JPX
JAPAN EXCHANGE GROUP

日本取引所グループ
JAPAN EXCHANGE GROUP

JPX WORKING PAPER

JPXワーキング・ペーパー

金融市場における分散型台帳技術の活用に係る検討の動向

近藤 真史†, 保坂 豪†, 土井 惟成† 山藤 敦史†

2017 年 9 月 14 日

Vol.20

† 株式会社日本取引所グループ 総合企画部 新規事業推進室 フィンテック・ラボ (jpx-fintech@jpx.co.jp)

JPX ワーキング・ペーパーは、株式会社日本取引所グループ及びその子会社・関連会社（以下「日本取引所グループ等」という。）の役職員及び外部研究者による調査・研究の成果を取りまとめたものであり、学会、研究機関、市場関係者他、関連する方々から幅広くコメントを頂戴することを意図しております。なお、掲載されているペーパーの内容や意見は執筆者個人に属し、日本取引所グループ等及び筆者らが所属する組織の公式見解を示すものではありません。

謝辞

本稿の執筆にあたり、実証実験のパートナーである日本アイ・ビー・エム株式会社及び実証実験にご参加いただいている国内金融機関等のご担当者様をはじめとする社外の有識者の方々には、貴重なご意見・ご指摘をいただきました。ここに深く感謝申し上げます。なお、あり得べき誤りは全て筆者の責任です。

目次

I. はじめに

ビットコインに代表される仮想通貨を支える技術基盤である「ブロックチェーン/分散型台帳技術（Distributed Ledger Technology。以下「DLT」という。）」が金融市場関係者の間で脚光を浴びて以降、これを金融市場インフラに活用しようとする取組みはここ 2～3 年において世界中で急速に拡大し、今日に至るまで衰えることなく継続している。当初は、金融機関や取引所・清算決済機関が DLT について個別に調査・実験を進めていたものの、直近においては多数の金融機関等による共同での実証実験の実施や、限られた関係者間において DLT を本番業務へと試験的に適用する試みも見られ始めている。

我が国においては、DLT を使った新たな金融サービスを複数の銀行が連携して検討できる環境について本年秋頃の整備を目途に検討することを全国銀行協会が発表[1]しているほか、銀行を中心に 61 の金融機関（2017 年 7 月時点）が参加する内外為替一元化コンソーシアム[2]では、DLT などを活用したリアルタイムでの送金インフラ構築に向けて具体的な検討が進められている。海外に目を向けると、DTCC（The Depository Trust & Clearing Corporation）がクレジット・デフォルト・スワップ等の OTC デリバティブに係るポストトレード処理サービスである TIW（Trade Information Warehouse）に対し DLT を段階的に適用していくことを発表[3]しているほか、ASX（Australian Securities Exchange）ではかねて検討してきた次世代の証券振替システムに対する DLT の適用の有無について 2017 年中に最終決定することとしている[4]。

DLT の技術開発についても直近ではいくつかの新しい展開が見られる。まず、昨年 11 月には Corda がオープンソース化されたほか、本年 7 月には Hyperledger Fabric のバージョン 1.0 正式版（以下「Fabric v1」という。）がリリースされた。また、本年 3 月には Enterprise Ethereum Alliance[5]が発足されて金融機関等も多数参加している状況にあるほか、JP モルガンは Ethereum をベースとした DLT 規格である Quorum を独自に開発して昨年 10 月に公開している。

日本取引所グループ（以下「JPX」という。）では、2015 年より社内で研究チームを立ち上げて DLT の金融市場インフラへの適用可能性について調査・分析を行っており、昨年 8 月にはそれまでの実証実験等から得られた知見について研究チームによるワーキング・ペーパー（以下「前回 WP」という。）として公表[6]している。本稿では、前回 WP 公表以降における DLT 規格の技術開発の動向及び金融市場における DLT の活用に向けた検討の具体的な課題について解説・考察した後、それらを踏まえて今後進展すると思われる金融市場インフラの変化の方向性等について述べる。

なお、DLT は様々な業界において技術開発及び活用に向けた検討が進められているが、本稿は主に金融業界、その中でもとりわけ株式、債券及びデリバティブ等の金融商品取引に関連したユ

---

1 https://www.zenginkyo.or.jp/news/detail/nid/8042/

2 SBI ホールディングス株式会社及びその子会社である SBI Ripple Asia 株式会社により 2016 年 8 月に発足。（http://www.sbigroup.co.jp/news/2016/0819_10389.html）

3 http://www.dtcc.com/news/2017/january/09/dtcc-selects-ibm-axoni-and-r3-to-develop-dtccs-distributed-ledger-solution

4 http://www.asx.com.au/services/chess-replacement.htm

5 パブリック型でのネットワーク運用を想定した仕様の DLT 規格である Ethereum について、処理性能や秘匿性等の面でユーザー企業の要件をより満たすよう独自の改修を目指すコンソーシアム。

6 http://www.jpx.co.jp/corporate/research-study/working-paper/tvdivq0000008q5y-att/JPX_working_paper_No15.pdf

ースケースに焦点を当てて執筆している。また、対象範囲をそれらに絞ってもなお、DLT の活用に係る検討状況や関連するトピックは多岐にわたっているため、本稿に記載の内容については、現状における筆者の理解不足等に起因して正確性や網羅性に不備がある可能性がある旨、予めご理解をいただきたい。新たな技術を活用してビジネスを大きく効率化・変革するためには、業界全体における理解の共有と幅広い議論が不可欠である。本稿が金融市場インフラにおける DLT の活用に向けた国内外における検討及び今後の技術開発の一助となれば幸いである。

II. DLT 規格の技術開発

本章では、金融業界において活用が検討されている代表的なオープンソースの DLT 規格である Hyperledger Fabric、Corda 及び Quorum（以下「金融市場向け DLT 規格」という。）[7]について、各規格の概要及び共通した特徴等を記載する。Hyperledger Fabric は実証実験から得られた知見に基づいているが、Corda 及び Quorum については公開されている情報での机上検証に基づいている。

1. 各規格の背景及び基本的な処理の流れ

(1) Hyperledger Fabric

Hyperledger Fabric は DLT 規格及びその周辺ツールについてオープンソースでの開発を進める世界最大規模のコンソーシアム Hyperledger（Hyperledger Project とも呼ばれている）の代表的[8]な DLT 規格である。バージョン 0.6 がこれまでに多くの金融機関等における実証実験で用いられているが、本年 7 月にリリースされた Fabric v1 では従前のバージョンから仕様が大きく異なっている。Fabric v1 の基本的な構成要素及び機能は以下のとおりである。

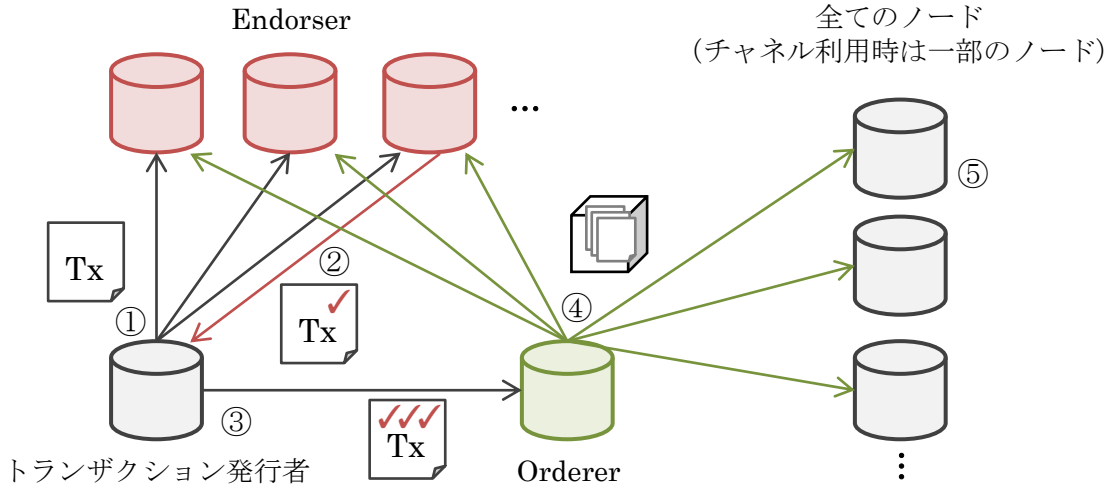
- エンドーサー（Endorser）
  トランザクションを実行し、署名を付して実行結果と共にトランザクションの発行者に返す役割のノード
- オーダラー（Orderer）
  トランザクションを 1 つないし複数まとめて順序を決め、ブロックとしてネットワーク全体にブロードキャストする役割のノード
- エンドースメントポリシー（Endorsement Policy）
  どのノードがエンドーサーとなるか、トランザクションが承認されるために何台のエンドーサーからの署名が必要か、などについての設定
- チャネル（Channel）
  ネットワーク上で台帳を共有するノードの範囲についての設定[9]

PBFT（Practical Byzantine Fault Tolerance）をベースとしたコンセンサスアルゴリズムを採用していた従前のバージョンとは異なり、コンセンサス処理[10]についてエンドースメントポリシーにより柔軟な設計が可能であるほか、チャネルにより台帳の共有範囲を限定してデータの秘匿性を確保する機能が実装されている。Fabric v1 におけるトランザクションの実行フローの概要は図 1 のとおりである。

---

[7] ただし、Hyperledger Fabric については金融市場での利用にのみ特化して開発されているわけではない。
[8] 元となるソースコードについて複数のプロジェクト参画企業から提供された結果、現状では複数の DLT 規格の開発が並行して進められている。
[9] スマートコントラクト（Hyperledger Fabric においてはチェーンコードと呼ばれる）はチャネル毎に実行インスタンスが生成され、エンドースメントポリシーは実行インスタンス毎に定義する。
[10] 台帳に記録するトランザクションの内容、実行可否（ユーザー権限の観点など）、実行順序及び実行結果等について、ネットワークに参加するノード間で合意を形成すること。

図 1 Fabric v1 におけるトランザクションの実行フロー



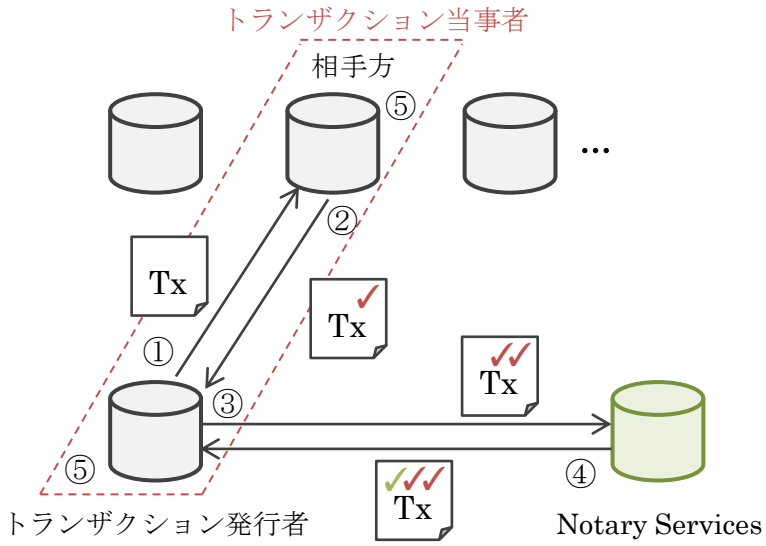
① トランザクション発行者はトランザクションをエンドーサーに送信する
② エンドーサーは当該トランザクションを実行し、署名を付して実行結果と共に返信する
③ トランザクション発行者はエンドースメントポリシーで定める必要な数のエンドーサーからの署名を集めた後、オーダラーにトランザクションと集めた署名を送信する
④ オーダラーはトランザクションをまとめてブロックとしてブロードキャストする
⑤ 各ノードは各トランザクションについてエンドースメントポリシーを満たしていること等を確認した後に台帳に反映させる

(2) Corda

Corda は 80 社超（2017 年 6 月時点）の金融機関等で構成される R3 コンソーシアム[11]にて開発されている DLT 規格である。データモデルとしてビットコインと同様の UTXO[12]を採用しているほか、トランザクションの実行時に二重支払い（Double Spend）をチェックするためにノータリーサービス（Notary Services）という仕組みを実装している。ノータリーサービスは既に消費済みのトランザクションの履歴を管理しており、新たにトランザクションを発行する際には、インプットとして指定した過去のトランザクションがまだ消費されていないことの証明をノータリーサービスに対し要求する。このノータリーサービスは特定のノードが担うシングル構成のほか、複数のノードでコンセンサスアルゴリズムにより合意を取る方式も可能となっている。また、トランザクションはブロードキャストされず、当事者が管理するノードでのみ実行される。Corda におけるトランザクションの実行フローの概要は図 2 のとおりである。

[11] R3 CEV 社により 2015 年 9 月に発足。
[12] Unspent Transaction Output の略。トランザクションのデータレイアウトとしてインプットとアウトプットを持ち、過去のトランザクションのアウトプットを新たに実行するトランザクションのインプットとして“消費”する。

図 2 Corda におけるトランザクションの実行フロー

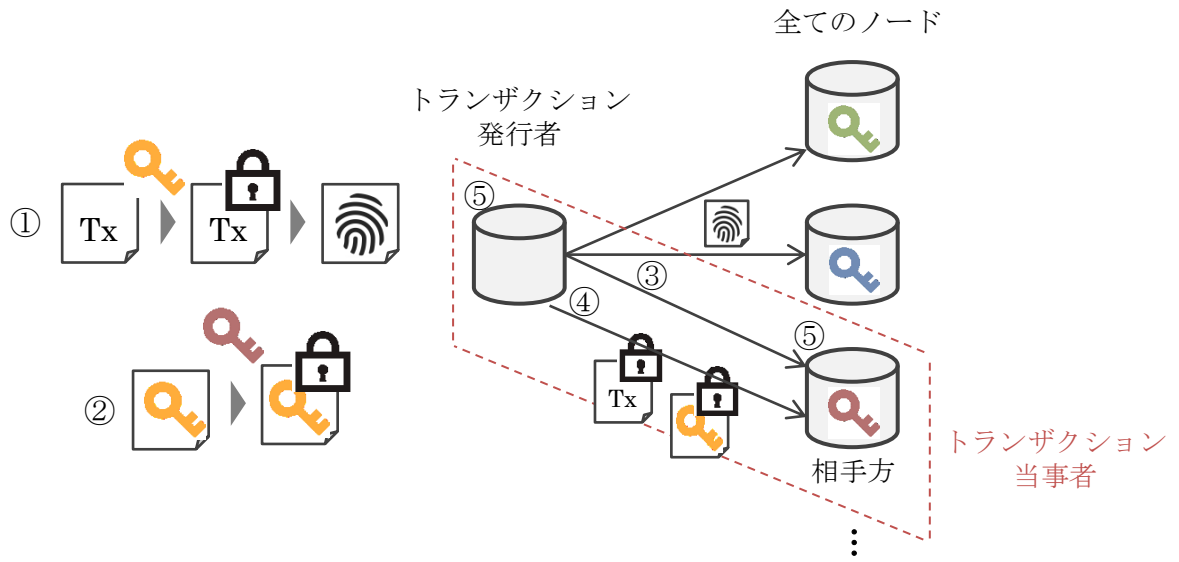


① トランザクション発行者はトランザクションの相手方が管理するノードにのみトランザクションを送信する
② トランザクションの相手方は内容を確認した上で署名を付して返信する
③ トランザクション発行者はトランザクションに自身の署名も付した後、インプットに指定した過去のトランザクションが未消費であることの証明をノータリーサービスに要求する
④ ノータリーサービスは未消費であることの証明として署名を付して返信する
⑤ ノータリーサービスの証明が得られたことを当事者間で共有した後、トランザクションを実行して結果を台帳に格納する

(3) Quorum

Quorum は Ethereum をベースとしつつ金融業界における利用を想定してデータの秘匿性を強化した DLT 規格である。Quorum のトランザクションにはパブリックとプライベートの 2 種類が存在する。パブリックトランザクションの実行フローは Ethereum と同様であるが、プライベートトランザクションについては、当該トランザクションの当事者が管理するノードでのみ実行され、ネットワーク全体ではトランザクションのハッシュ値のみ共通の台帳に書き込まれる。Quorum におけるプライベートトランザクションの実行フローの概要は図 3 のとおりである。

図 3 Quorum におけるプライベートトランザクションの実行フロー

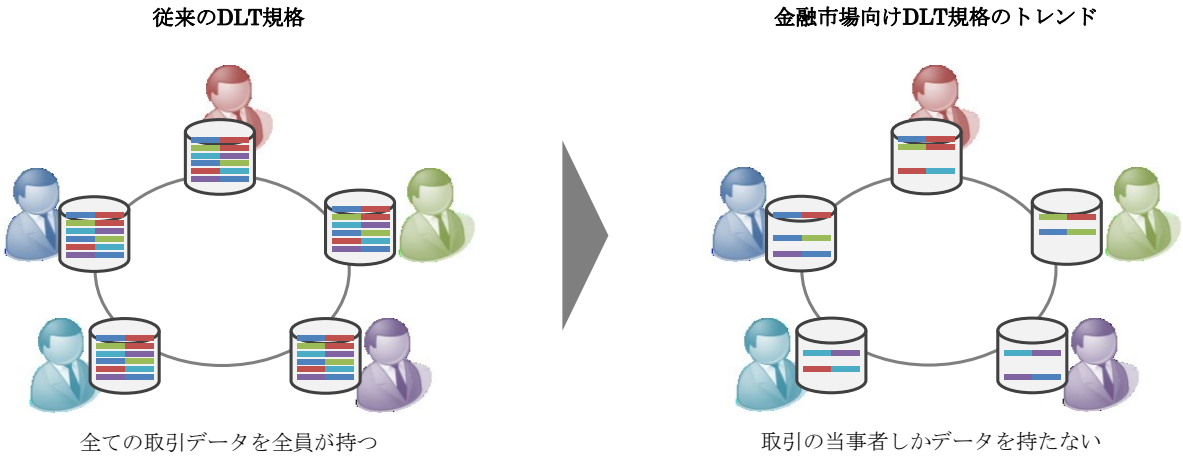


① トランザクション発行者は共通鍵を生成してトランザクションを暗号化すると共に、暗号化されたトランザクションのハッシュ値を作成する
② ①で用いた共通鍵を、トランザクションの相手方が管理するノードの公開鍵で暗号化する
③ ①で作成したハッシュ値を全ノードにブロードキャストする
④ トランザクションの相手方にのみ、暗号化されたトランザクションと共通鍵を送信する
⑤ トランザクションの内容について当事者間で合意した後、実行して結果を台帳に格納する

2. 金融業界における DLT の特徴

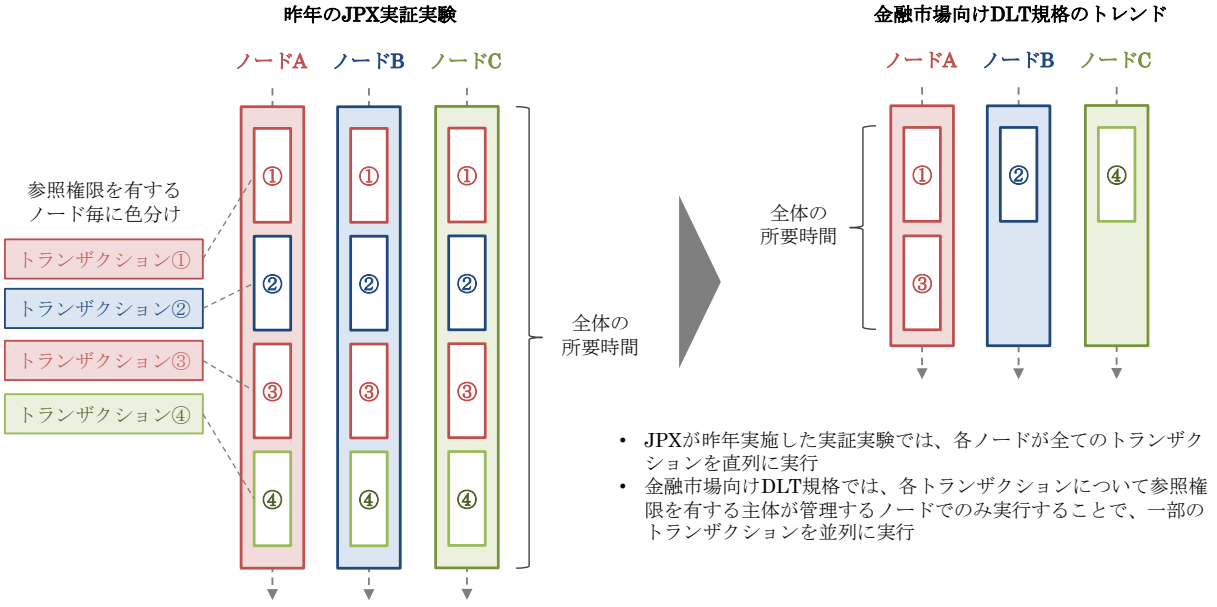
前節で述べた金融市場向け DLT 規格の特徴等を踏まえると、金融業界では参加者間におけるデータの秘匿性の確保が重視されていることが分かる。従来は全てのデータが格納された共通の台帳を各ノードが保有することが前提であり、一部の DLT 規格では当該前提の下で公開鍵暗号基盤により各参加者に異なるデータ参照権限を与えるアクセス制御を実装していた。ただし、トランザクションは実行時には台帳上のデータと共に一時的に復号される必要があるため、ノードを保有する金融機関等において内部者が不正にアクセスすれば復号された情報を盗み見ることは不可能とは言い切れないほか、利用されている暗号技術の安全性が将来に渡り保証できるとは必ずしも限らない。これらの懸念を踏まえて、暗号化したまま一定の演算が可能な準同型暗号の DLT への活用も検討されているが、高度な演算が可能であるほど処理性能が著しく低下するため、仮想通貨と異なり商品性やワークフローが複雑な金融市場での実用化は現時点では困難であると考えられる。こうした背景から、最新の金融市場向け DLT 規格では、トランザクションは当事者が管理するノードでのみ実行され、データも当該ノードにのみ格納する方式が主流となっている（図 4 参照）。

図 4 物理的な隔離によるデータ秘匿性の確保のイメージ



また、トランザクションが特定のノードでのみ実行されることは、従来と比べて処理性能の面でも有利となる。前回 WP にて記載したとおり、JPX が昨年実施した実証実験においては、各ノードが全てのトランザクションを直列で実行していることがネットワーク全体のスループット性能上のボトルネックとなっていた。ただし、最新の金融市場向け DLT 規格においては、異なるノードで実行されるトランザクションは並列で処理されるため、当該ボトルネックについての改善が期待される（図 5 参照）。

図 5 トランザクションの並列実行のイメージ



一方で、トランザクションの内容が必ずしも全てのノードに共有されないことから、従来の DLT において重要な概念であったコンセンサス処理についても変化が見られる。Fabric v1 のエンドースメントポリシーや Corda のノータリーサービスのように、コンセンサス処理のルールについてはユーザー側で柔軟に設定できる傾向にあり、特定のエンティティに承認権限を集中させてコンセンサス処理を不要とすることも可能となっている。ネットワーク参加者が互いに信頼された既

存の金融機関等のみで構成される場合、一定以上の割合のノードが故障ないし故意により同時に不正な挙動を示すことは想定し難いことから、コンセンサス処理を割愛ないし簡素化させるという選択肢も採用され得る。前節で述べた金融市場向け DLT 規格における機能や役割の細分化は、ビザンチン障害耐性よりも秘匿性や処理性能[13]を追求した結果であるため、少なくとも従来の DLT と同等の厳格なコンセンサス処理を実施することはあまり想定していないものと考えられる。

3. 既存技術との比較

前節までに述べてきたとおり、最新の金融市場向け DLT 規格は金融機関等の実務的な要望を取り込みながら、当初のコンセプトに固執せずに技術開発が進んだ結果、結果的に既存の分散データベース[14]と大差ないのではないかという指摘がある。分散データベースは、主に処理性能の向上（負荷分散）及びスケーラビリティの観点から、特定の主体が一元的に管理する複数のデータベースに対してデータを分散して配置するものであり、一般的にビザンチン障害耐性は持たない。確かに、金融市場向け DLT 規格では必ずしも各ノードが全てのデータを互いに持ち合わなくなり、コンセンサス処理についても柔軟な運用が可能となった結果、設計次第では分散データベースとの類似点は多くなるほか、処理性能や技術的な成熟度の観点では分散データベースのほうが現時点では優れていると言える。ただし、分散データベースでは予め指定する何らかのキー項目についての値やレンジ毎にデータを分散し、分散された個々のデータベース間で格納するデータは重複しないのに対し、金融市場向け DLT 規格では秘匿性の確保と共に関係者間での情報共有に主眼が置かれているため、データを共有するノードについてトランザクション毎に柔軟に指定できる。また、データの可用性の観点から比較すると、金融市場向け DLT 規格では特定のノードでデータが喪失してもネットワーク全体としてデータを復旧できる可能性がある[15]のに対し、分散データベースでは分散された個々のデータベースにおいて冗長構成を組む必要がある（図 6 参照）。

両者の違いはデータベースとしての技術的な観点からは細かい設計レベルに過ぎないかもしれないが、金融市場向け DLT 規格は、分散データベースの技術を応用しつつ、複数エンティティ間でのワークフローの効率化等に向けて、より広範なサービス[16]が各規格の特徴に合わせてパッケージングされたものと言える（表 1 参照）。今後、さらなる技術開発により、様々な業界で活用できるミドルウェア[17]として発展することが期待される。

---

[13] 日本銀行の実験によると、コンセンサス処理に参加するノードを増やすほどスループット性能の低下が見られる。（https://www.boj.or.jp/announcements/release_2017/data/rel170227a5.pdf）

[14] 様々な種類が存在するが、本稿では主に Mongo DB の特徴を踏まえて記載している。

[15] 理論的には可能であると考えられるものの、次章で述べているとおり、実務的には課題が想定される。

[16] データベース基盤に加えて、スマートコントラクトとしてのプログラムの実行環境、ノード間でのメッセージング機能、開発ツールキットなど。

[17] ハードウェアや OS といった基盤部分と各業務処理を記述したアプリケーションの間で、一定の性質のユースケースに共通的な処理を担う汎用ソフトウェア。

図 6 データの冗長化に関する運用の違い

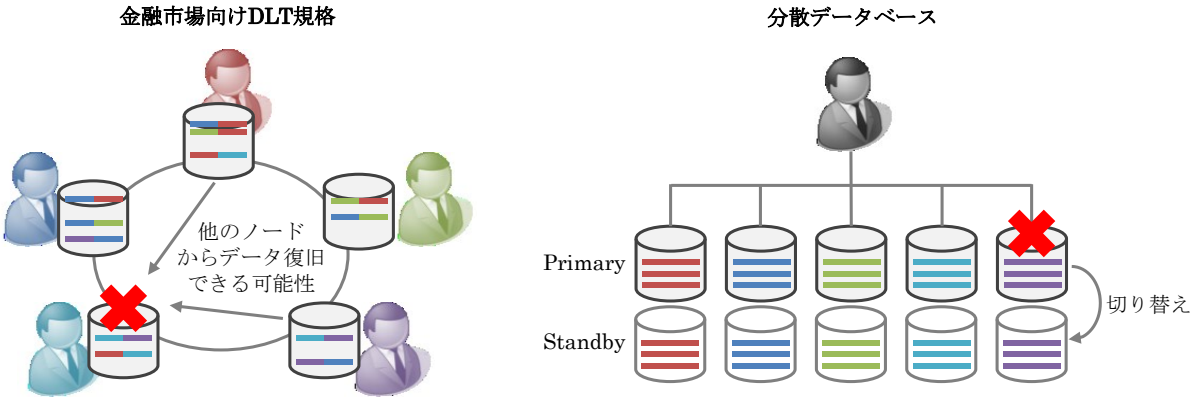


表 1 金融市場向け DLT と分散データベースの比較

	金融市場向けDLT	分散データベース
主な目的	秘匿性を確保しつつデータを関係者間で効率的に共有	処理性能の向上とスケーラビリティ
管理主体	複数の機関による共同運営も想定	特定の主体が一元的に管理
データ分散の単位	トランザクション毎にデータを共有するノードを柔軟に指定	予め指定する何らかのキー項目についての値やレンジ毎に分散
ビザンチン障害耐性	ユースケースに合わせて選択可能	なし ※特定の主体が一元的に管理する想定であるため
データの可用性	特定のノードでデータが喪失しても他のノードから復旧できる可能性	分散された個々のデータベースにおいて冗長化が必要

III. 金融市場への活用に向けた検討

DLTにより金融業界における幅広い業務において効率化や抜本的な変革がもたらされる可能性については、金融業界においてDLTに係る調査・研究が活発化した当初から繰り返し指摘されてきたが、近年における金融市場を取り巻く規制環境の変化という観点からも、新しい技術を活用してITシステムの開発・運用について見直しを模索する機運が高まっている。一方で、世界中で実証実験が活発に実施され、技術開発が急速に進んでいるものの、DLTの実用化に向けては引き続き検討・解決すべき課題も存在する。

1. 複雑化する規制環境とDLTに対する期待

金融業界におけるITシステムには高い信頼性が求められることから、可能な限り自社でアプリケーションを開発すると共にハードウェアも含めて自ら運用することが、これまで長年にわたり一般的であった。しかしながら、各金融機関等においてこうしたオンプレミス型[18]のITシステムを開発・運用していくことは、近年における様々な経済・金融環境の変化、とりわけ金融規制の変化による負担が大きくなってきている。

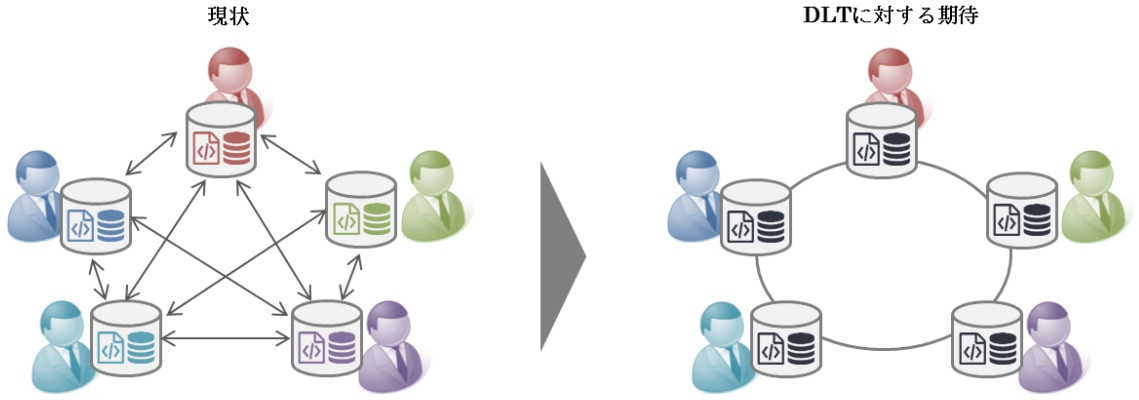
その代表例として、2008年のリーマンショックを端緒とした金融危機を踏まえて議論されてきた様々な金融規制改革について、近年その適用が次々と開始されていることが挙げられる。例えば、バーゼル銀行監督委員会（BCBS）が主導する一連の規制改革であるバーゼルⅢは2013年から2019年にかけて段階的な適用が進められているほか、BCBSと証券監督者国際機構（IOSCO）が共同で進める店頭デリバティブ市場改革においても、システミックリスクの把握・低減に向けた様々な規制が順次導入されている。これらの規制改革は国際的な協調の下で進められているが、BCBS等は規制の対象となる金融機関等に対して何ら強制力を持たないため、BCBS等が公表したガイドラインを元に最終的には各国の規制当局において法制化される。従って、各国における規制は原則として共通する内容であるものの、細部において実務慣行を踏まえた差異は生じうる。国際的にビジネスを展開する金融機関等においては、同時期に複数国において提示される新たな規制を適切に理解した上で、それらを満たすようワークフローの見直しやITシステムの改修を進める必要があるため、急速に変化する規制に対して如何に的確かつ効率的に対処していくかが課題となっている。

金融市場におけるワークフローにDLTを適用できれば、その基本的な機能やデータフォーマットはスマートコントラクトとして定義・実装されるため、関係する金融機関等の間では必然的にアプリケーションの仕様の標準化が図られることとなる。規制を含め経済・金融環境が急激に変化している中で、それに対応するワークフローの見直しやITシステムの改修を各企業が独自に進めることは大きな負担であり、少なくとも非競争的な分野においては各社の知見等を共有すると共にアプリケーションの一部を共同で利用する等によりコストを抑えることは有効な解決策となる。また、アプリケーションの仕様の標準化は自ずとデータフォーマット変換等の作業を削減して業務の効率化に資すると共に、関係者間でのデータ連携がDLTネットワーク上でシームレスに実施されることでワークフロー全体の高速化も期待される。一連の規制改革ではシステミックリスクの把握・低減という観点から、取引内容の報告や証拠金の授受等について取引の発生を起点

[18] サービス提供者がITシステムのハードウェアを自社で保有し、自社保有物件や自社契約データセンター等の設備内に設置・運用する形態。

とした厳しい時限が設けられており、これらの要素の実現は今後の金融市場において不可欠となってくるものと考えられる（図 7 参照）。

図 7 金融業界における IT システムの課題と DLT に対する期待



2. 実用化に向けた課題

前章で述べたとおり、金融市場向け DLT 規格においてはデータの秘匿性や処理性能を重視した技術開発が進んでいるが、これまでの調査・分析及び実証実験から得られた知見等を踏まえると、これらの観点については前進が見られる一方で新たな課題も生じている。また、具体的なユースケースについて関係者間での共同実証実験及び試験適用が進む中で、既存のインフラと組み合わせた DLT の実装方式やアプリケーションの開発・運用に係るガバナンス等、実用化に向けた実務的な論点についても検討が必要となっている。

(1) 秘匿性

従来の DLT では各ノードが全てのデータを互いに持ち合うことで高い可用性や改ざん耐性（完全性）を実現していたが、各ノードが保有するデータが互いに異なる場合には、これまでとは異なる方法でそれらを担保する必要がある[19]。

Fabric v1 でチャネルを活用して秘匿性を高める設計について検討したところ、チャネル毎の台帳を相互に連携する機能は現時点では提供されていないため、チャネルを跨いだ資産の移転等が発生する場合にはデータを連携する役割を担う特別なノードが必要となる点が課題となった。当該ノードは可用性等の面で単一障害点となるほか、連携する双方のチャネルの台帳を参照する権限が必要であるため、管理者には中立性と信頼性が求められる。また、各ユースケースにおける個別のアプリケーションとして実装するとバグを内在させてしまうリスクが高まるため、今後、

[19] 秘匿性（Confidentiality, 機密性と訳すほうが一般的）、完全性（Integrity）及び可用性（Availability）の頭文字をとり、情報セキュリティを構成する三大要素として“情報セキュリティの CIA”と表現される。従来の DLT は、秘匿性に対する要件を大胆に放棄する代わりに完全性と可用性を大幅に高めていると言える。

DLT 規格の基本機能として実装が進むことが望ましい。

Quorum では、非決定性を排除したプログラム実行環境[20]をスマートコントラクトに用いているため、同じトランザクションを同じ順番で実行すれば結果は必ず一致することから、プライベートトランザクションについてハッシュ値及び実行順序を全てのノードで合意し共有しておくことで、データの改ざん検知や障害時復旧のための“信頼できる唯一の情報源（Single Source of Truth）”としている。このような仕組みでは、当事者間でデータの不整合が生じた際や一部のノードでデータロストが発生した場合、各ノードが保有するトランザクションを持ち寄ることで正しいデータの検証やデータの復元が理論的には可能であると考えられる[21]。ただし、当該オペレーションの実施には多大な労力が必要と想定されることからあくまで最後の手段であり、実務的には全てのデータ及びトランザクションを参照できる特権的なノードを設置しておくことが適当ではないかと思われる。また、カナダ中央銀行（Bank of Canada）が実施した実証実験に基づくレポートによると、Corda を利用した場合には、可用性の実現のために各ノードにおいて冗長構成を組む必要がある旨が指摘されている[22]。

以上より、これらの DLT 規格では秘匿性を高める機能が実装されているものの、当該機能を実際に活用するためには、従来の IT システムと同様に冗長構成により可用性を確保するか、または何らかの特殊な役割を担う存在が必要となるものと考えられる。取引所、清算機関及び振替機関等の金融市場インフラ運営者や金融機関といった既存プレイヤーの存在を前提とすれば、当該役割について信頼性のある中立的第三者が担うことも可能であるが、DLT の利点を損なうことがないよう慎重な検討が必要である。

(2) 処理性能

処理性能について Fabric v1 を用いて検証したところ、基本的には従前のバージョンと比較して高いスループット性能が期待できるものの、特定の条件下では処理性能が低下することが確認された。これは、Fabric v1 ではトランザクションの実行と台帳への反映がプロセスとして非同期で処理されていることが原因となっている。エンドーサーはトランザクションを実行し、署名を付して実行結果と共に返信するが、その際に当該トランザクションが読み出したデータベース上のキー項目及びその読み出し時点における状態についても添付する。その後、オーダラーがトランザクションの順序を決めてブロードキャストし、各ノードにおいて 1 件ずつ台帳に反映する際に、当該時点と比較して読み出したキー項目の状態が古いトランザクションは却下される（図 8 参照）。

[20] Quorum は Ethereum をベースとしており、スマートコントラクトは EVM（Ethereum Virtual Machine）で実行される。
[21] 実際のデータを用いた検証はしておらず、公表資料等から得られる情報に基づいて記載。
[22] http://www.bankofcanada.ca/wp-content/uploads/2017/05/fsr-june-2017-chapman.pdf

図 8 トランザクションの台帳への反映時におけるキー項目の衝突チェックの例

【ユースケース：銀行口座（入金・出金・振込み）】
データベース判例：(キー項目(key), 状態(ver), 値(val))
データベース初期状態：(投資家 A, 1, 10000)、(投資家 B, 1, 10000)、(投資家 C, 1, 10000)
※状態は当該キー項目の値の更新の都度カウントアップされる

トランザクション 1~3 が同時に発生したとき、エンドーサーからの返信内容は以下のとおり。
トランザクション 1：投資家 A に 5000 円を入金
読み出し｛(key：“投資家 A”, ver：“1”)｝、実行結果｛(key：“投資家 A”, val：“15000”)｝
トランザクション 2：投資家 B に 2000 円を出金
読み出し｛(key：“投資家 B”, ver：“1”)｝、実行結果｛(key：“投資家 B”, val：“8000”)｝
トランザクション 3：投資家 A から投資家 C に 3000 円を振込み
読み出し｛(key：“投資家 A”, ver：“1”)（key：“投資家 C”, ver：“1”)｝、
実行結果｛(key：“投資家 A”, val：“7000”)（key：“投資家 C”, val：“13000”)｝

各ノードがオーダラー経由で各トランザクションを上記順序で受け取った際の挙動は以下のとおり。
①トランザクション 1 を台帳に反映
データベース更新｛(投資家 A, 2, 15000)｝
②トランザクション 2 を台帳に反映
データベース更新｛(投資家 B, 2, 8000)｝
③トランザクション 1 を①で反映した結果、キー項目“投資家 A”の状態が“2”となっているため、
古い状態を読み出しているトランザクション 3 は却下

大量トラフィック中の各トランザクションが読み出しているキー項目が分散しており衝突が発生しない場合には、従前のバージョンを上回るスループット性能が得られた。一方で、同一のキー項目を読み出して更新するトランザクションばかりを投入した場合には、キー項目の衝突が大量に発生してしまい、本来のスループット性能が発揮されない一方でシステム負荷だけが高まる結果となった。また、現状の仕様ではトランザクションを台帳に反映させるプロセスは各ノードにおいて直列で実行されているため、チャネルを活用しておらずネットワーク全体で 1 つの台帳を共有している場合には、全てのトランザクションが直列で処理されてしまう点にも注意が必要である。キー項目の衝突チェック以外の部分は並列処理が可能と考えられるため、今後のバージョンアップにおいては台帳への反映プロセスの部分的な並列化の実現が望まれる。

(3) 実装方式

仮想通貨を支えるパブリック型のネットワークは、マイニングによる当該仮想通貨の獲得を経済的なインセンティブとして組み込む事で、参加者自身による非中央集権的なインフラの維持・運営を実現している。しかし、本稿で主に取り扱っているコンソーシアム型のユースケースでは、こうした経済的インセンティブを付与することが難しいため、ワークフローの効率化等の共通の

目的の下で、主要な利用者がインフラの維持・運営に係るコストを負担し合う必要がある。これらの背景を踏まえて、ノード保有に対するコストとシステム運用に係る負担の軽減及びネットワーク構成の効率化のため、DLT の実装においてクラウドサービスを活用する検討が進んでいる。

クラウドサービスには、クラウド環境上で CPU、メモリ及びストレージ等の基本的なシステムリソースを提供する IaaS（Infrastructure as a Service）[23]と、クラウド環境上（またはサービス提供者が管理するデータセンター）で構築された具体的な業務アプリケーションを提供する SaaS（Software as a Service）の 2 種類が存在するが、近年、金融業界ではいずれについても注目が高まっている[24]。IaaS を利用してノードをクラウド環境上に構築できれば、利用者は比較的安価かつ容易に DLT アプリケーションの利用を開始できる。また、各利用者が自社のデータセンターでノードを構築した場合と比較して、ノードが地理的に過度に分散せずネットワーク構成の観点からも効率的である。ただし、天災や人的エラー等によるデータセンター等の広域障害は大手クラウドサービスベンダーにおいても発生しているため、各々が独自にクラウド環境上でノードを構築した結果、特定のクラウドサービスベンダーの同一の地域（Region）やデータセンターに多数のノードが集中しないよう注意が必要である。以上より、DLT とクラウドサービスは親和性が高いと考えられるため、上手く組み合わせれば DLT の実用化に向けたハードルが下げられると考える。ただし、具体的なシステム構成については、コストやネットワークの観点からの効率性だけではなく、可用性等も踏まえた幅広い観点からの検討が求められる。

一方で、クラウドサービスの利用が金融業界で今後広く普及すれば、DLT の活用は業務効率化の観点からは必ずしも重要ではないとの指摘もある。確かに、クラウド環境上にアプリケーションやデータを置くことについて全ての利用者が了解できる場合には、当該ユースケースについては SaaS として提供されたほうが業界全体のコストは低廉になるものと考えられる[25]。ただし、当該サービスは金融市場における新たな単一障害点となるほか、その提供者の業界内における影響力が中長期的に極めて大きくなる可能性について懸念する声もある。

(4) ガバナンス

DLT は複数の関係者間で基本的なアプリケーションをスマートコントラクトとして共同利用する技術であることから、実用化に向けてはその開発の推進体制やガバナンスも重要な論点である。

DLT の効果的な活用においては業務プロセスの見直しも併せて必要と想定されるため、アプリケーションの仕様等について各利用者が積極的に提案し、コンソーシアムとして一体感を持って開発を推進することが実用化に向けた鍵となると考えられる。また、幅広い関係者が共通の理解の下で議論に参加できるよう、利用を想定する DLT 規格や開発言語についてはオープンソースである等、仕様が公開されていることが望ましい。

一方で、高い信頼性が求められる既存の金融サービスに対する DLT の適用においては、アプリケーションをオープンソースで開発する場合であっても、特定の主体が品質について責任を持つ

[23] 基本的なシステムリソースに加えて DBMS や計算・分析ツールなどアプリケーション構築に際し有用な様々なツールが提供される場合には PaaS（Platform as a Service）と呼ばれる場合もあるが本稿では IaaS に含める。
[24] 金融業界ではクラウドサービスについて情報セキュリティに対する懸念が長年存在していたが、大手クラウドサービスベンダーは当該分野のスペシャリストを多数抱えて日々研究及び実用化に努めているため、今日では情報セキュリティ強化の観点からもむしろ積極的に活用していくべきとの指摘が多数なされている。
[25] 金融業界におけるワークフローの一部が SaaS で提供されて関係する金融機関の間で普及すれば、クラウド環境上で仕様の共通化やシームレスなデータ連携等が実現し、DLT と同様の効果が期待できるほか、システムリソースの配分やデータの冗長化についてサービス提供者が効率的に一元管理できる。

必要があるものと考える。また、近年におけるビットコインの仕様変更に係る対立等を踏まえると、競合関係でもある利用者のみでは意見の相違の調整が難しいため、当該コンソーシアムには中立的第三者が何らかの形で関与することが望ましい。さらに、実際の運用を考えると、最新の金融市場向け DLT 規格の特徴を活かすためには、DLT ネットワーク上でも中立的第三者が一定の機能を担う必要が生じる可能性もある。これらの役割の担い手については、既存の業界団体や金融市場インフラ運営者が候補として想定されるが、コンソーシアムを形成する金融機関同士が新たなエンティティを設立することも考えられる。

業界横断的な利便性の向上のために中立的なエンティティを設立することは金融市場がこれまで通ってきた道筋であり、DLT の活用において中立的第三者の存在を前提とすることは“車輪の再発明”ではないかという指摘もある。しかしながら、DLT を活用すればインフラの運営について中立的第三者が担う範囲を従来から大きく削減しつつ、より低コストかつ効率性の高いワークフローを構築できる可能性がある。既存プレイヤーの間で長年に渡り築き上げてきた信頼があり、それを活用したガバナンス体制を構築できる場合には、DLT の実用化に向けた強みとなる。既存の金融市場における DLT の活用においては中立的第三者を完全に排除するのではなく、効率的なインフラの構築に向けてその役割を変化させていくことが求められると考える。一方で、パブリック型のネットワークで運用されている仮想通貨や、昨今注目されている ICO（Initial Coin Offering）のような新しい金融サービスについては、従来の金融市場とは全く異なる非中央集権的なガバナンス構造の下で、今後、大きく発展していく可能性もある。

IV. まとめ

本稿では、JPX の研究チームとして昨年 8 月に前回 WP を公表した以降の DLT に係るさらなる調査・分析と金融市場を取り巻く状況等を踏まえ、DLT 規格の技術開発の最新動向及び金融市場における DLT の活用に向けた検討の具体的な課題について解説・考察した。最後に、それらを踏まえて、今後想定される金融市場インフラの進化の方向性及び JPX における直近の取組みについて述べる。

1. 金融市場インフラの進化の方向性

本稿で述べた金融市場を取り巻く近年の状況を踏まえると、今後は業務の効率性向上に向けて主に非競争分野における協調の機運が高まり、その実現手段として新しい技術の活用が進んでいくものと考えられる。今日における技術的な成熟度を踏まえると、まずはクラウドサービスの普及拡大によるシステム運用の負担軽減やワークフローの効率化等が、DLT よりも先行して進展することが想定される。例えば SWIFT では本年 2 月より開始した GPI（Global Payment Innovation）[26]というプロジェクトにおいて、クラウド環境上で各銀行が情報連携することで国際送金の送金状況をリアルタイムで把握可能とするサービスを提供しているほか、金融商品取引のポストトレード分野においても様々な機能について SaaS で提供する新たなサービスが近年増加している。一方で、基幹業務も含めて金融市場の広範囲にわたる機能がクラウド環境上で運用可能か否かについては引き続き慎重な見極めが必要であるほか、クラウドサービスのメリットは事業規模が大きく IT の専門人員を豊富に擁する金融機関であるほど相対的に低下するため、当面はオンプレミス型の IT システムとクラウドサービスの活用が混在するものと考えられる。

アプリケーションの開発において DLT を基盤技術として適用できれば、各利用者における IT システムの実装方式を問わずに、データの効率的な連携及び整合性の確保が実現することが期待される。実際に、CLS 銀行が DLT を用いて新たに開発を進めている CLS Net[27]では、自社でノードを保有して DLT でデータ連携する方法と CLS 銀行が管理するサーバに SWIFT ネットワーク経由でアクセスする方法との 2 通りの接続手段が提供される予定となっている。また、今後のさらなる技術開発により、パブリック型も含めたネットワーク間の連携についても検討が進めば、将来的には仮想通貨等の発展に伴い既存の金融サービスにおいて抜本的な変革が実現する可能性もある。

本稿で述べたとおり、金融市場向け DLT は金融機関等の要望を取り込みながら当初のコンセプトからは大きく異なる方向性へと変貌してきており、もはや従来から存在する技術と大差ないのではないかという指摘も見られる。しかしながら、新しい技術について利用者サイドが主体的に研究し、実務的なニーズを踏まえて開発者サイドに対してフィードバックすることは有意義なプロセスであり、結果的に既存の技術と大差ないとしても、実用化へと結び付けて金融サービスを着実に進化させることが重要である。金融市場における DLT の適用に係る検討は、仮想通貨に由来する革新的なイメージに基づいたユースケースから、まずは既存の金融機関やインフラ運営者

[26] 国際送金における透明性やトレーサビリティの向上を目的としたプロジェクトであり、将来的な DLT の活用についても検討されている。
（https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi）

[27] 140 種類以上の通貨に係る多様な外為取引について照合及びネッティングを提供するサービス。
（https://www.cls-group.com/ProdServ/Pages/CLSNet.aspx）

が有する信頼性を活かしつつワークフローを改善するという、現実的な活用方法へとシフトしている。それに伴い、当初の熱狂的な関心は薄れてきており、今後はその反動により各金融機関等における取組みが後退することも危惧される。ただし、新しい技術の発展過程においてそういった期待感の浮き沈みは発生し得るものであり、フィンテックという潮流の下で金融サービスの効率化・高度化が強く期待されている中、中長期的な視点から検討を継続していくことが必要である。

また、本稿では主としてプライベート/コンソーシアム型のユースケースについて言及しているが、仮想通貨に代表されるパブリック型のサービスが、多くの課題を指摘されながらも、世界中から注目を集め、拡大し続けている事実についても忘れてはならない。スマートコントラクトによる柔軟なサービス設計と仮想通貨による決済システムの組み合わせは、金融市場の役割や金融サービスの新たな可能性を提示している。金融市場インフラの健全な運営という使命を追求しながらも、真に利用者に資するサービスが提供できているのかを常に問い続ける姿勢が、今後はより一層重要となってくると考える。

2. JPX における最近の取組み

JPX では、金融市場における DLT の活用に向けて継続的な技術検証と業界横断的な議論が必要であるとの認識の下、金融機関等からの参加を広く受け付けて実証実験等を共同で実施する業界連携型の新たな取組み[28]（以下「業界連携型 DLT 実証実験」という。）を 2017 年 3 月より開始している。当該取組みには 2017 年 8 月末時点で 33 社の金融機関等が参加しており、専用のコミュニケーションサイトを用いて各金融機関等の担当者間における情報共有や意見交換等を行っているほか、証券市場の基本的な機能を DLT 上で実装したアプリケーションを DLT に関する理解の共有のために参加者向けに公開[29]している。また、DLT の具体的なユースケースについて参加している金融機関等や外部の IT ベンダーから提案し、他の金融機関等に対してニーズ調査や意見交換等を実施することも可能となっている。直近においてはユースケースの提案が徐々に活発化しており、既に 2 件のアイデアについては、業界連携型 DLT 実証実験の枠組みの中で、金融機関同士による共同検証プロジェクトへと発展している[30]。

近年、情報技術の発展により様々なサービスの利便性が急激に高まっている一方で、既存の金融市場インフラは長年にわたる改修や機能追加により仕様が複雑化・サイロ化しており、外部環境の変化への迅速な対応が困難となってきている。IT システムについて各社が独自に開発するか IT ベンダーが各社に提供するというプロセスからは、業界横断的な業務効率化や新たなインフラの構築は生まれにくい。ただし、新しい技術の活用に向けて既存プレイヤー同士が相互に協力して知見を共有できれば、従来は実現が難しいと考えられていたような革新的なアイデアについても具体的な検討が進むことが期待される。DLT が金融業界で脚光を浴びて以降、そのような取組みが盛んに行われていることは大きな変化の兆しではないかと考える。今後、これが DLT の活用

[28] JPX の子会社である東京証券取引所、大阪取引所及び日本証券クリアリング機構が共同で推進。
[29] JPX が昨年実施した実証実験で開発したアプリケーションをベースとして東京証券取引所が開発しており、概要については動画で公表している。（https://youtu.be/1ckIjKwTotY）
[30] 株式会社大和証券グループ本社が主導する日本株取引のポストトレード業務に関するプロジェクト並びに SBI ホールディングス株式会社、株式会社 SBI BITS 及び日本電気株式会社の 3 社が共同で主導による顧客確認業務に関するプロジェクト。JPX はこれらのプロジェクトに対して、業界連携型 DLT 実証実験の枠組みの提供者として、アプリケーションの実行環境やコミュニケーションサイトの提供等により支援する。

に限らず様々な技術・分野へと拡大していくことで、金融サービスの持続的な発展に向けたオープンイノベーションの風土として定着することを期待したい。