2017 年 12 月
日 本 銀 行
決 済 機 構 局
金 融 研 究 所

「FinTech 勉強会」における議論の概要

日本銀行では、FinTech が金融に与える影響等について、学際的に議論することを目的に、決済機構局および金融研究所が共同で「FinTech 勉強会」を設置し、５回にわたって議論を行った。

近年、情報技術を金融サービスに利用して新しいサービスを生み出す FinTech と呼ばれる動きが注目されている。金融業が IT を活用すること自体は必ずしも新しいものではないが、最近の特徴として、ブロックチェーンや分散型台帳、それらを具現化した仮想通貨の出現、金融サービスの担い手の多様化、スマートフォンや携帯型端末の普及に伴う金融サービスへのアクセスの拡大などが挙げられる。

こうした中、FinTech が金融システムや中央銀行の政策を取り巻く環境に与える影響についての経済学的な分析、新たなサービスに対する法制度・規制の検討、そして技術そのものの頑健性の検証など、新しい技術の実用化に向けて必要な様々な論点を、アカデミックな観点から検討する社会的要請が高まっている。これまでも通貨のデジタル化、金融サービスの電子化については、法律学、経済学、情報学等あらゆる角度から議論され、研究されてきた。しかしながら、ブロックチェーンや分散型台帳技術を利用する分散管理型ネットワークの特性といった新しい要素は、従来のパラダイムを大きく転換し得る観点を孕んでおり、近年、様々な議論が行われている。

そこで、本勉強会では、法律学、経済学、情報学の３つの領域の研究者などが一堂に会し、FinTech、とりわけ分散管理型ネットワークの特性といった新しい技術要素が生み出す金融の課題に焦点をあてて議論を行った。

本稿は、総括討議（最終回（2017 年６月 12 日開催）に実施）の内容を事務局（日本銀行決済機構局、金融研究所）の責任において取りまとめたものである。なお、本報告書において意見にわたる部分は、各メンバーの会合における発言を並べたものであり、各メンバーの所属する組織や日本銀行の公式見解を示すものではない。

「FinTech 勉強会」メンバー（五十音順、敬称略）

―― 肩書は勉強会当時のもの

岡田 仁志	国立情報学研究所情報社会相関研究系准教授
片岡 義広	片岡総合法律事務所パートナー弁護士
加毛 明	東京大学大学院法政治研究科准教授
北村 行伸	一橋大学経済研究所教授
小塚 荘一郎	学習院大学法学部教授
藤木 裕	中央大学商学部教授
本多 正樹	東京国際大学経済学部教授
松浦 幹太	東京大学生産技術研究所教授
松尾 真一郎	MIT メディアラボ研究員・所長リエゾン（金融暗号）
松本 勉	横浜国立大学大学院環境情報研究院教授
柳川 範之	東京大学大学院経済学研究科教授
事務局	日本銀行　決済機構局、金融研究所

【概要】

○　本勉強会では、主として分散管理型のネットワークについて、集権的な仕組みとの比較等を通じた検討等を行った。検討にあたっては、例として、①イノベーション、②コンセンサス・アルゴリズム、③仮想通貨の法的側面の検討、④デジタル通貨の発行者による違い、⑤情報セキュリティ面での分散型・集中型ネットワークの違い、を題材に議論を行った。

○　昨今、FinTech が注目される中、数多くの先進的な決済サービスが生み出されている。このような先進的なサービスは分権的に生じるものであるが、生み出された決済サービスは、「ネットワーク外部性」という効果が働くことによって、次第に集権的なサービスへと変わっていく傾向がみられる。ただ、支払決済は、集権的な「決済」と分権的な「支払」を併せ持つ制度設計であるため、分権から集権、集権から分権という揺らぎを生み易い側面もある。いずれにせよ、分権と集権の議論を行う際には、サービスレベルや技術レベルといったレイヤー毎に分権化に進むか集権化に進むかが異なり得ることに留意する必要がある。議論を進めるにあたっては、どのレイヤーに関する議論なのかを常に意識しておくことが大切である。

○　分散型台帳技術には、検証作業というプロセスが必要となる。この検証作業には、当該作業に参加する者を限定しないパブリック型と限定するコンソーシアム型があるが、それぞれについて持続可能性の観点から留意すべき課題がある。前者については、「長期にわたり一定数以上の検証参加者をいかに継続的に確保するか」、後者については、「仮に広く利用されるようになった技術にセキュリティ面の脆弱性等が含まれる場合等にも、参加者がそれを利用し続けるために過大なメンテナンス・コストを負担することを強いられること」が問題となり得る。

○　仮想通貨（例えばビットコイン）の私法上の位置づけについて、法的に金銭と評価することは現時点では難しい。仮想通貨の保有者に仮に一定の法的保護を認める場合に、それが物権なのか、債権なのか、あるいはそれ以外の権利なのか、については議論の余地がある。仮想通貨には、一般的に主張可能な財産的価値が想定されるなど物権的要素があるものの、物権的アプローチをとることにより過不足のない保護が実現されるかについて、検討する必要がある。また、ネットワーク参加者間のコンセンサス・アルゴリズムをある種の「合意」と捉える考え方もあり得るが、そうした「合意」によりどのような権利義務が発生し得るかも論点となり得る。

○　デジタル通貨は、①民間発行のもの、②発行者が存在しないもの、③中央銀行が発行するもの、が考えられる。また、それぞれについて、①発行

者としての適切性をいかに確保するか、②実際には通貨管理者の集中化・集権化が進み得ることをいかに評価するか、③ユニバーサル・アクセスをいかに確保するか、といった課題がある。

○　「分散型システムはセキュリティ上、安全」とか「分散型システムの方が集権型のものに比べ低コスト」といった議論があるが、実際にそう評価できるかどうかは直ちには明らかではない。分散型システムでは、セキュリティ確保やそのためのコストの負担を各ノードに転嫁している面がある。したがって、システム全体としてのコスト負担を勘案する必要があるほか、セキュリティ面の評価も、集中型システムと目線を揃えた上で行う必要がある。

１．議論の対象

- 近年、スマートフォンや分散型台帳技術といったテクノロジーの進化と金融への適用が進むにつれ、FinTech を活用した新たな金融サービスが注目されている。金融業においては、これまでもその時々で応用可能な情報技術が活用されてきたが、足許、社会的に FinTech が着目される要因として、既存の中央集権的なシステムとは異なる、分散管理的なシステム構築の動きがあげられる。このため、FinTech 勉強会では、主としてこうした分散管理型のネットワークの仕組みの特徴は何か、それは集権管理型の仕組みと何が異なるのかといった点について、①イノベーション、②コンセンサス・アルゴリズム、③ビットコインを例とした仮想通貨の法的側面の検討、④デジタル通貨の発行者による違い、⑤情報セキュリティ面での分散型・集中型ネットワークの違い、を題材に議論を行った。

２．イノベーションの起こり方

- 新しいサービスは一般的に分権化された状態で開始されるが、効率性を追求する過程で集権化の方向に落ち着いていくことが多い。とりわけ、決済については、スケールメリットやネットワーク効果が非常に大きいため、集権化が進みやすい。その意味では、ある決済サービスが分権的、集権的のいずれの状態なのかは、決済サービスの特性上、自然に生じる単なる時間経過を示しているだけに過ぎないとも考えられる。他方、別の見方として、ある決済サービスが分権か集権かのいずれを指向するかは、「フィロソフィー」の違いだとする見方もある。例えば、ビットコインをデザインした人々は、中央集権的な権力に支配されない通貨を構築することを目指しており、それを支持する層によって支えられている面もある。

- また、分権と集権が共存する決済サービスもあり得る。すなわち、効率性の観点からは集権化が指向される一方、中央に管理されないことを望む人々や取引は常に一定程度存在する。このため、分権を求める人と集権的な効率性を求める人との間で、ある種の緊張関係が生じ、分権的構造と集権的構造とが共存することがあり得る。

- 「支払決済」は、「決済」の側面では、ネットワーク効果により、集権化が進むことを通じて効率化する傾向がある。一方、「支払」の側面では、端的に支払をする者と受ける者の合意により支払の効果を生ぜしめることができるという分権的な性質もある。「支払決済」は、このように、集権的な「決済」と分権的な「支払」を併せ持っているため、分権から集権、集権から分権という揺らぎを生み易いとも考えられる。

- 分権と集権の議論を行う際には、サービスレベルや技術レベルといった「レイヤー」ごとに分権化に進むか集権化に進むかが異なり得ることに留意する必要がある。デジタル通貨における「集権」あるいは「集中」と言う場合に、それが国民国家に裏打ちされた、例えば中央銀行が発行するものか、国家と関係のない私企業が発行するものかにより、性格が異なることに留意する必要がある。

- 新しい技術やサービスモデルを考えた人が、その対価を得る方法としては主に２つある。一つは「特許」のように集中的に権利を独占することで利益を得る方法、もう一つは多くの人に分散して使ってもらうことで先行者利益を得る方法である。ここで留意すべきなのは、対価を得るのに適する方法が、同じ技術に関することであってもレイヤーによって異なる点である。例えば、分散型台帳の場合、台帳を分散して保管するインフラ技術のレイヤーではなるべく多数の人が分散して使うことで利益を得る方法が適するのに対し、分散型台帳のインフラ技術を基にビジネスロジックを動かすレイヤーでは、集中的に権利を独占することで利益を得る方法が指向されやすいと考えられる。

３．分散型台帳のコンセンサス・アルゴリズムにみる「公共財とクラブ財」

- 分散型台帳には、過去の履歴を確定させる検証作業に関し、ビットコインのように不特定多数の参加が可能である「パブリック型」の仕組みと、参加者を限定する「コンソーシアム型（またはプライベート型）」の仕組みが存在する。パブリック型では、互いの参加者の信頼を前提にせず、ビットコインの Proof of Work などでみられるような多大な資源の費消に基づくコンセンサス・アルゴリズムが採用されている。他方、コンソーシアム型では、参加者間のある程度の信頼関係を前提に、検証参加者の一定割合の合意など集権的要素を持つコンセンサス・アルゴリズムが採用されている。

- パブリック型のコンセンサス・アルゴリズムは、検証作業に誰でも参加可能という点で、排他性がゼロである「公共財」、コンソーシアム型のコンセンサス・アルゴリズムは検証作業の参加者を限定している点で、ある程度排他性を持つ「クラブ財」であるとの見方もできる。ただ、実際にはパブリック型の代表であるビットコインは、マイニング報酬という私的なインセンティブにより検証作業の確実性を確保しており、実際には対価を支払わずに財を消費しようとする行為を排除できる性質を持つとは言えず、経済学上の「公共財」には該当しない。むしろ、公共財的なサービスを私的なインセンティブを用いて提供する仕組みを設計したものと考えられる。

- 通貨は、その仕組みが長期にわたりサステイナブル（持続可能）であるこ

とが重要である。例えば、ビットコインが通貨として機能するためには、長期にわたり安全性を保証し、検証作業が永続することを担保する仕組みが必要である。そのためには、マイニング報酬が低減していく中で、①マイニングのインセンティブを維持できるか、②特定の先による過度な影響力を排除するガバナンス構造を構築できるか、といった問題の解決が課題となる。

- 一般に、あるサービス基盤が、将来のセキュリティの問題等を考慮することなく開発され、その基盤が世間に幅広く普及した場合には、その基盤を利用する参加者に多大なメンテナンス・コストを課したり、セキュリティ面の脆弱性をもたらし得ることに留意する必要がある。例えば、パソコンの OS をアップデートし続けなければならないことを考えると分かりやすい。あるコンソーシアム型またはプライベート型の分散型台帳の基盤技術に関して、仮にそのデザインに問題があるとしても、先行者利益が極めて大きく、その基盤が広く使われるようになった場合には、それを利用し続けることを強いられ、参加者は、過大なメンテナンス・コストを払い続ける等の悪影響を甘受せざるを得なくなる。仕組みの違いによって将来のセキュリティ面にも差を生ぜしめることに留意が必要であろう。

４．仮想通貨の法的性質

- 仮想通貨といっても実際には様々なタイプがあり、それぞれの特徴によって、法的側面に関する議論の射程や内容も変わり得る。また、仮想通貨に関する法規整としては、私法上のルールのほか、わが国における交換所に対する規制等のような公法的規制をも念頭に置く必要がある。

- そのうち、現在広く利用されているビットコインの私法上の位置づけについてみると、現時点では一般的受容性があるとは考えにくく、法的に金銭と評価することも難しい。したがって、仮想通貨の交付については、円建ての金銭債務とは切り離した債務を想定したうえで仮想通貨の引渡しが履行される、と整理するのが自然ではないか（金銭債務の履行と整理することは難しい）。

- そのうえで、仮想通貨について一定の法的保護を認めるとして、仮想通貨を物権、債権、あるいはそれ以外の権利のいずれに位置づけるのが適当なのか。この点、（少なくとも一定の範囲での）一般的に主張可能な財産的価値が想定されている点で物権的な要素があるとの見方がある。もっとも、実際の仮想通貨の財産的価値の移転は、同一性を有する価値の移転ではなく、価値の消滅と発生により実現しており、この点はむしろ債権的な支払手段に類似するとも評価できる。いずれにせよ、仮想通貨の法的性質の検討に際しては、いかなるルールを当てはめるのが適切かを判断する必要が

ある。この点、他人の競合行為を排除する物権的なアプローチを適用することで、過不足のない保護が実現されるかについては慎重な検討を要する。また、物権的な保護を与えることにより支払システム全体のコストを高める可能性にも留意する必要がある。すなわち、取引の安全の観点から、金銭には物権的な返還請求権が認められていないことと同様に、仮想通貨においても、過去の履歴はいったん切り離される取り扱いをした方が、仮想通貨を受領する取引当事者にとっては安心であろう。

- また、仮想通貨は、特定の者に対する請求権が明確に観念されていない点で既存の債権的な支払手段とは異なる。こうした中、ネットワーク参加者間のコンセンサスに着目し、ネットワーク参加者が互いに何らかの「合意」をしていると考えることもできるかもしれない。例えば、ビットコインの取引の参加者間で、ある種のネットワークとしての「合意」を想定することは可能かもしれない。もっとも、分散型ネットワークにおける「合意」は、既に存在するプロトコルを利用するといった程度の希薄なものであり、それを法的な合意とみなしてよいのか、あるいはそうした「合意」のもとでどのような権利義務が発生するのか、といった論点がある。

５．民間発行・中銀発行デジタル通貨から見る「分権と集権」

- 情報技術の発展に伴い、デジタル通貨（ここでは、必ずしも資金決済法の定義を前提とした「仮想通貨」に限定しない）の発行が可能となり、さまざまなところでデジタル通貨の議論が進められている。特に発行者に着目すると、分権性の強いものとしては、ビットコインのような発行体が存在しないデジタル通貨、他方、集権性の強いものとしては中央銀行発行デジタル通貨、が考えられる。例えば、発行者が存在しないデジタル通貨では、発行上限額を固定する等、あらかじめ定めたルールに従って運用することで通貨としての信頼を確保しているとされる。その一方、中央銀行がデジタル通貨を発行する場合には、中央銀行という中央管理者が集権的に通貨供給量をコントロールすることが可能であると考えられる。加えて、単に分権型デジタル通貨か集権型デジタル通貨かの二元的な議論のみならず、例えばRSコイン[1]のように階層型構造をとることによる、民間発行と中銀発行の中間的な性格のデジタル通貨発行の可能性も提案されている。

- 民間が発行するデジタル通貨は、その発行者が発行者として適切かどうかが論点となる。例えば、民間企業が通貨発行により自らの資金需要を満

[1] RSCoinとは、英国ロンドン大学の研究者が考案した中央銀行による暗号通貨。論文では、中央銀行と利用者の間に介在する「ミンテッツ」が取引内容を検証し、検証結果を中央銀行に送り、中央銀行が確認を行うという２重構造が提案されている。

たそうとする場合、発行者には価格や発行時期を操作するインセンティブが生じ、これまで中央銀行が絶対に行わなかったような操作を意図的に行う懸念がある。シニョレッジのインセンティブが非常に強く、信頼性を維持することが困難であるため、供給量を恣意的にコントロールできる貨幣を民間主体が上手く供給できた例はおそらく殆ど存在しない。

- また、発行者が存在しないデジタル通貨の場合、―例えばビットコインは、これまで発行者がいないというフィクションを貫いているが―、実際には通貨管理者の集中化もしくは集権化が進み、発行者がいないという建前を維持することが難しくなることも考えられる。

- ビットコインは、技術的に発行上限に制約が課されており、恣意的なコントロールが難しい設計となっている。この発行上限の制約が、人々が価値を認める源泉の一つとなっている。その一方、需要の変動や投機的な行動に対して貨幣価値が安定せず、計算単位としては使いにくいというデメリットもある。最終的に、適切な通貨を供給できるのは、供給量を柔軟に変化させながら、全体の物価動向に対して価値を安定的に保つことができる中央銀行のような集権的な管理主体であろう。もちろん、信頼のできない中央銀行であれば民間企業が発行した通貨の方が信頼できるとの事象も生じうる。

- 実際にデジタル通貨を導入する際には、現金からデジタル通貨への移行過程において、中央銀行マネーへのユニバーサル・アクセスをどのように確保するか、という点も課題となり得る。例えば、銀行が地方における現金供給サービスから撤退する中で、全ての国民にデジタル通貨を保有するための媒体を配付するといった対応をどこまで行うべきか。こうした実務的な観点では、実際にキャッシュレス化が進んでいる北欧の例などが参考になるかもしれない。

６．セキュリティを巡る論点からみる「分権と集権」

- 分散型システムにおいて、「分散型だからセキュリティ上、安全である」といった一様の表現は適切ではない。分散型システムでは、各ノードがそれぞれにセキュリティ対策を行う責任を負っている。ビットコインのように、ほぼすべてのノードが同じソフトウェアを使用しているようなケースでは、ソフトウェアに不具合が発見された場合の影響が多大となる。

- 分散型システムの方が、集中型システムより低コストとの論調があるが、コストを比較する際には同程度のセキュリティ水準が確保されたシステム間で行う必要がある。セキュリティ水準を揃えたうえで評価した場合には、

分散型システムの方が低コストか否かは定かではない。また、コストを評価する際には、システム構築とその維持にかかるコストに加え、想定されるリスクが顕現化した場合の影響と不具合発生時のリカバリーに要するコストも勘案する必要がある。近年は、オープンソースを利用することにより、システム構築にかかるコストを抑えているものが多いが、ユーザが継続的に利用していくうえで必要なメンテナンスを確実に実現できるかは問題となり得る。すなわち、オープンソースのソフトウェアの場合には、エンジニアやアカデミアに対し、報酬の支払いなど強いインセンティブがある条件下で開発や維持管理が行われているとは必ずしも限らないため、ユーザ側のメンテナンス・ニーズに対し、十分かつ持続的に対応してくれない可能性があり得る。このため、その利用に当たってはこういった可能性に対するリスクやコストも勘案しておく必要がある。

- セキュリティの面では、ユーザ利便性が向上し、利用者が増加すればするほど、攻撃者側の攻撃インセンティブも高くなる点に留意する必要がある。また、ソフトウェアの開発・維持を行っているエンジニアと利用者との間には、セキュリティ面での認知バイアスが存在する。このため、仮に、利用者にセキュリティ確保に要するコストを負担させようとしても、うまく機能しない可能性があることも認識しておく必要がある。

- FinTech の分野では、ユーザの本人確認に関する情報や購入履歴等、多くの情報が取り扱われる。情報流出の問題はもとより、特定の主体がこうした個人情報を集約管理することについては、プライバシーの観点から議論が必要であろう。また、プライバシーの問題を議論するにあたっては、ブロックチェーンのようなインフラと、その上で機能する仮想通貨のようなものとではセキュリティ負担の構造が異なるため、各々のレイヤーに応じた検討が必要である。

以　上