある。購入者はトークンの将来的な値上がりを期待してICOに参加する。

なお、この際、発行されるトークンの対価として主に利用されているのはイーサリアムのブロックチェーン上で発行されているイーサ（ETH）である。これは、イーサリアムがスマートコントラクトを実装しており、「イーサリアムが払い込まれた際に、予め設定していたレートでトークンを対価として発行する」という処理を自動的に行うことができ、詐欺などのリスクを低減することができるからである。

先述のように、ICOの仕組みは、サービスがリリースしていないプロジェクトの開発資金として製品（トークン）を事前に売り出して調達する点でクラウドファンディングに似ている。一方、①ICOはイーサなどの仮想通貨が払込手段

4）ロイター「アングル：バブル警戒のビットコイン、ジンバブエでは逃避先」https://jp.reuters.com/article/bitcoin-idJPKBN1DE07M

となる点、②クラウドファンディングサイト運営者等に掲載手数料を払う必要なく資金を調達できる点、③トークンが発行後に流通、価格の上下が生じ、「相場」が生じる点はICOの特徴的な点である。

ICOのメリットは、事業者にとっては株式発行や借入に頼らず資金調達できることや、トークンの利用用途まで含めた発行条件を自由に決められること、既存株主や債権者の権利を希薄化せず調達ができること、多くの取引所に上場することができればトークン自体の流動性を高められること、などが挙げられる。

こうしたメリットを考えると、ICOは現状、単なる注目度上昇だけではなく、企業に対して実質的に有利な資金調達手法を提供しているとも考えられる。ただし会計・法制など未だ未整備な点も多く、実際に資金調達を行おうとする場合多くの論点が生じる。また、後述するように、トークンを販売した後、トークン保有者へ今後の事業の説明や情報開示をする必要も生じるし、実際のサービスでトークンがどのように発行され、利用されるのかを設計する必要もあるなど、事業者側で考えなければならないことは非常に多い。

ICO の市場規模と今後

スタートアップがICOにより資金調達を行う事例も目立つ。2017年後半から、ICOでの資金調達が件数・金額ともに大きく伸び、2017年11月末時点のICOでの調達額は世界全体で35億ﾄﾞﾙ超にのぼる。ブロックチェーン関連企業に限定すれば、ICOでの調達額がVC（ベンチャーキャピタル）の調達額を上回っていると言われている。プロジェクト当たりの調達金額でみても、2億ﾄﾞﾙ以上の資金を調達したプロジェクトもあり、巨大な規模となっている。ブロックチェーンの利用例として前述したFilecoinやAugurも、ICOにより資金の調達を行い、開発プロジェクトを進行させている。国内の事業者においても、ICOで100億円以上の資金を集めた例が数件確認されている。

ICOに関しては、今後も更なる動きが予想される。大型のICOプロジェクトには、徐々にベンチャーキャピタルを中心としたファンドが資金を投入しはじめている。この資金は、ICOプロジェクトを行うベンチャー企業の株式購入という形で投入されるものもあれば、ICOで発行されるトークンを購入する形で投入されるものもある。プロジェクトに対してファンドの審査が行われ、結果としてリスク資金が投じられたということは、一般の購入者からしてみると、トークン購入に対してある種の「呼び水効果」を発揮すると考えられる。ICOプロジェクトの中には、本格的なトークン・セールに入る前に、多額の資金を投入する購入者のための「プレ・セール」と呼ばれる資金調達を行い、トークンをディスカウントして販売するものもある。

ICO の課題

このように注目されるICOだが、様々な課題もある。例えば、ICOプロジェクトの中にはトークン・セール終了後、プロジェクトの活動状況の報告がなくなるものや、活動を停止してしまうものなども存在する。また、ホワイトペーパーを読んでも技術的な側面が曖昧なもの、実体としてプロジェクトがないが、あたかもプロジェクトが行われているかのように装うものなどもあり、詐欺として告発されたものもある。

こうした状況を踏まえ、米証券取引委員会（SEC）は2017年7月25日、ICOに関する注意喚起（Investor bulletin）を公表した[5)]。公表文の中では、ICOに関する詐欺等のリスクに関する注意喚起や、ICOが発行条件次第では証券に該当し、SECへの登録が必要であること、今後ICOに関する規制を検討していることなどが示された。

日本では、金融庁が2017年4月に施行した改正資金決済法で仮想通貨の定義付けや、利用者保護のために仮想通貨交換業の登録制の導入などを行っている。ICOについ

5）米SEC ”Investor Bulletin: Initial Coin Offerings” https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings 2017年7月25日

ては明文化されたルールは存在しないが、金融庁は2017年10月29日に、ICOに関する注意喚起を行っている[6)]。ICOと一括りに言っても、個々のプロジェクト毎に発行条件も違う。資金決済法や金融商品取引法等のルールが適用されるかは個別具体的に考えて行く必要がある[7)]。

ICOについては、購入者保護は重要な課題である一方、企業にとっては資金調達手段としての有用性も大きい。ICOの信頼性を担保できるようなルール作りを念頭に置いた議論が求められる。

ICOの今後

ICOトークンを購入するということは、ある種、サービスごとの独自の経済圏への「参加権」を購入していることと同じ意味合いを持つ。通貨に置き換えてみると、外国人が中国でビジネスをしたり、製品・サービスを購入したりするには、中国という経済圏で通用する元を買う必要があるし、欧米の経済圏に参加するためにはドルやユーロを手に入れる必要がある。それと同様、あるサービスを利用するとき、そのサービスの経済圏だけでしか利用できないポイントのようなものを購入することは今までもよく行われることであった。ただ、そのポイントがトークンや仮想通貨に置き換わり、転々流通し、価格が日々変動し、相場を形成している、という点がこれまでと最も違う点といえる。また、従来のポイントや電子マネーは利用者が望む限りは、際限なく発行される一方、多くのICOトークンは発行上限が決まっている。ある価格帯において需要が供給を上回るなら、需要と供給をバランスするために価格が変動し調整されることになろう。ICOにより発行したトークンがサービスを受ける対価として、ひいては利用され、法定通貨との「為替レート」を変動させながら転々流通していくという「トークン経済圏」が、トークンの数だけ登場することになるかもしれない。

今後ICOを行ったプロジェクトで課題となるのは、実際のサービスがリリースされた際に、どのようにトークンが使われるかということである。取引所で取引されるトークン価格が単に投機的に値上がりするのではなく、トークンの利用価値と連動する形で上昇するようにトークンの使われ方を設計することが重要となる。例えば、サービス内でトークンが使われる毎に、使われたトークン量の一定量がデジタルに「消滅」していくようなモデルの場合、経済圏全体のトークン量が徐々に少なくなっていくことになるため、トークンの利用量は増えていく一方、トークンの発行量は少なくなっていく。すると、供給に対して需要が多くなり、理論的にはトークンの価格の上昇に繋がると考えられる。このような設計手法はいくつか提案されているものの、ICO自体が始まったばかりでもあり、「正解」といえるトークン設計がどのようなものなのかについて、事業者側の試行錯誤が続くことが想定される。

今後、ICOで資金調達したプロジェクトが、どのようにサービスを運営し、トークンによる新しい経済圏を立ち上げていくのかに今後も注目したい。

なお、本稿は2018年2月時点での情報をもとにしており、今後の仮想通貨並びにICOについては規制を含めて急速に状況が変化していくことが予想される。新たな動向については適宜調査を行っていく。

■参考文献
・日本政策投資銀行（2017）「注目を集める仮想通貨市場～ビットコインからICOまで～」
・日本政策投資銀行（2017）「ブロックチェーン（分散型台帳技術）とは」
・鳩貝淳一郎「ブロックチェーン:ビットコインを動かす技術の未来」『ハーバード・ビジネス・レビュー』2017年8月号、ダイヤモンド社

6）金融庁「ICO（Initial Coin Offering）について～利用者及び事業者に対する注意喚起～」2017年10月29日　http://www.fsa.go.jp/policy/virtual_currency/06.pdf
7）行政・法制度面の対応については第3章で詳述。