2018 年 4 月
日本銀行決済機構局

第 5 回 FinTech フォーラム（2 月 7 日）議事概要

（エグゼクティブ・サマリー）

日本銀行決済機構局は、ブロックチェーン・DLT（分散型台帳技術）の将来をテーマとする「第 5 回 FinTech フォーラム」を、2 月 7 日に開催しました（プログラムは別紙 1、参加企業・団体は別紙 2 を参照）。

第 1 部では、日本銀行決済機構局の参加者から、FinTech の中でのブロックチェーン・DLT の位置付けや、これらの技術の活用動向や課題、日本銀行をはじめとする各国中央銀行の取組み等について、説明を行いました。

第 2 部では、参加者を限定しないパブリック型ブロックチェーンについて議論が行われました。このようなブロックチェーンには、「単一障害点」を持たない等の長所がある一方、取引ボリュームの増加に伴って処理が遅延する「スケーラビリティ」の問題などが指摘されています。この点、ビットコインやイーサリアムといった代表的な基盤において、ブロックチェーンの外側で処理を行うことによる処理負荷の分散や、新たなコンセンサス方式への移行などを通じて、セキュリティを確保しつつスケーラビリティを向上させる取組みが行われていることが紹介されました。

その後のパネルディスカッションでは、分散構造を特徴とするパブリック型ブロックチェーンにおけるガバナンス構築の難しさが指摘されました。また、仮想通貨を巡る問題への対応として、交換業者を介さずに仮想通貨を直接交換する技術や、秘密鍵を信託するアイディアなどが紹介されました。

第 3 部では、参加者を限定するコンソーシアム・プライベート型 DLT について議論が行われました。まず、さまざまな DLT 基盤が存在し、それぞれ分散構造や情報秘匿性の程度などに違いがある中、これらを比較評価する手法の提案が行われました。また、複数の DLT 基盤を比較した実証実験が紹介され、業務と各基盤との相性を見極めることの重要性も指摘されました。さらに参加者からは、DLT の潜在的メリットとして、情報の共有やコミュニケーションの改善、オペレーションの効率化等も指摘されました。

その後のパネルディスカッションでは、分散型の長所（単一障害点の影響を受けにくいこと等）とガバナンス構築とを両立させる取組みなどが紹介されました。また、コンソーシアム・プライベート型 DLT が持つ潜在的メリットとして、技術が業務自体の効率化などの改革を促す可能性が指摘されました。

１．日本銀行決済機構局 FinTech センター長　河合祐子による挨拶

（概要）

○　ブロックチェーン・DLT の応用分野と言えばまずは「仮想通貨」だが、その技術には改善の余地が多い。今般発生した仮想通貨交換業者における不正送金事件を取ってみても、仮想通貨を取り扱う上で組み合わせるべきセキュリティ対策などの実務、制度や、関連技術の観点から、考えるべきことは多い。（撮影：野瀬勝一、以下同じ）

○　しかし、ブロックチェーン・DLT という技術そのものへの期待は引き続き強い。すなわち、こうした技術の活用は、特に国境を越えた送金という用途においては、コストを引下げ、複数当事者間のやり取りを容易にするなどの効果も期待される。また、分散型の管理という根底にある考え方に基づき、金融取引や、情報のやりとりなどを大きく効率化できる可能性がある。日本銀行でも、欧州中央銀行との共同調査などを通じて、技術の理解深耕に取り組んでいる。

○　そうした調査を進めるうえで、実務に携わっておられる方々、研究をしておられる方々との交流は必要不可欠。その意味で、本日ご参加の皆様からは、大きな学びがあるものと大変楽しみにしている。

２．プレゼンテーションとパネルディスカッションの概要

第１部：ブロックチェーン・DLT と中央銀行

決済システムレポート・フィンテック特集号 ―金融イノベーションとフィンテック―（日本銀行決済機構局 FinTech センター企画役補佐　近藤崇史）

（説明の概要）

○　ブロックチェーン・DLT は、これまで中央集権型が主であった取引等の価値移転システムに「分散型」のアプローチを提示する高い革新性を持っている。反面、パフォーマンスやガバナンス面の課題が残存し、まさに発展途上の技術といえる。また、こうした技術としての新しさもあって、同技術を用いた仮想通貨や ICO は、投機資金の流入による市場変動の激化等のリスクを含んだものとなっており、サービスを提供する側による自主的な説明や、利用する側の理解が求められる。

○　この間、技術自体に対する中央銀行の関心は強い。リテール決済にも使用できる、所謂「中央銀行デジタル通貨」の導入については日本銀行はじめ多くの中央銀行が慎重な姿勢であるものの、大口決済システムなど、すでにデジタル化が進んでいるホールセール取引の分野については、諸外国において、技術への理解深耕を目的とした実証実験が精力的に行われている。日本銀行としても、欧州中央銀行との共同調査「プロジェクト・ステラ」が進行中であり、今後も更なる理解に向けて積極的に動いていく。

第２部：パブリック型ブロックチェーンの将来

（１）ビットコイン／ブロックチェーンの技術的動向と今後（DG Lab Chief Technology Officer (Blockchain) 渡辺太郎 氏）

（説明の概要）

○　当社では、ビットコインのブロックチェーン基盤を仮想通貨以外のアプリケーションに適用することができないかという視点から、基盤の技術開発を行っている。

○　ビットコインについては、昨年、スケーラビリティへの対応が注目を集めた。処理性能を向上させる方法について、慎重派と呼ばれる技術者を中心としたコミュニティは、セキュリティの確保と非中央集権的管理の堅持という観点から、ブロックサイズの拡大を主張する一派と意見を対立させ、その結果、ブロックチェーンの分裂につながった。慎重派は、ブロックチェーンそのものには手をいれずに、ブロックチェーンの外側で処理を行う方法（レイヤー2）について検討を行っている。

○　処理性能以外の観点からもさまざまな検討が進んでいる。異なるブロックチェーン間であっても、仲介者なしに、安全にアセットを交換できる技術である「アトミックスワップ」は有力な技術。これが実現すれば、仮想通貨の分野については、交換業者を介することなく、ユーザ同士が直接仮想通貨を交換することができるようになる。

○　国内ではプライベート型・コンソーシアム型の技術基盤の検証が盛んに行われており、その結果として当初期待された革新性を見出しにくいという声も聞かれる。こうしたなか、パブリック型の技術を改めて見直す動きも出始めており、パブリック型の技術進展に注目が集まってきているのではないだろうか。

○　パブリック型の本質的な価値は、「悪意の参加者がいたとしても、信頼を必要とする第三者なしに安全にネットワークを運営できる」という点にある。これを社会インフラとして発展させていくには、技術進歩を支える人材の育成と技術者のインセンティブ付けが必要であり、当社としても積極的にサポートしていきたいと考えている。

（２）イーサリアム・ブロックチェーンに関する技術動向（カレンシーポート株式会社代表取締役／CEO 杉井靖典 氏）

（説明の概要）

○　イーサリアム・ブロックチェーンの開発方針は、コアデベロッパー間での会議で決定されていくが、会議の模様はウェブ上で公開されており、オープンな場となっている。こうした会議に提案された技術仕様は、ERC（Ethereum Request for Comment）等として付番されており、代表的なものとしては、イーサリアム上に発行する「トークン」に関する仕様（ERC20 等）や、スマートコントラクトに関わる係争を仲裁するための仕様（ERC792）などがある。ERC20 を使用したトークン発行では、仮想通貨イーサリアムと新規トークンを 1 つのウォレットにまとめることができるという特長から、殆どの ICO は ERC20 に準拠したものとなっている。

○　イーサリアムでは、2015 年より、大幅な機能拡充（「メトロポリス」）が進められている。最終的には、コンセンサス形成の方法が PoW[1]から PoS[2]に

[1] PoW（Proof of Work）は、用意された計算問題を一番早く解くことができた者に、ブロックチェーンへの記録（ブロック内取引の正当性の検証）を許可するコンセンサス方式。膨大な計算量（仕事量）に基づきコンセンサスを形成することから、「仕事量による証明」と呼称される。

[2] PoS（Proof of Stake）は、仮想通貨の保有量・保有期間等に応じて、計算量を調整する

移行される予定だ。加えて、つい先日、匿名性の強化などが実施されたところ。これらの機能拡充はハードフォークを伴うものであるが、ハードフォークによって新たなコインを生まない工夫も施されているのが特徴。また、イーサリアムのスケーラビリティを向上させるプロジェクトとして、ブロックチェーンの外側で一定の処理を行う方法（プロジェクト Raiden）や、ブロックチェーンそのものを階層化し並列処理させる方法（プロジェクト Plasma）など、多様な検討が進められている。

○　今後は、異なるブロックチェーン間のインターオペラビリティに関するニーズが増えてくるものと想定され、当社でも、多数の国内開発業者と連携してインターオペラビリティの確保に向けた検討を行っている。

（３）パネルディスカッション

パブリック型ブロックチェーンが抱える課題への対応や、代表的なユースケースである仮想通貨についてパネルディスカッションを行った。その概要は以下のとおり。

【左より、モデレーター：日本銀行・橋本、パネリスト：DGLab・渡辺氏、カレンシーポート・杉井氏】

・ビットコイン・コミュニティ（慎重派）が考えるスケーラビリティ向上策

（DG Lab：**渡辺氏**）ブロックサイズの拡大はセキュリティ低下に繋がることが実証されているため、慎重派はそれ以外の方法でスケーラビリティを向上させることができないか検討している。ブロックチェーンの外で処理性能を上げようとするレイヤー2 のアイディアは、ブロックチェーンそ

コンセンサス方式。具体的には、より多額の、あるいはより長期に仮想通貨を保有する者は、システムの信頼性担保のために正直に行動するインセンティブを持つ、との前提に立って保有量や保有期間に応じて所要計算量を少なく調整する。これにより、PoW と比べて消費電力を低く抑えることが可能。

のものには影響を与えないことから、セキュリティが確保可能。レイヤー2は完全なトラストレスではないが、慎重派はセキュリティを最優先としつつ、最適解を探る作業を鋭意続けている。

・法整備によるコントロール効果

（**カレンシーポート：杉井氏**）ICOについては、法律の専門家と議論を行っているところ。9割方はビジネスモデルとして成立していないというのが正直な印象だが、実例を重ねることで徐々に成熟に向かっていくのではないだろうか。

（**DG Lab：渡辺氏**）仮想通貨が盗難された場合の対応として、「規制当局がハードフォークの実施を命令する」といった案も考えられようが、運営主体をもたない仮想通貨におけるハードフォークには参加者の同意が必要であり、実現は不可能に近い。パブリック型ブロックチェーンには、ガバナンスに課題があるといわれるが、そもそもガバナンスを効かせない思想の下で設計されており、どうしようもないというのが実情。マネーゲームの対象となった仮想通貨の分野には、さまざまな主体が参入してきているが、何らかの方策で私利私欲に向かわないようなコミュニティを作り上げていくことが重要だと考えている。

（**カレンシーポート：杉井氏**）パブリック型ブロックチェーンで発生するハードフォークは、大半が思想の対立によるもの。仮想通貨であれば新しいコインが組成されるだけのことであり、法的コントロールが効かない領域である。

・スマートコントラクトの開発の課題

（**DG Lab：渡辺氏**）スマートコントラクトの多くは、イーサリアム上で実装されているが、ビットコインでも活発な検討が行われている。ただし、過去の事件にみるように、スクリプトやコンパイラーの不備が脆弱性に繋がる可能性があることから、慎重に検討を進めているところ。最近では、加Blockstream社がスマートコントラクト用に開発した言語Simplicityが発表され、環境が徐々に整備されてきている。

（**カレンシーポート：杉井氏**）スマートコントラクトは、アプリケーションを自由に記述できるうえに、不特定多数が使用可能であるという特性上、セキュリティの観点から入力が制限されている。そのため、特殊なプログラミング言語を使わざるを得ない状況であり、これをどう改善していくかが課題であろう。

・仮想通貨交換業者における不正送金事件への対応を巡って

（DG Lab：**渡辺氏**）仮想通貨交換業者のセキュリティ対策については、今後、監督当局による規制等によって強化されていくものと期待される。今回の事件は、仮想通貨交換業者というトラストポイント（信頼を必要とする第三者）で発生したもの。パブリック型ブロックチェーンは、トラストポイントを存在させないという思想で設計されており、アトミックスワップのように、仮想通貨の交換をも第三者を介さずに行える仕組みすら実現されようとしている。

不正送金事件後への対応としては、過去に、コミュニティがハードフォークを発生させて不正そのものを取り消したという事例がある（The DAO 事件＜2016 年 6 月＞）。しかし、過去に遡ったハードフォークはブロックチェーンの書き換えを意味し、こうした対応は、改ざんの難しさを特長とするブロックチェーンの価値を毀損する行為であったように思う。これに対し、今回、NEM.io 財団が「ハードフォークは選択肢にない」と発言したことは評価したい。一方、ホワイトハッカーによって、不正送金された仮想通貨のアドレスが追跡されているようであるが、こうした対応は、プライバシーの観点からは必ずしも望ましいとは限らないのではないか。

（**カレンシーポート**：**杉井氏**）仮想通貨の追跡可能性については、マネーロンダリング対策とプライバシー保護の両面から検討が必要であり、今後、仮想通貨業界として考えていくべき課題であろう。今回の不正送金事件は、仮想通貨取引に使用する秘密鍵の管理が適切でなかったことが原因といわれている。秘密鍵の管理はインターネットとは切り離したハードウェア（コールドウォレット）で行うことが推奨されているが、非中央集権的思想により、米国連邦政府標準暗号でない暗号アルゴリズムを採用した仮想通貨が多く、こうしたアルゴリズムに対応した耐タンパー暗号モジュール[3]の調達が難しいといった側面もあったのではないか。安全性を高める方法としては、秘密鍵データを紙で印刷して管理する方法（ペーパーウォレット）やマルチシグネチャーの採用が挙げられるが、著しく利便性が下がることから、運用に耐えられるかは疑問が残る。

[3] 米国・カナダの耐タンパー暗号モジュールに関する認証制度は、米国国立標準技術研究所（NIST）が定めた FIPS 140-2 に準拠することを認定するものであり、FIPS 140-2 では承認暗号アルゴリズム（米国連邦政府標準暗号を含む）が定められている。このため、一般的な暗号モジュールは同承認暗号アルゴリズムの利用を前提としたものとなっている。

・仮想通貨の秘密鍵の信託スキーム

（カレンシーポート：杉井氏）当社では仮想通貨交換業者が管理する秘密鍵を信託することができないか検討しているところ。マルチシグネチャーに使用する秘密鍵の一部を信託するというアイディアであり、信託銀行はコールドウォレットの運用のみを担うことになる。仮想通貨自体を信託するものではないので、信託銀行が管理するデータ（秘密鍵の一部）が盗取されたとしても、不正取引が成立することはないという点が特長。ただし、秘密鍵の分割は攻撃への耐性を高めるが、分割数に伴い管理負担も大きくなることには注意が必要。

第３部：基盤技術の比較分析、今後の展望

（１）分散台帳技術におけるインテグリティとプライバシー保護に関する考察（日本アイ・ビー・エム株式会社東京基礎研究所 FSS&ブロックチェーン・ソリューションズ担当部長 吉濱佐知子 氏）

（説明の概要）

○　多くの DLT 基盤が提案されているなか、ニーズに合う最適なものを選択するにあたっては、DLT 基盤の比較・評価が必要となる。しかしながら、現時点では比較評価のためのベンチマークは存在せず、評価環境も整備されていないのが実情。

○　特に、安全性については、「安全」や「プライバシー」といった用語の捉え方も開発者によって区々である。そこで、当方の研究論文では、①DLT の基本機能を整理し、②DLT 参加者の種類と役割を定義したうえで、③安全性を、「正しくコンセンサス形成できること」と「セキュリティ」に分けて整理している。後者のセキュリティには、インテグリティ（一貫性）とプライバシー（匿名性／秘匿性）があり、「何のインテグリティか」、「誰に対するプライバシーか」という観点で 8 つのセキュリティ要件に分類することができる。

○　DLT を応用したさまざまなユースケースについて、8 つのセキュリティ要件がどの程度要請されるのかという分析を行ったところ、例えば、仮想通貨では、ファイナリティや、匿名性以外の秘匿性要件への要請が弱いのに対し、証券ポストトレード処理や金融契約では、法規制上強いプライバ

シー保護への要請がある。加えて、インテグリティとプライバシーにはトレードオフがあることから、そのバランスを考慮することが重要となる。

○　上記評価軸を用いて DLT 基盤の比較を行った結果、①PoW やその亜種ではファイナリティが保証できない、②パブリック型では匿名性は保証できるが、トランザクションの存在や中身は秘匿できない、③コンソーシアム型はデータの暗号化や配付範囲の制限によりプライバシー保護の工夫をしている一方、特別な役割のノードを持つことからビザンチン障害を許容できない場合が多い、といったことが分かった。今回は安全性の観点から比較評価を行ったが、他の性質についてもベンチマークの整備や評価の枠組みが必要であろう。

（２）MUFG におけるブロックチェーンの取組み（株式会社三菱 UFJ フィナンシャル・グループデジタル企画部長 相原寛史 氏）

（説明の概要）

○　当グループでは、決済を中心に、国内外のさまざまな実証実験に参加しているほか、手形・小切手電子化、サプライチェーン自動化、MUFG コインといった独自の取組みも積極的に行っているところ。

○　実際に手を動かすことで、机上整理ではみえなかったブロックチェーン基盤の特性やユースケースとの相性を理解することができてきている。例えば、小切手電子化のプロジェクト（2016 年 4 月実施）では、当初パブリック型基盤の使用を試みたが、処理速度やコストの観点から、現行サービスと同じクオリティの実現には向かないことがわかった。また、サプライチェーンの自動化に関する検討では、単一障害点の存在などのブロックチェーン基盤が持つ課題にも直面した。MUFG コインの技術基盤に関する検討では、複数の基盤（Hyperledger Fabric、Corda、イーサリアム）の性能比較も実施した。具体的には、コンセンサス・メカニズムの確認、データ保有方法、開発生産性、単一障害点やセキュリティ、プライバシーの制御方法、パフォーマンスについて比較評価を行ったが、今後は Quorum など他の基盤についても性能比較を行っていく方針。

○　ブロックチェーン・DLT はいまだ発展途上にあり、現時点において金融取引のプロダクションに利用可能なものは限定的と言わざるを得ない。いまは、基盤それぞれが目指す方向が明確になりつつあるという段階であり、ユーザとしては、トレードオフの中から業務特性に応じて適切なものを選択できる目利きが重要であると感じている。

○　当グループにおけるブロックチェーンに関する取組みは単なる勉強ではなく、実サービスの提供に向けて行っているもの。今後は、技術面からの検討はもちろんのこと、ガバナンスや運営面での検討、スマートコントラクトの法的位置づけ、プライバシー機能を付加した場合における台帳の監査方法についても、検討を行っていく予定である。

（３）証券市場からみた DLT 活用可能性の検証（株式会社日本取引所グループ　総合企画部フィンテック・ラボ室長 山藤敦史 氏）

（説明の概要）

○　当グループでは、業界内の非効率を改善することを目的に、36 の金融機関・IT ベンダーとともに、DLT の活用に向けた業界連携型の実証実験をオープンな形で実施している。

○　検討の対象としているコンソーシアム型の DLT は、金融分野での活用を企図して開発されているものであり、金融業界からの要望を取り込みながら進化している。このため、パブリック型のコンセプトから乖離してきてはいるが、DLT が有する「情報共有の効率化」と「処理の自動化」によって、金融業務の効率化を実現しようとする挑戦であると捉えている。特に、スループットの向上については、並列処理可能な部分を増やしたり、負荷の大きい処理をオフチェーンとするなど、さまざまな観点から検討を行っているところである。

○　業界連携型実証実験では、現在、ポストトレード照合と顧客確認業務を対象に検討を行っている。いずれも、プレイヤーが多く、情報（データベース）が分散・分断されているほか、オペレーションが非常に複雑であることから、長年効率化が課題となっていた領域である。検討にあたっては、個社の庭先だけをきれいにするということではなく、エコシステム全体を考えたシステム設計が必要となってくる。

○　しばしば、「本当に DLT でないといけないのか」といったことを問われることがあるが、「レガシー技術で実現できるのであれば、なぜこれまでできなかったのか」というのが私の答えである。新たな金融サービスのデザインにチャレンジできるというのは、新技術の特権である。ドラスティックな業務効率化を実現するためには、個社のコスト削減に止まらず、業界横断的な効果を目指すべきであり、DLT は世界を変え得る可能性を秘める技術であると考えている。

（４）パネルディスカッション

コンソーシアム型ブロックチェーン・DLT の技術開発動向や今後の展開について、パネルディスカッションを行った。その概要は以下のとおり。

【左より、モデレーター：日本銀行・宮、パネリスト：日本アイ・ビー・エム・吉濱氏、三菱 UFJ フィナンシャル・グループ・相原氏、日本取引所グループ・山藤氏】

・単一障害点と単一信頼点の考え方

（**日本取引所グループ：山藤氏**）DLT によるシステムにおいても、既存システムと同じような冗長構成によって単一障害点の問題に対応できると考えている。一方、ミッションクリティカルなシステムでは、なんらかの問題が発生した際にコミュニティ全体のことを考えて意思決定できる主体が必要であり、そのスピードが重要となることから、ある程度権力を集中させることが必要。そのため、事実上の単一信頼点は必要であるが、あらゆる障害・紛争のパターンをコードに落とすことができれば、将来的には中央集権的な決定の役割を減らしていくことができよう。

（**日本アイ・ビー・エム：吉濱氏**）Hyperledger Fabric をはじめとするコンソーシアム型 DLT の開発は、単一障害点を排除する方向で進化してきている。また、ガバナンスについても技術面からの工夫がなされており、例えば、DLT への参加審査を特定の主体が行うのではなく、分散型で実施すること

ができるようになってきている。ただし、山藤さんが指摘されたとおり、緊急時には、分散型の意思決定プロセスではなく、スピード重視の特権的な対応を可能にすることが必要となろう。

（三菱 UFJ フィナンシャル・グループ：相原氏）現行 DLT には単一障害点があるものも多いが、コスト面から冗長化することも難しく、今後の技術改善が期待されるところ。ガバナンス面については、参加者の管理やコンセンサスの形成について、一定の権限が与えられたノードが攻撃された場合の対応が必要かもしれない。こうしたノードを単一障害点とする見方もあり、単一障害点と単一信頼点が重なる領域についても検討が必要となろう。

・基盤の標準化とインターオペラビリティ

（三菱 UFJ フィナンシャル・グループ：相原氏）ユースケースによってブロックチェーン・DLT に求める要件は異なる。高速に単純な処理をさばきたいといったケースや、複雑な処理を効率的に処理したいといったケースなど、それぞれのニーズに合致するブロックチェーン・DLT を選択していくということではないか。将来的に、サプライチェーンのような複雑なネットワークを決済システムと繋ぐようなケースでは、それぞれの DLT を接続するための標準プロトコルが必要になってくるであろう。

（日本取引所グループ：山藤氏）各国の証券取引所がそれぞれ異なる DLT 基盤を採用することも考えられるなか、DVP 決済の要件が達成できるのかはよくわからないが、少なくとも取引タイミングの同期は課題の 1 つとなろう。

（日本アイ・ビー・エム：吉濱氏）DLT 基盤を統一すべきということではなく、さまざまなタイプの基盤がニーズに合う分野でそれぞれに使用されていくということになるのではないだろうか。こうした前提のもと、各 DLT 基盤を繋ぐための準備として、連繋のためのプロトコルや概念整理などをしていくことが必要となろう。

・イーサリアムにおけるプライバシー強化

（日本アイ・ビー・エム：吉濱氏）イーサリアムのゼロ知識証明の機能の詳細までは把握していないが、参加者全員で同じ情報を共有するパブリック型において、処理負荷の高いゼロ知識証明によって実現できることは限られると考えている。例えばトークン交換のようなことはゼロ知識証明で実現可能でも、スマートコントラクトで実現可能な複雑な処理を全てゼロ知識証明で実現するのはハードルが高いと考えている。

（**カレンシーポート**：**杉井氏**）イーサリアムは、ファイナリティのあるコンセンサス方式を目指して、Casper と呼ばれる PoS 方式に移行する準備を進めている。Casper にはいまのところ 2 種類（CBC と FFG）が存在し[4]、今後、それぞれについてテストが行われていく予定。

・実ビジネス領域での実用化に向けたハードル（技術面以外）

（**三菱 UFJ フィナンシャル・グループ**：**相原氏**）サービス提供開始後、バージョンアップなどの必要なメンテナンスが可能かという点が実務上論点となる。Hyperledger Fabric について言えば、バージョン 1.x の間はソフトフォークで対応できると想定されるが、バージョン 2.x 以降のアップデートではサービスの全面停止が必要になるかもしれない。ミッションクリティカルなサービスでの対応が可能か、データ移行が確実にできるのかといった整理は必須。

（**日本取引所グループ**：**山藤氏**）DLT の活用にあたっては、ある程度効果が得られる範囲で少しずつトラックレコードを積み上げていき、徐々に適用範囲を広げていけばよいのであって、DLT ですべてを構成しなければいけないということではない。レガシーなシステムを DLT に置き換える ―ルビコン川を渡る― かどうかの判断は、技術の問題よりは、むしろ、DLT 利用によってシステムの効率化を図ることができるのかという戦略上のコンセンサスがとれるかどうかという問題に帰着するように思う。

・コンソーシアム型 DLT が描く未来

（**日本アイ・ビー・エム**：**吉濱氏**）SNS の普及によって情報発信のあり方がデモクラタイズしてきているように、FinTech の進化は金融サービスをデモクラタイズし、金融システムのあり方を変えていくだろう。しかし、既存の金融システムがパブリック型へ一足飛びするとは考えにくく、当面は、これまでに培われてきた信頼のもとで構成された中央集権的システムのよい部分を残しつつ、既存システムの非効率を取り除く目的でコンソーシアム型 DLT が活用されていくことになるのではないだろうか。

（**三菱 UFJ フィナンシャル・グループ**：**相原氏**）トラストレスなシステムを実現可能なパブリック型に比べると、コンソーシアム型は既存の発想の域を出ないという意味で面白みに欠けると言われることもある。しかし、技術的には興味深い点も多く、可能性を秘めていると感じている。具体的には、

[4] CBC（Correct-by-Construction）は PoS タイプのコンセンサス方式であるのに対し、FFG（Friendly Finality Gadget）は PoW と PoS のハイブリッドタイプのコンセンサス方式。

DLT の活用範囲が、金融機関のシステムを接続させることに止まらず、非金融分野との台帳共有に広がっていく可能性があると考えている。ステークホルダーとの情報共有やスマートコントラクトの活用によって新しいビジネスモデルが誕生することも考えられ、これまでとはまったく違う世界がみえてくるものと期待している。

（**日本取引所グループ：山藤氏**）自主独立した企業間で効率よく情報を共有するうえで、コンソーシアム型 DLT の役割は大きい。業界におけるデータ・情報が分断されているという現状では、コミュニケーションをよくするだけでも、これまでとは異なる世界がみえてくるはずである。将来的には証券とトークンの本質的な境がなくなるかもしれないし、そうした世界が社会全体にとって望ましいのであれば、関係者が協力していく価値があるのではないか。コンソーシアム型 DLT が社会をより幸福なものとするところに寄与する技術になればと願っている。

３．ラップアップ

日本銀行決済機構局長・山岡浩巳は、フォーラムにおけるプレゼンテーションやパネルディスカッションの内容について、以下のとおりラップアップを行った。

○　本日は、ブロックチェーン・DLT の現状や課題、将来展望などについて、パブリック型・コンソーシアム型を含め、さまざまなお話を頂いた。この中で、これらの新技術を活かすには、金融のあり方自体をフレキシブルに考え直していく発想が必要と再認識した。以下、4 点にまとめさせて頂く。

○　まず、DLT 基盤自体が、更なる進化を続けているということである。ビットコインにおけるレイヤー2 のアプローチは、金融のネッティングの仕組みに似ていると感じた。例えば手形交換は、紙の手形や小切手を 1 件ずつ取り立てる代わりに、交換所で集中的に受払差額を計算し、紙の運搬などの効率化を図った仕組みといえる。その後、情報の電子化に伴い、ネッティングからリアルタイム処理（即時グロス決済）への移行が進んだが、これに伴う計算負荷を軽減するため、一部にネッティング類似の仕組みを入れたり、複数の階層構造を通じて計算負荷を分散させる工夫が行われている。もっとも、こうした決済の歴史はここまで約 300 年かかっているのに対し、

DLT の世界では類似の展開が僅か数年で起こっていることに驚きを覚える。こうした技術の進歩が金融に新たな刺激を与えていくことを期待している。

○　第二に、技術を実務に応用する過程で、さまざまな技術の特性やトレードオフも明らかになってきていることである。例えば、「仮想通貨に追跡可能性は必要か」という議論があったが、現金は絶対にハードフォークしないし、「それは昔俺が盗まれた現金だから返せ」と言われることはないが、一方で紛失すれば戻ってこない可能性が高い。このように、さまざまな決済手段には追跡可能性の強弱に伴うトレードオフがあり、どちらが良いかは状況次第であろう。また、短期金融市場は「顔見知りのマーケット」であり、仮に匿名性が確保されていても、具体的な取引内容をみれば誰が取引をしているか推測可能であることが多い。このため、取引情報の秘匿が可能な技術が求められやすい。このように、金融実務や市場の特性に応じて、パブリック型やコンソーシアム型など、求められる DLT も変わり得る。

○　第三に、世界的な監視が強まっている仮想通貨・ICO を巡るトラブルは、ブロックチェーン・DLT といった新技術とは直接の関係が薄いことも認識された。もっとも、グローバル金融危機の一因となった複雑な証券化商品については、その複雑性を背景とする「高度な金融技術」のイメージがむしろ投機を煽ったように、仮想通貨・ICO についても、「ハイテクのイメージ」が投機を煽っている面がないか、注意が必要であろう。仮に一般の方々が新技術やイノベーション自体に懐疑的な見方を持ってしまうと、金融イノベーションそのものが制約されてしまうおそれもある。仮想通貨や ICO を巡る問題と、ブロックチェーン・DLT といった背景技術は分けて考えるべきであるし、日本銀行としてもこうした点の説明に努めていく所存である。

○　第四に、ブロックチェーン・DLT を活用していく上では、法的問題など技術以外の論点も重要になるということである。例えば、「秘密鍵の信託」や「スマートコントラクト」は、法的な裏付けがあってこそ有効に機能し得る。この点、日本銀行の決済機構局や金融研究所では、互いに協力しながら、ブロックチェーン・DLT を巡る法的論点についてもさまざまな研究を進めている。先般金融研究所が公表した「証券取引における分散台帳技術の利用を巡る法律問題研究会」報告書なども、是非ご活用いただきたい。

（注）本フォーラム中の各参加者の発言は、必ずしも参加者の属する組織の見解を示すものではありません。

以　上

（別紙 1）

プログラム

1. テーマ　ブロックチェーン・DLT の将来

2. 日　時　2018 年 2 月 7 日（水）　14:00～17:20

3. 場　所　日本銀行本店会議室

4. プログラム

（1）開会挨拶

日本銀行 決済機構局 FinTech センター長　河合祐子

（2）プレゼンテーション・パネルディスカッション

◆第 1 部：ブロックチェーン・DLT と中央銀行

プレゼンター：日本銀行 決済機構局 FinTech センター 企画役補佐　近藤崇史

◆第 2 部：パブリック型ブロックチェーンの将来

プレゼンター：

DG Lab Chief Technology Officer (Blockchain)　渡辺太郎　氏

カレンシーポート株式会社 代表取締役／CEO　杉井靖典　氏

モデレーター：日本銀行 決済機構局 FinTech センター　橋本康範

◆第 3 部：基盤技術の比較分析、今後の展望

プレゼンター：

日本アイ・ビー・エム株式会社 東京基礎研究所 FSS&ブロックチェーン・ソリューションズ担当部長　吉濱佐知子　氏

株式会社三菱 UFJ フィナンシャル・グループデジタル企画部長　相原寛史　氏

株式会社日本取引所グループ 総合企画部 フィンテック・ラボ室長　山藤敦史　氏

モデレーター：日本銀行 決済機構局 FinTech センター 企画役　宮 将史

（3）ラップアップ

日本銀行 決済機構局長　山岡浩巳

以　上

（別紙 2）

参加企業・団体（アルファベット順、50 音順）

BaseLayer	ｸﾞｯﾄﾞﾊﾟｯﾁ	野村證券
BCN	ｸﾚﾃﾞｨ・ｽｲｽ証券	野村総合研究所
BlueLab	光世証券	ﾋﾞｼﾞﾈｽﾌﾞﾚｰｸｽﾙｰ大学大学院
DG Lab	国際銀行協会	日立ｵﾑﾛﾝﾀｰﾐﾅﾙｿﾘｭｰｼｮﾝｽﾞ
DG Lab Haus	国際通貨基金	日立ｺﾝｻﾙﾃｨﾝｸﾞ
DMM.com	国際通貨研究所	日立製作所
Fressets	笹川平和財団・海洋政策研究所	ﾋﾞｯﾄﾜﾝ
GMO ﾍﾟｲﾒﾝﾄｹﾞｰﾄｳｪｲ	証券保険振替機構	百五銀行
Information Services International-Dentsu	常陽銀行	ﾋﾞﾖﾝﾄﾞﾌﾞﾛｯｸﾁｪｰﾝ
KDDI	信金中央金庫	ﾌｨｽｺ仮想通貨取引所
LIFULL	真摯国際特許事務所	富士通
MicroWorld	新日鉄住金ｿﾘｭｰｼｮﾝｽﾞ	富士通ｴﾌ・ｱｲ・ﾋﾟｰ
NTTPC ｺﾐｭﾆｹｰｼｮﾝｽﾞ	ｾｰﾙｽﾌｫｰｽ・ﾄﾞｯﾄｺﾑ	ﾌﾛﾝﾃｨｱﾊﾟｰﾄﾅｰｽﾞ
NTT ﾃﾞｰﾀ	全銀電子債権ﾈｯﾄﾜｰｸ	毎日新聞出版
NTT ﾃﾞｰﾀｼﾞｪﾄﾛﾆｸｽ	全国労働金庫協会	ﾏﾈｰﾌｫﾜｰﾄﾞ
NTT ﾄﾞｺﾓ	ｾﾝﾄﾗﾙ短資	ﾏﾈｯｸｽ証券
Omise Japan	ｿﾆｰ銀行	みずほ証券
PwC あらた有限責任監査法人	第二地方銀行協会	みずほ情報総研
R3	大和証券	みずほ信託銀行
Sansan	大和総研	三井情報
SmartTrade	ﾃｯｸﾋﾞｭｰﾛ	三井住友ｱｾｯﾄﾏﾈｼﾞﾒﾝﾄ
SMBC 日興証券	ﾃｯｸﾌｨﾅﾝｼｬﾙｽﾞ	三井住友銀行
SMILABLE	電通	三井住友信託銀行
SOC 株式会社	電通国際情報ｻｰﾋﾞｽ	三井住友ﾌｨﾅﾝｼｬﾙｸﾞﾙｰﾌﾟ
ｱｲﾈｽ	東海東京証券	三橋政策事務所
あおぞら銀行	東京国税局	三菱商事
赤坂国際法律会計事務所	東京大学	三菱電機
ｱｻﾋｾｷｭﾘﾃｨ	東京短資	三菱 UFJ 国際投信
ｱﾄﾞｰﾋﾞｼﾞﾈｽｺﾝｻﾙﾀﾝﾄ	東京都	三菱 UFJ ﾄﾗｽﾄ投資工学研究所
ｲｵﾝﾌｨﾅﾝｼｬﾙｻｰﾋﾞｽ	ﾄﾞｺﾓ CS	三菱 UFJ ﾌｨﾅﾝｼｬﾙ・ｸﾞﾙｰﾌﾟ
池田泉州銀行	ﾄﾗﾝｽﾌｧｰﾜｲｽﾞ・ｼﾞｬﾊﾟﾝ	ﾓﾙｶﾞﾝｽﾀﾝﾚｰ MUFG 証券
ｲﾉﾍﾞｰｼｮﾝ・ｴﾝｼﾞﾝ	内閣官房	ﾔﾌｰ
ｴｲﾌｧｽ	ﾆｯｾｲ基礎研究所	山梨中央銀行
ｵｳｹｲｳｪｲｳﾞ	日本ｱｲ・ﾋﾞｰｴﾑ	預金保険機構
ｵﾘｴﾝﾄ総合研究所	日本格付研究所	楽天
ｶﾚﾝｼｰﾎﾟｰﾄ	日本ｸﾗｳﾄﾞｷｬﾋﾟﾀﾙ	ﾙｰﾄｴﾌ
監査法人ﾄｰﾏﾂ	日本証券金融	ﾛｰｿﾝﾊﾞﾝｸ設立準備会社
かんぽ生命保険	日本ﾃﾞｼﾞﾀﾙﾏﾈｰ協会	ﾜｲｼﾞｪｲ FX
ｷｬｯﾌﾟｼﾞｪﾐﾆ	日本取引所ｸﾞﾙｰﾌﾟ	
金融情報ｼｽﾃﾑｾﾝﾀｰ	日本ﾌﾞﾛｯｸﾁｪｰﾝ協会	

以　上