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

金融市場インフラに対する分散型台帳技術の適用可能性について

山藤 敦史†, 箕輪 郁雄‡, 保坂 豪†, 早川 聡§, 近藤 真史†, 一木 信吾†, 金子 裕紀¶

2016 年 8 月 30 日

Vol.15

† 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)
‡ 株式会社東京証券取引所 IT 開発部
§ 株式会社大阪取引所 IT 開発部
¶ 株式会社日本取引所グループ 決済連携推進部

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、株式会社野村総合研究所及びカレンシーポート株式会社、実証実験にご参加いただいた国内金融機関等 6 社*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。

* 株式会社 SBI 証券、株式会社証券保管振替機構、野村證券株式会社、マネックス証券株式会社、みずほ証券株式会社、株式会社三菱東京 UFJ 銀行（五十音順）

目次

I. はじめに

近年、「ビットコイン（Bitcoin）」に代表される仮想通貨が、世界中で話題となっている。また、当初は仮想通貨の通貨としての側面に対して多くの関心が寄せられていたものの、ここ 1~2 年においては、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。）」について、仮想通貨以外の領域に応用しようとする動きが様々な産業分野において活発になり、脚光を浴びている。DLT を用いて実現可能な合意形成の対象は通貨の移転に限らず、技術的には現在稼働している全ての中央集権型合意形成システムを DLT で書き換えることが可能であるため、その革新性や応用範囲の広さから、DLT は IT の進化における「第 5 世代へのパラダイム・シフト」をもたらす技術基盤と評されている。

その応用先の 1 つとして有望視されているのが金融市場インフラである。DLT が有する技術基盤としての特性は、清算・決済業務といったポストトレード分野を中心に、金融市場インフラの幅広い領域との親和性が高いと考えられており、金融市場インフラに更なる効率性をもたらすだけに留まらず、既存の金融市場インフラそのものを置き換えるような抜本的な変革をもたらす可能性さえも指摘されている。そのため、世界各国の取引所、清算決済機関、投資銀行及び情報ベンダーをはじめとする金融市場関係者による DLT に関する取り組みは急速に進展しており、DLT に関する実証実験の実施、関連企業への出資及びコンソーシアムへの参加を通じて、その可能性を検討しているのが現状である。

DLT を金融市場インフラに適用することのメリットの 1 つとして、コスト削減効果が期待されている。M Mainelli et al.[2016][1]によれば、世界中の証券市場における清算・決済業務に係るコストは年間 400 億ドル以上に及んでおり、その多くがデータの照合と自動化されていないマニュアル業務から発生しているが、DLT を金融市場におけるポストトレード業務に適用することでコストの削減が見込めるという指摘がある。実際に、オーストラリア証券取引所は、DLT に関する研究開発を行う Digital Asset Holdings 社に 8.5%出資するとともに、自身が運営するオーストラリアの現物市場の清算・決済を含むポストトレード・サービスの IT システムを刷新するにあたり、DLT の適用を検討していることを発表している。

一方で、M Mainelli et al.[2016]は、DLT を金融市場インフラに適用するにあたり、技術的課題を解決したとしても、証券市場における取引所、清算機関及び振替機関といった金融市場インフラ運営者は、資産の保有・移転の証明だけでなく、規制執行と紛争解決の役割も担っていることから、これらの存在を排除することは現実的ではないことや、DLT を適用した新しい IT システムへのリプレースに係るコストは膨大となることを指摘している。また、SWIFT[2016][2]は、金融市場インフラへの DLT の適用に関する技術評価を行い、DLT について有望な進展は見られるものの、金融市場へと大規模かつ本格的に適用するには、より一層の研究開発が必要であると結論付けているなど、更なる技術革新の必要性も指摘されている。

株式会社日本取引所グループ（以下「JPX」という。）では、昨年来、社内で研究チームを立ち上げ、DLT の金融市場インフラへの適用可能性について調査・分析を行ってきた。また、2016 年 4 月

---

1 http://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf

2 https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services

～6 月にかけて行った 2 つの実証実験[3]を通じて、証券市場における発行・取引・清算・決済・株主管理といった一連のプロセスが DLT 上で実現可能かについて技術評価を行った。その結果、DLT を金融市場インフラに適用した場合、いくつかの課題があるものの、新たなビジネスの創出、業務オペレーションの効率化及びコストの削減等に寄与する可能性が高く、金融ビジネスの構造を大きく変革する可能性を持つ技術であることが分かった。

我々は、これまでの調査・分析等の結果から認識している課題や、今後期待する技術的な発展の方向性について、ワーキング・ペーパーとして公表し、広く関係者間で共有することによって、金融市場インフラに対する DLT の適用に向けた世界中における検討及び技術革新の一助となることを期待し、本稿を執筆することとした。なお、DLT は様々な規格が提案されているほか、世界中で日々研究・開発が行われていることから、本稿に記載した DLT に対する評価等については、あくまでも執筆時点の情報をもとにした見解であり、現状における筆者の理解不足や DLT の今後の技術革新により、将来的に変更の可能性がある旨、予めご理解をいただければ幸いである。

JPX は、当社の前身となる東京株式取引所及び大阪株式取引所が 1878 年に開設されて以来、約 140 年にわたり世界で有数の証券市場を運営してきた。また、我が国における証券市場の歴史を遡ってみても、1999 年の立会場閉鎖や 2009 年の株券電子化など、IT の進化を活用し、これまでに幾度となく金融市場インフラをより効率的なものへと変容させてきた。これらの経験と知見を活かし、今後も未来の金融市場インフラのデザインに貢献していきたい。

[3] 日本アイ・ビー・エム社との Hyperledger を用いた実証実験と、野村総合研究所(NRI)及びカレンシーポート社との Ethereum 系の「コンソーシアム/プライベート型」の DLT 規格を用いた実証実験。いずれも国内金融機関 6 社が参加。

II. ブロックチェーン/分散型台帳技術の概要

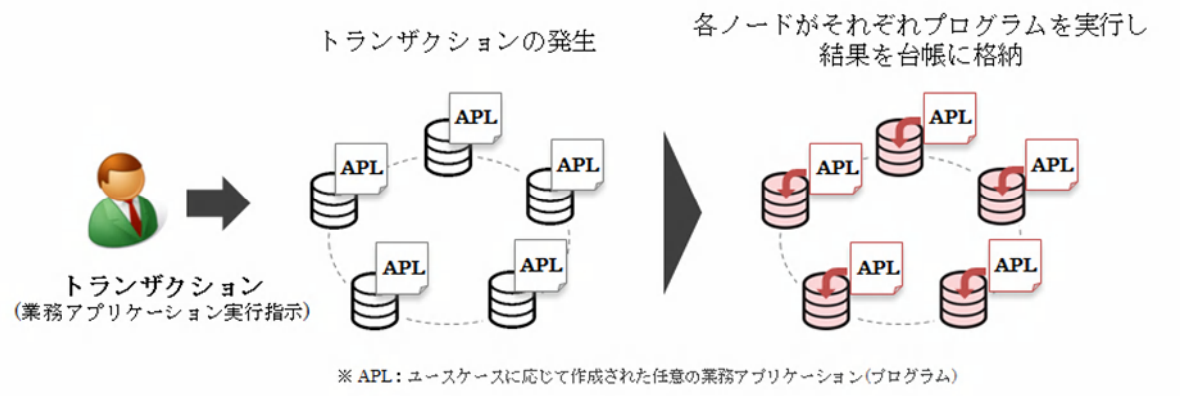
DLT は、ネットワークの参加者間で権利の移転を相互認証し、暗号技術を用いて実質的に改ざん不可能な形で台帳を共有する技術基盤である。2008 年 11 月に Satoshi Nakamoto を名乗る人物が公表した論文「Bitcoin: A Peer-to-Peer Electronic Cash System」[4]が DLT の始まりである。

従来型の法定通貨の場合、中央管理機関（各国における政府や中央銀行）が管理し、それを利用者が信頼することによって、通貨としての発行や流通の仕組みが成り立っている（中央集権型システム）。一方で仮想通貨の場合、政府や中央銀行のような中央管理機関の存在を必要とせず、参加者間の相互信用によって、その発行や流通の仕組みを成立させている（分散型合意形成システム）。

DLT は、(1)台帳を管理するデータベース技術、(2)暗号学的ハッシュ関数[5]と呼ばれるデータを圧縮する関数、(3)公開鍵暗号技術[6]、(4)P2P[7]と呼ばれる通信技術、(5)分散台帳の整合性を保つためのコンセンサスアルゴリズム[8]、の 5 つの技術要素から構成されている。現在、これらの各技術要素の組み合わせにより、様々な DLT の規格が提案・開発されており、仮想通貨以外にも様々なユースケースが提案されている。

利用を検討する分野によっては、複雑な取引条件や多様な業務プロセス等を DLT 上で実行する必要が生じる。このため、DLT 上で動作するチューリング完全なプログラミング言語[9]及びその実行環境を実装した規格も存在する。それらの規格を利用して、必要な業務アプリケーション(プログラム)を作成し、DLT 上に登録して実現する機能は、スマートコントラクトと呼ばれている[10]（図 1 参照）。

図 1 スマートコントラクトのイメージ



DLT の起源であるビットコインでは、誰もがネットワークへと参加することができる。一方で、法人間ビジネスのユースケースにおいては、ネットワークへの参加者を制限したい場合もある。DLT

---

[4] https://bitcoin.org/bitcoin.pdf
[5] 何らかのインプットを与えると、インプットの文字列の長さに関わらず、固定長のアウトプット（ハッシュ値）を出力する関数。
[6] 暗号化と復号をするための鍵が異なってペアになっている暗号化方式。鍵を「本人だけが用いる鍵（秘密鍵）」と「誰でも利用できる鍵（公開鍵）」の二つに分けることによって、鍵の受け渡し問題を解決している。
[7] ネットワーク上で対等な関係にある端末間を相互に直接接続し、データを送受信する通信方式。
[8] トランザクションをネットワークの参加者において認証し、複数のトランザクションをまとめた「ブロック」として台帳に取り込むための、一連の処理等のルールを指す。
[9] チューリングマシンと同じ記述・計算能力がある場合、そのプログラミング言語はチューリング完全であるとされる。チューリングマシンは、計算理論を議論するための仮想の計算機械であり、一定の手順に従えば答えが求められるような計算は、理論上すべてチューリングマシンで実行できる。
[10] 代表的な規格としては、Solidity と呼ばれる独自のプログラミング言語を実装した Ethereum がある。

の規格は、このネットワークへの参加に係るポリシーにより、「パブリック型」と「コンソーシアム型/プライベート型」の 2 種類に大別される（表 1 参照）。「パブリック型」の DLT 規格においては、悪意ある参加者のネットワークへの参加を事前に排除することができないが、「コンソーシアム型/プライベート型」の DLT 規格においては、ネットワークの参加者は互いに信頼できる限られた機関ないし単一企業内のみに限定される。このネットワークの参加者の信頼性等の違いにより、組み合わせるコンセンサスアルゴリズムが異なる傾向がみられる。

「パブリック型」の DLT 規格では、誰もがブロックを生成可能であるため、一部の悪意ある参加者が過去のデータを不正に改ざんできないよう、Proof of Work（以下「PoW」という。）のように一定の作業負荷をコンセンサスアルゴリズムに組み込んでいる。また、そのような作業を実施してブロックを生成する見返りとして、ブロックの生成者には仮想通貨による報酬等のインセンティブが付与されていることが一般的である。

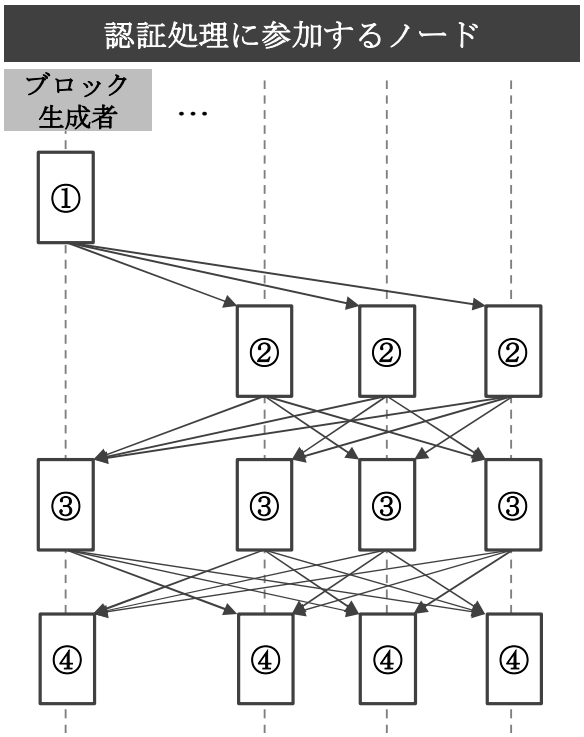
表 1 「パブリック型」と「コンソーシアム型/プライベート型」の比較

	パブリック型	コンソーシアム型/プライベート型	
ネットワークへの参加	自由	承認が必要	
特徴	中央管理機関が不要	[コンソーシアム型] 特定の企業グループなど信頼の置けるメンバーのみが利用	[プライベート型] 特定の組織の内部で利用

一方、「コンソーシアム型/プライベート型」の DLT 規格では、ブロックを生成する権限を特定の参加者のみに限定することが可能である。また、同一の個人や企業等がネットワーク上にノードを複数所有することを制限することが可能である。こうしたアクセス制限があるため、単純なルールに従い定められたノードがブロックを生成し[11]、特定の参加者の一定比率の合意により認証するという、比較的高速なコンセンサスアルゴリズムの採用が可能となっている。現状では、M Castro et.al [1999][12] によって提唱された分散型合意形成アルゴリズムである Practical Byzantine Fault Tolerance（以下「PBFT」という。）を DLT へと応用したコンセンサスアルゴリズムが多く見受けられる。PBFT では、約 3 分の 2 以上の合意を条件とする事によって頑健な合意を確保するとともに、総ノード数 n 台に対して(n-1)/3 台までの障害耐性を持つ（図 2 参照）。また、PoW で求められるような計算処理等を必要としないため、比較的高速な認証処理が可能である。

[11] ノード障害等が発生しない限りブロック生成者を常時固定する、1 ブロックずつラウンドロビンに交代する等、DLT の規格により異なる。
[12] http://pmg.csail.mit.edu/papers/osdi99.pdf

図 2 PBFT をベースとしたコンセンサスアルゴリズムにおける認証処理の流れ



n … 認証処理に参加するノードの総数
f … (n-1)/3　※ 障害を許容できる最大ノード数

①新しいブロックを生成し、他のノードに対し送信

②ブロックに含まれるトランザクションが改ざんされていないこと等、ブロックの内容の正当性を確認し、確認結果を他のノードに対し送信

③2f台のノードがブロックについて合意していることを確認し、ブロックを承認する準備が整った旨を他のノードに対し送信

④自身を含む2f+1台のノードでブロックを承認する準備が整ったことを確認し、自身が持つ台帳にブロックを取り込む

III. 実証実験

金融市場インフラに対し DLT を適用する実証実験の実例は現時点では乏しいため、公表情報に基づいた調査・研究だけでは得られない知見を獲得すべく、実証実験を実施した。

1. 採用した規格

仮想通貨と証券は、その商品性や取引・決済手法が異なるため、DLT に求められる機能も異なる。

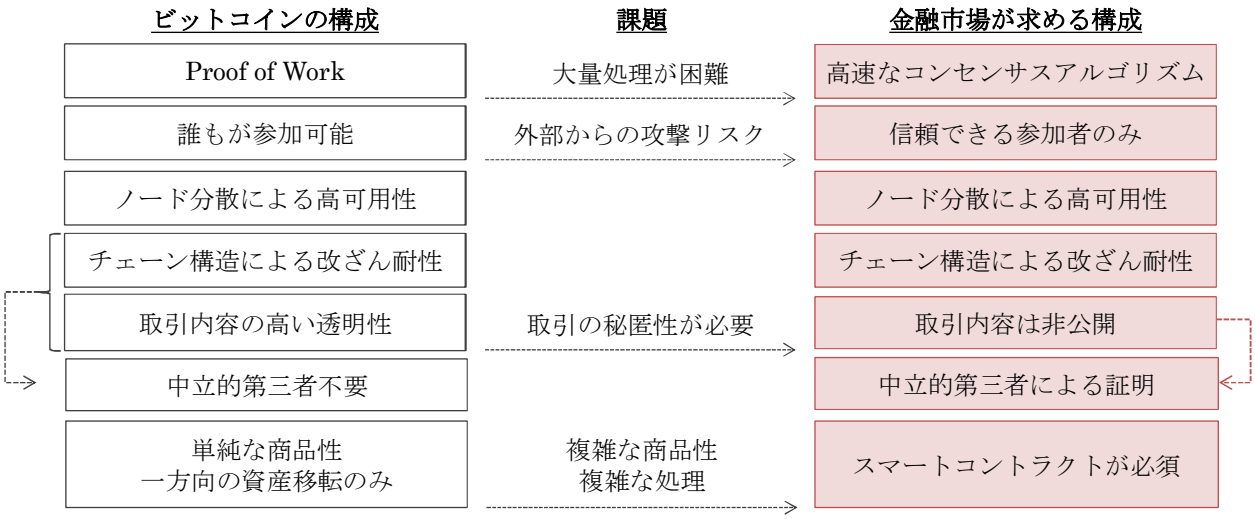
まず、既存の仮想通貨のスループット性能[13]は日々の証券決済を安定的に処理するには不足であり、スループット性能の向上が求められる。長期的な視点から PoW 型をベースとした性能向上には限界があると考え、PBFT をベースとしたより高速なコンセンサスアルゴリズムを採用することとした。ノード支配や外部攻撃への耐性といったセキュリティ強度は、信頼できる参加者のみが認証処理に参加するノードを保有する許可型ネットワークと組み合わせる事により解決を図る事とした。

また、ID の匿名性が保たれているといえども、大口取引の存在や相対取引における価格等の条件が即時に参加者間で共有されることが、利用者に受け入れられるとは考えにくい。従って、通常の利用者は自身が当事者である情報のみが参照でき、一方で市場管理者が全ての情報を参照し権利等の移転・所有の証明を担うといった、情報の複層的な参照制御が実現できることが望ましい。

さらに、金融市場で取り扱う商品は仮想通貨と比較すると商品性が複雑であり、合意・確認が必要な比較的複雑な処理が多いため、スマートコントラクトの活用は必須である。

以上の観点より、本実証実験においては、「コンソーシアム型」の DLT 規格を用いることとした。

図 3 金融市場が求める DLT の構成



2. 実証実験環境の概要

今回は 2 つの実証実験を行っており、検証範囲や実装方法について細かい差はあるが、説明の単純化のために両者を総合して概要の説明を行う。

[13] 参考として、現状、ビットコインのスループット性能は秒間 7 件程度となっている。

実証実験環境はパブリッククラウドサービス上に構築し、ノード数はトランザクションの認証処理等に必要な最小限とした。取引所/清算機関/振替機関を市場管理者として、認証処理には市場管理者及び市場参加資格を有する金融機関のみが参加することとした。また、上場会社は DLT 上における自社に関するデータの参照のみ可能とした。証券は DLT 上の記録の書き換えを振替処理とみなす事とし、資金決済は DLT 上にトークンの移転として記録した後、外部決済システムとの連携を行う事とした。また、投資家単位の口座情報を DLT に登録することで、金融機関名義ではなく投資家間での決済等を DLT 上に直接的に記述し、投資家単位での保有者情報がリアルタイムで更新されることとした。一方で、投資家に対する口座開設における事前審査等[14]は、DLT の外部で金融機関により実施される想定とした。

① 証券発行
- 市場管理者は DLT 外での発行体(上場会社)からの申請に基づいて、DLT 上に発行体情報を登録し、新たに発行する証券を発行体の口座に記録
- 新たに発行した証券は発行体から引受金融機関、引受金融機関から投資家へと DLT 上で移転

② コーポレートアクション(配当・株式分割)
- 発行体の申請に基づいて市場管理者がコーポレートアクション処理を実行
- 該当する証券の保有者に対し、残高に応じて配当として付与される資金トークンや分割により増加する証券が計算され、DLT 上の記録が更新される

③ 証券保有者参照
- 証券を保有する投資家及び保有残高のリアルタイムでの更新
- 発行体は自社の株主のみ参照可能である一方、市場管理者は全ての投資家を参照可能

④ 取引(照合)
- 注文を DLT 上に登録し、新たに到来した注文が登録済みの反対注文のいずれかを選択した場合、取引として記録（掲示板方式のマッチング）
- DLT 外での交渉により二社間で取引条件に合意した取引を、一方が DLT 上に登録し、他方がその内容の確認を行う（二社間の取引内容照合）

⑤ 証券決済
- 証券の振替処理は DLT 上での認証をもって完了とみなす
- DVP 決済（資金証券同時決済）実現のために市場管理者の承認を必要とする機能や、複数の決済をネッティングする機能も実装

⑥ 資金決済
- 資金決済は DLT 上にトークン移転として記録され、既存の外部資金決済システムに連携されると想定
- DVP 決済実現のために市場管理者の承認を必要とする機能や、複数の決済をネッティングす

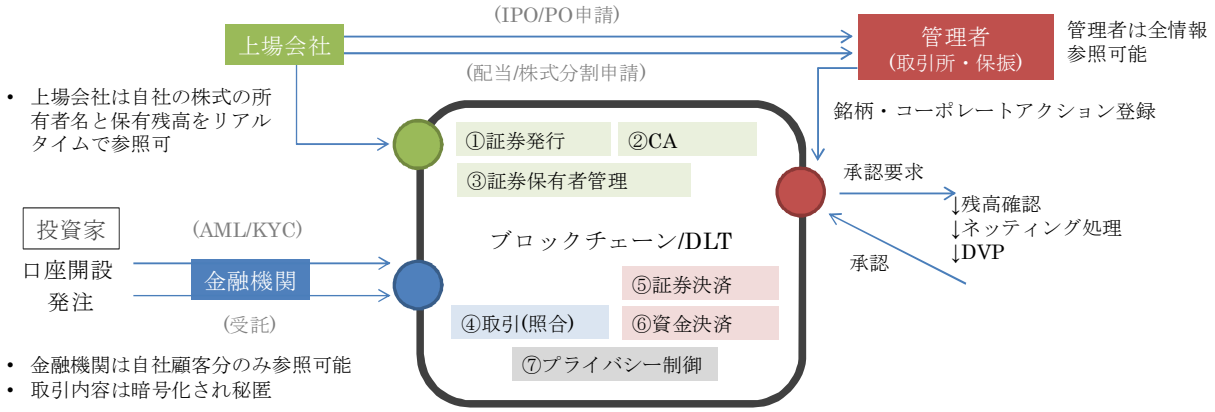
[14] KYC（Know Your Customer、各種書類手続き等）や AML（Anti-Money Laundering、マネーロンダリング対策）など。

る機能も実装

⑦ プライバシー制御

- 金融機関は自社の顧客以外の投資家情報及び無関係な取引内容は参照不可
- 発行体は自社の株式の所有者名と保有残高をリアルタイムで参照可能である一方、他の発行体に関する情報や取引内容の参照は不可
- 市場管理者は DLT 上の全て情報への参照権限を持つ

図 4 実証実験環境の概要



IV. 評価・考察

1. 技術基盤としての特性

本節では、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、金融市場インフラに対する適用を想定した場合における DLT の技術基盤としての特性について、(1) 金融市場業務との親和性、(2)処理性能、(3)認証処理、(4)秘匿性、(5)可用性、(6)コストの 6 つの観点から評価・考察する。

(1) 金融市場業務との親和性

証券は仮想通貨と異なり、複雑な商品性と処理フローを持っているため、スマートコントラクトの利用が必須となる。実証実験において採用した DLT 規格は、いずれもスマートコントラクトの実行を想定してチューリング完全なプログラミング言語の実行環境が実装されているため、前章で列挙した金融市場における基本的な機能は、概ね DLT 上で実装することができた[15]。ただし、DLT との親和性については業務や機能毎に異なるため、以下にそれぞれの所見を述べる。

(a) 取引（照合）

証券市場における「取引」では、その機能上の工夫のほとんどが、取引が成立する前のプレトレード処理における「注文を如何に効率的にマッチングさせるか」にある。取引の相手方が見つかる確率を上げて、価格競争により最良価格での取引を成立させるために、市場運営者は如何に注文を自市場に集中させるかの努力を行っている。こうした特徴と分散ネットワーク上での処理という DLT のアーキテクチャーは基本的に親和性が低く、既に効率的な集中処理型の市場が存在している場合、改善をもたらすのは難しい。

また、取引の多い株式市場等では注文の変更・取消が頻繁に発生するため、DLT の改ざん不可能という特徴が逆に効率を悪くしてしまう。こうした状況を踏まえると、プレトレード処理については、DLT の外で処理した方が良いと考えられる。

ただし、相対取引については、上記の競争売買の要素が少ないため、DLT で処理する事も可能である。また、関係者間での照合プロセスは有望なユースケースとなり得る。

(b) 清算・決済

取引と異なり集中処理の必要性が薄いため、DLT による分散処理は可用性をはじめとした便益をもたらす。中心的なユースケースと考えられるため、次節において詳説する。

(c) 証券保有者管理

仮想通貨の移転に係るフロー情報のみを台帳に記録するビットコインとは異なり、実証実験で採用した DLT 規格においては、業務データのステート情報についても管理されている。また、規格により詳細は異なるものの、木構造を用いた効率的なデータ格納方式等により、過去のブロックの生成時点毎におけるステート情報について比較的容易に参照可能となっている（図 5 参照）。

---

15 チューリング完全なプログラミング言語により、多種多様な機能が実装できる一方で、無限ループ等、予期せぬ不具合が生じる可能性もあるため、タイムアウトによる強制終了等、適切なエラー処理の実装も必要となる。

この特性により、過去の任意の時点における証券等の保有者・保有残高について、当該時点においてスナップショット情報の取得等の特段の対応をせずとも、遡及的に確認可能である。

(d) コーポレートアクション

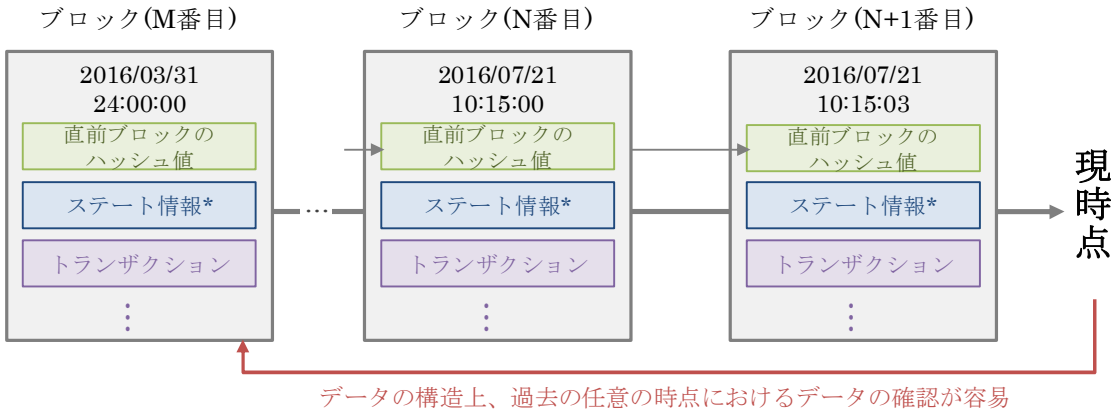
上記(c)において述べた DLT の特性より、配当・株式分割等のコーポレートアクション処理における、株主に対する権利付与の基準日時についても、過去の任意の時点の指定が可能である。従って、DLT を活用することで、コーポレートアクション処理に係る事務負担について、軽減されることが期待できる。

以上を踏まえると、証券市場のポストトレード分野において DLT を活用することにより、将来的に既存の業務フローの大幅な効率化が達成される可能性があると考えられる。

一方で、適用の障害になりえる幾つかの懸念事項も発見された。将来における債券の金利の支払いやデリバティブの満期処理等のタイムトリガーイベントの処理については、各ノードが保持するシステム時刻の差により、実行タイミングに差異が生じる可能性がある。また、変動金利型商品の対象金利情報や、オプションの権利行使における原資産価格のように、外部データを取得する際も、各ノードが独自に取得すれば異なる値となる可能性がある。乱数発生を要する複雑な計算処理を行う場合、各ノードが独自に計算する事で異なる結果となる可能性がある[16]。

特定のノードにこうした処理を担わせる解決方法もあるが、当該ノードが単一障害点になるという別の懸念をもたらす。

図 5 過去のブロックの生成時点毎におけるステート情報の参照



*実際には、木構造で格納されたステート情報のルートノードのハッシュ値のみをブロックに格納することが一般的

(2) 処理性能

金融市場インフラに対する DLT の適用を検討する際に、トランザクションの処理性能は大きな課題となる。対象とする商品の取引頻度にもよるが、例えば先進国の上場株式市場のポストトレードに係るインフラとしての活用を考えるのであれば、秒間数千～数万件の処理性能が望ましい。

16 実行結果については、業務データ自体ではなくハッシュ計算されたダイジェスト値で比較されるため、各ノードが保持する台帳はバイト列レベルで完全に一致する必要がある。

DLT の単位時間あたりのトランザクション処理可能件数であるスループット性能は、コンセンサスアルゴリズムの仕様に大きな影響を受ける。最も基本的な例として、ビットコインにおけるスループット性能は、以下の式で定義される。

スループット性能＝1 ブロックあたりの最大処理件数÷ブロックの生成及び認証処理の所要時間

（1 ブロックあたりの最大処理件数＝ブロックサイズ上限÷トランザクションの平均メッセージサイズ）

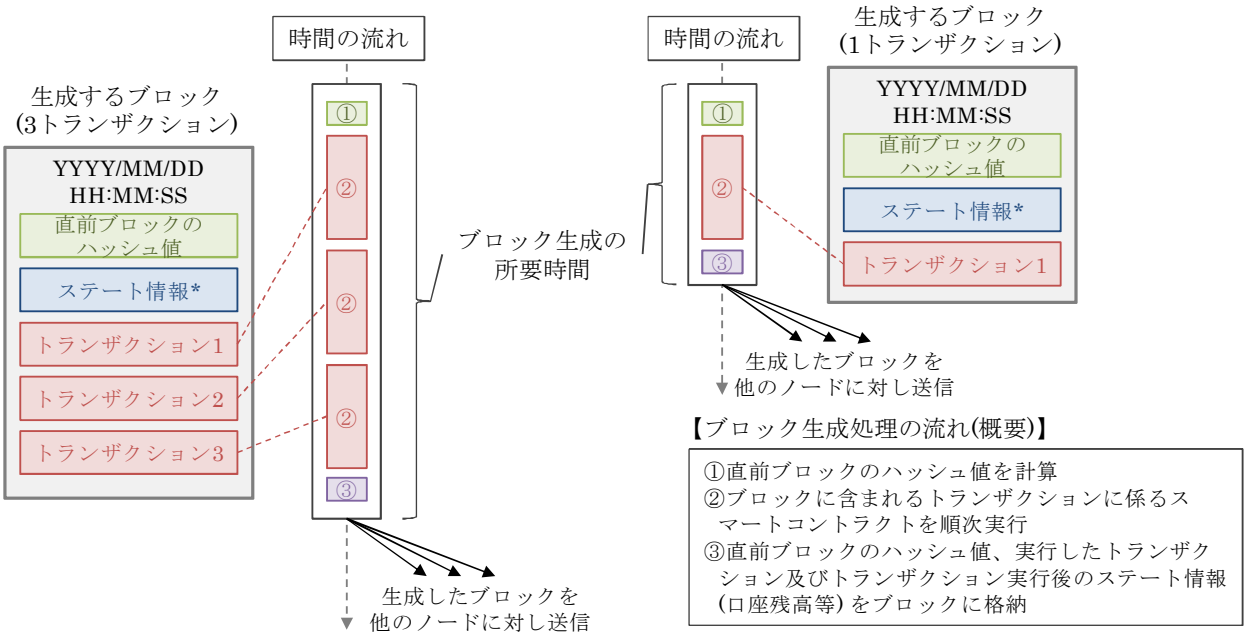
この場合、スループット性能を向上させるためには、1 ブロックあたりの最大処理件数の増加またはブロックの生成及び認証処理の高速化が必要となる。ただし、前者については、1 ブロックあたりのデータ容量の上限を引き上げる必要があるが、ブロックサイズが大きくなると認証処理におけるノード間通信に必要なネットワーク帯域が増加する。また、後者についても単純な議論ではない。ブロックの生成及び認証処理に要する時間の大部分を占める PoW に要する所要時間を短くした場合、改ざん耐性の低下と、仮想通貨供給速度の上昇によるインフレーションを招く恐れがあるため、安易な高速化を行いにくいという問題がある。

一方で、「コンソーシアム型/プライベート型」の DLT 規格のように、予め信頼されたノードのみでブロックを生成できる場合、PoW を必ずしも必要とせず、より高速なコンセンサスアルゴリズムを採用することが可能である。なお、コンセンサスアルゴリズムが十分に高速である場合、認証処理に要する時間に関してノード間のネットワークレイテンシーが無視できない要素となるため、ノードを地理的に近接させたほうがスループット性能の面では有利となる。一方で可用性の観点からは、天災等に対する障害耐性の面で、ノードは地理的に分散していることが望ましいことから、これらのバランスには留意する必要がある。

実証実験において実際に大量のトランザクションを投入するハイトラフィックテストを実施したところ、秒間で数十～百件程度のスループット性能が上限となった。特に Hyperledger について、このハイトラフィックテスト時におけるシステム稼働状況について分析したところ、CPU 等のシステムリソースには余力がある状態であり、スマートコントラクトを 1 件ずつ直列実行していること等がボトルネックとなっていることが分かった（図 6 参照）。ビットコイン等のシンプルなユースケースにおいては、権利の移転に係る情報がトランザクション内に直接的に記述されているが、スマートコントラクトを活用するユースケースにおいては、トランザクションが指示する内容はプログラムにより実行されるため、スループット性能の向上のためにはプログラムの効率的な実行等が課題となる。また、今回の実証実験ではスマートコントラクトの直列実行がボトルネックとなっていたが、スループット性能にはノード総数やネットワークの地理的分散状況等、様々な要因が影響すると考えられることから、今後、更なる検証が必要である。

リアルタイムでの処理性能が重視される上場株式市場の売買システム等においては、処理対象となる銘柄等を複数のサーバに分散させて並列処理することで、市場全体のスループット性能を高めている。DLT において各ノードはシングル構成であることを前提とすれば、今後の技術的な改善は想定されるものの、上場株式市場の売買のようにトランザクションが多い処理への適用は課題がある。一方で、ミリ秒・マイクロ秒といったレベルでのリアルタイム性が必ずしも必要とされないポストトレード分野に限定することや、トランザクション数が相対的に少ない相対取引の分野を適用対象とすれば、現状の DLT の処理性能でも一定程度の要件充足は可能であると考えられる。

図 6　スマートコントラクトの直列実行による処理性能のボトルネック



*実際には、木構造で格納されたステート情報のルートノードのハッシュ値のみをブロックに格納することが一般的

(3)　認証処理とネットワークアクセス

適切な認証アルゴリズムとネットワークアクセスの組み合わせはユースケースによって異なる。

「パブリック型」の DLT 規格においては、悪意ある参加者のネットワークへの参加を事前に排除することができないため、データの改ざん等の不正行為に対する堅牢性が不可欠であることから、PoW やその派生型のコンセンサスアルゴリズムを選択するのが合理的である。一方で、「コンソーシアム型/プライベート型」の DLT 規格においては、認証処理の参加者は信頼された機関内ないし自社内のみに限定されるため、ブロックの生成権限を信頼できる特定のノードに限定する等により改ざん耐性を担保することで、大量のトランザクションを効率的に認証できる処理性能に重点を置くことができる。

また、市場参加資格を有する金融機関が投資家と市場の間を仲介する現状の仕組みは、仮に DLT を用いて金融インフラを構築したとしても、投資家保護やマネーロンダリング防止措置といった要件を満たすために効率的かつ現実的な方法である。この点からも、「コンソーシアム型/プライベート型」の規格を採用することが合理的であると考えられる。

「コンソーシアム型/プライベート型」において多く採用されている PBFT をベースとしたコンセンサスアルゴリズムにおいては、予め指定されたノードの 3 分の 2 以上の承認により処理が進むため、台帳の一時的な分岐(フォーク)を防ぐ設計が可能であり、トランザクションのファイナリティが安定して即時に得られる。この点も、金融市場インフラへの適用を想定した際の大いなる利点である。

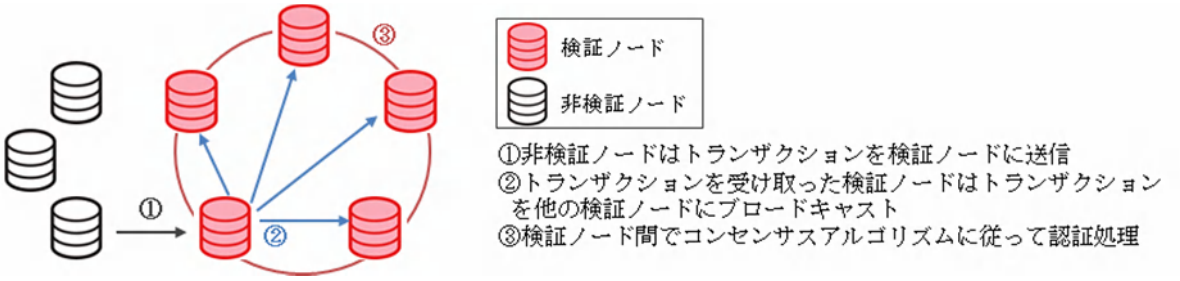
PBFT をベースとしたコンセンサスアルゴリズムにおいて、台帳を保持すると共にブロックの認証処理に参加できるノードは検証ノードという。一方、認証処理に参加しないが、トランザクションを

生成する権限のみを持つノードは非検証ノードという（図 7 参照）[18]。金融市場インフラに対する DLT の適用を想定した場合、各ノードの管理主体は金融市場インフラ運営者及び金融機関とする事が適切と考えられる。ただし、全ての金融機関が検証ノードを保有する必要は必ずしもないため、各金融機関の判断に応じて検証ノードと非検証ノードどちらを保有するかの選択が行われると考えられる。

また、認証処理により飛び交うメッセージ量は検証ノード数に比例するため、必要なネットワーク帯域にも影響を及ぼす。PBFT をベースとしたコンセンサスアルゴリズムにおいては、最初にブロックの生成者が新しいブロックを他の検証ノードに対して送信する通信が、トランザクションの内容自体を含んでいるために、最もメッセージサイズが大きい。一方で、その後に検証ノード間で検証結果等を送信し合うフェーズにおいては、ブロックの情報についてはダイジェスト値のみやり取りされるため、メッセージサイズは小さいものの、各検証ノード間で相互に通信が発生することに留意が必要である。

なお、内部通貨によるインセンティブ付与がないコンセンサスアルゴリズムの場合、金融機関が検証ノードを保有するインセンティブをどこに置くのかは、「コンソーシアム型」のユースケースにおける今後の課題になると考えられる。

図 7 検証ノードと非検証ノードの違い



(4) 秘匿性

「パブリック型」のサービスの代表例であるビットコインにおいては、過去の全ての取引の記録を取引当事者の匿名 ID と共に公開することにより、どの ID がどれだけのビットコインを所有しているかを追跡可能としている。この高い透明性と過去の取引の改ざんが困難なコンセンサスアルゴリズムが、中央管理機関の介在を必要とせずに各 ID におけるビットコインの所有証明を実現するための基盤となっている。

一方で、金融市場における取引については、大口取引や大口ポジションの存在がリアルタイムに公開されてしまうことにより、フロントランニングを誘引する可能性があるほか、法定開示書類等と照らし合わせることで、本来は匿名である DLT 上の ID と最終投資家の紐付け情報の特定につながるおそれがある。また、相対取引のケースにおいては、取引条件(数量及び価格)を取引当事者以外に対して公開したくないという要望等も想定される。

こうした懸念や業務要件を踏まえると、過去の取引の記録等について、取引当事者以外は参照できないことが望ましい。一方で、公衆監視による所有証明という要素が失われてしまうため、当事者が

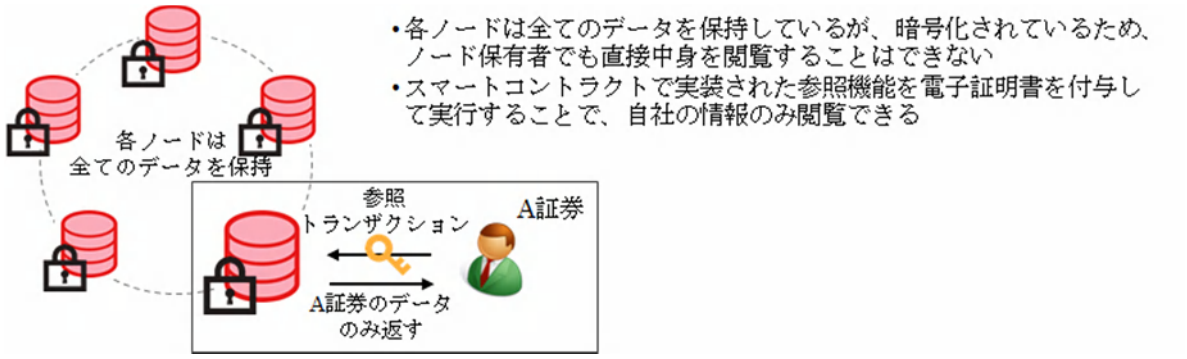
[18] 執筆時点における Hyperledger 等の DLT 規格の定義に基づく。

所有を主張したとしても、他者はその正当性を確認する術がない。したがって、中立的第三者に全ての情報の閲覧権を与えて、所有証明の役割を担わせる仕組みが必要となる。

また、「コンソーシアム型」の DLT を利用する場合、全取引情報が含まれた台帳を複数金融機関で共有する事になるが、ノード所有者であっても自社以外の取引情報は見られないという秘匿性要件が満たされないと、共有型インフラとしての利用は進まないと考えられる。

実証実験では、取引所/清算機関/振替機関といった金融市場インフラ運営者が、中立的第三者として公開鍵暗号基盤における認証局の役割を担い、ネットワークへの参加資格を有する各金融機関に対して電子証明書を発行した。その上で、台帳及びトランザクションについては暗号化を施し、各金融機関は各々が参照権限を持つデータのみ参照できるようアクセス制御を施した。具体的には、台帳上の過去の取引等の参照はスマートコントラクトにより業務機能として実装し、各金融機関は自身の電子証明書を添付してトランザクションを実行することで、自身が取引当事者である取引の情報や自社の顧客の口座のみが参照できる仕組みを構築した（図 8 参照）。また、トランザクションは他のシステム領域から保護・隔離されたスマートコントラクトのプログラムを実行するための仮想マシン上でのみ復号されるため、認証処理に参加する検証ノードの保有者であっても、無関係なトランザクションの内容を知ることはできない。検証ノードを保有する各金融機関において、既存の一般的な金融 IT システムと同様にソフトウェアに対する不正・改ざんが適切に防止され、かつ暗号化された台帳及びトランザクションについて、対応する秘密鍵なしに復号することは不可能であるとみなせる場合[19]、これらの実装により、各金融機関が共通の台帳を保有しつつも、取引内容等について他社に対して情報を秘匿することが可能である。ただし、これらは Hyperledger を用いた環境でのみ実現できた内容であり、金融市場インフラへの適用において求められる秘匿性要件を満たせる DLT 規格は、現状では極めて限定的であると考えられる。

図 8 暗号化と電子証明書を用いた秘匿性の実現



(5) 可用性

取引所、清算機関及び振替機関といった金融市場インフラ運営者にとって、可用性の向上は DLT を採用する大きな動機となる。もちろん、これらの機関が運営する現状の金融市場インフラにおいても、ハードウェア機器の徹底した品質管理や冗長化等を行う事で高い可用性を実現できているが、これらを維持するのは容易ではなく、また相応のコストも必要である。

DLT を採用すれば、一部のノードにシステム障害が発生しても、全体としてブロックの認証処理

[19] 暗号化されているとはいえ、物理的には自社の情報が競合他社の保有するサーバ内に格納されることとなるため、採用する暗号化技術の信頼性に対しては事前に十分な見極めが必要である。

に必要な一定数以上のノードが存在する限り、インフラの維持運営を続ける事が可能である。従って、ノードの保有が金融市場インフラ運営者だけでなく、金融機関といった金融市場インフラ利用者まで普及すれば、現在のサーバーセントリックなモデルよりも障害耐性が高まると想定される。さらに、国際的な金融市場インフラ運営者同士で検証ノードを分散保有する事で、可用性の高い IT インフラ上に協調してサービスを展開することも考えられる。

また、各ノードが互いに同期されたデータを保有しているため、一部のノードにおいてシステム障害等によりデータロストが発生した場合でも、データの復旧が容易に可能であるという点も DLT の特徴である。

このような DLT の技術的特性を踏まえると、現状ではインフラ運営者及び各市場参加者が個々に実施している BCP 対策について、業界横断的に効率化することも可能である。ただし、そのためには本節(4)に述べた暗号化技術による情報の秘匿処理が必須となる。

なお、こうした DLT が有する特徴を活かすためには、天災等により多数のノードが一斉にシステム障害となる状況を避けるべく、ノードの設置場所は地理的に分散されていることが望ましい。また、本節(1)にて述べたとおり、現時点で金融市場インフラに対する DLT の本格的な適用を考えた場合には、DLT による実装が困難な一部の機能について特定のノードに担わせることや、外部システムとの連携が必要となるため、機能単位では単一障害点は残る可能性がある点について留意しておく必要がある。また、スマートコントラクトとして実装する業務アプリケーション自体は、従来どおりユースケースに応じてユーザー企業が開発することになるため、複雑な業務機能を実装した場合にはアプリケーション障害の発生リスクが高まり、DLT の特性としての高可用性が充分に活かせなくなるおそれがある。

なお、DLT を適用したインフラ上において特別な権限を有する管理者ノードの要否については、ビットコインを端緒とする「パブリック型」の DLT の思想においては不要とされるが、DLT を金融市場インフラに適用する事を考えた場合、中立的第三者の存在を想定した方が円滑なインフラ運営が可能となると想定される。ただし、DLT の技術的な利点を活かすためには、管理者ノードが単一障害点化しないよう、その役割を限定する事が望ましい。この中立的第三者の役割を担う候補としては、既存の取引所/清算機関/振替機関といった金融市場インフラ運営者の他、監督官庁や IT ベンダー等も考えられる。

(6) コスト

金融市場における IT システムを一般的なクライアントサーバ型システムで構築した場合と、「コンソーシアム型/プライベート型」の DLT 規格を用いて構築した場合について、a.アプリケーション開発、b.ハードウェア、c.ソフトウェア、d.保守の 4 つの観点からコスト比較の検討を行った。結果は表 2 のとおりであり、厳密な計算等は行っていないものの、ハードウェア・ソフトウェア関係の費用や保守費用が低下する可能性がある。ただし、これらの単純な IT インフラの置き換えによるコスト削減効果は限定的であり、DLT の採用によるコストへの主要なインパクトは、本節(1)に述べたようなビジネスプロセスの改善によるオペレーションコストの削減によりもたらされるものと考えられる。また、本節(5)に述べた業界横断的な BCP 対策の実現により、業界全体の BCP 対策費用の削減へと繋がることも期待される。

表 2 クライアントサーバ型の IT システム構成と DLT のコスト比較

項目	DLTを採用した場合のITコスト
a.アプリケーション開発	差異なし 開発単価を同等と仮定した場合、コストに差異は認められない
b.ハードウェア	削減の可能性あり 必要なデータ容量は大きくなるが、複数ノードによる冗長構成となっていることから、ハイエンドストレージを採用する必要がない
c.ソフトウェア	削減の可能性あり ただし、現在、DLTはオープンソースであるものの、将来的に製品化された場合は不明
d.保守	削減の可能性あり 複数ノードによる冗長構成となっていることから、ハードウェア故障時における復旧までのリードタイム等のサービスレベルを緩和できる可能性

2. 証券決済に係る論点と評価

本節では、DLT の証券決済への適用可能性について、(1)ファイナリティ、(2) DVP 決済の実現、(3) 大規模ポストトレード処理への適用における留意点、の 3 点に注目して議論を行う。

(1) ファイナリティ

決済業務におけるファイナリティとは、一般に「決済が無条件かつ取消不能となり、最終的に完了した状態」を指し、決済インフラとしての安定性を考えるにあたって重要な概念である。

「パブリック型」の DLT 規格では、台帳の一時的な分岐(フォーク)のリスクがある事が知られており、トランザクションの認証の状態が手戻りする可能性がある。このため、権利移転のタイミングを明確に定義することが出来ず、ファイナリティが不安定なものとなる。

これについては、「コンソーシアム型/プライベート型」の DLT 規格を採用するとともに、PBFT 等をベースとしたコンセンサスアルゴリズムを採用し、フォークを発生させない設計とすることにより、解決する事が可能であると考えられる。

(2) DVP 決済の実現

今日における金融市場は、資金と証券の受け渡しを同時に行う DVP 決済により、円滑な決済を行っている。実証実験においては、スマートコントラクトにより受渡しタイミングをコントロールする事で、技術的には DLT 上で DVP 決済が実現可能であることを確認した。

一方で実務への適用にあたっては幾つかの課題がある。まず、既存の業務プロセスにおいては、電子化された有価証券を証券保管振替機構(CSD)の参加者間の口座振替を行う事で、証券決済のファイナリティを得ている。技術的にはそのような機能を DLT 上で実装する事はできるが、法律や規制上の有価証券の権利記録は DLT を真正なものとする、という制度上の整理が必要である。また、資金

決済のファイナリティについては、現実の決済通貨である日本円は DLT 上に記録されていないことから、DLT 上でファイナリティを得るための工夫が必要となる。対応案としては、案 1：既存の決済インフラとの連携、案 2：決済にかかわる金融機関内のみで流通する貨幣トークンの活用、案 3：デジタル通貨の活用の 3 点が考えられる。

対応案 1：既存の決済インフラとの連携

資金決済に現実の法定通貨を利用する場合、法定通貨としての日本円の決済が銀行口座間で移転して初めてファイナリティが得られる。これを DLT 上で実現するためには、既に出来上がっている法定通貨ベースの決済インフラ(日銀ネット等)に対して、決済指示電文を送るという形で資金決済を解決するという方法が考えられる。

他の案と異なり、証券決済と資金決済が異なるインフラで行われるため、タイミングを合わせるための工夫が必要である。具体的には、証券決済のトランザクションについて、DLT 上で決済に必要な証券を拘束した状態で留保しておき、外部資金決済インフラからの資金決済完了の電文授受をトリガーとして、DLT 上での証券決済を完了させることが考えられる。この方法では、日銀当預口座における資金の移転が行われるため、対応案 2 と異なり、現行のファイナリティに対する考え方を踏襲することができる。

対応案 2：決済にかかわる金融機関内のみで流通する貨幣トークンの活用

貨幣トークンの活用にあたっては、決済にかかわる金融機関が法定通貨を信託銀行に預託し、それを裏付けとして貨幣トークンの発行を受け、その貨幣トークンを用いて当該金融機関間での資金決済を行う方法が考えられる。厳密なファイナリティではないが、金融機関が破たんした場合には裏付けとなる法定通貨を差し押さえる事が出来るという前提で、貨幣トークンの授受をもって資金決済が完了したものとみなすことが出来ると考えられる。対応案 1 と比較すると、外部システムとの複雑な通信が不要となるため、DLT 上の処理の効率化が期待できる。

なお、貨幣トークンの流通範囲を金融機関以外にも広げた場合は、換金需要への対応や破たん時の処理という問題が発生するため、論点が複雑となることに留意が必要である。

対応案 3：デジタル通貨の活用

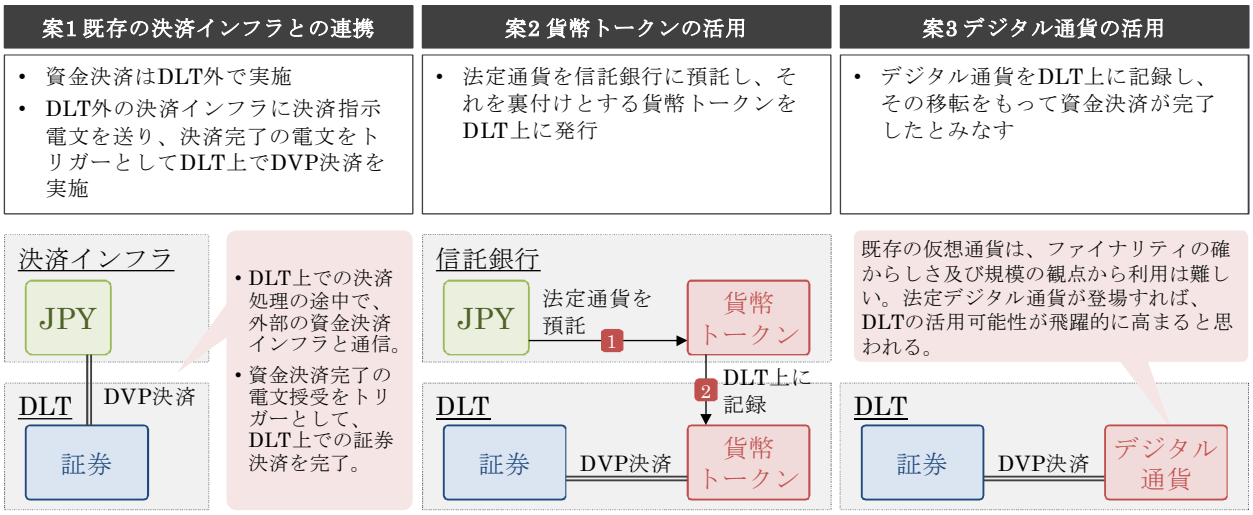
仮想通貨を DLT 上に記録し、その仮想通貨の移転をもって資金決済完了とする事は、技術的には可能であるが、実務への適用にあたっては 2 つの課題があると考えられる。1 点目は、仮想通貨を受け取った主体が、仮想通貨の受領をもって、資金決済のファイナリティが得られたと判断できるかという点である。資金決済のファイナリティは、それを受け取った主体が、決済・商取引・貯蓄に利用できる事の確からしさ、または法定通貨との換金の確からしさを信じられるかどうかに依存する問題であり、解決には仮想通貨を取り巻くエコシステムの醸成が必要となる。2 点目は、仮想通貨の規模である。最大の市場規模を持つビットコインでも時価総額は 1 兆円程度（2016 年 6 月末現在）であり、1 つの先進国の金融インフラを支えるのすら難しいという課題がある[20]。

安定したファイナリティと十分な発行量を保証する法定デジタル通貨を中央銀行が発行し、DLT 上で取り扱う事を可能とすれば、これらの問題を抜本的に解決する可能性がある。法定デジ

[20] 例えば、2015 年における日本国債の売買代金は売り買い合計で 11 兆 9,401 億円（日本証券業協会調べ）。また、東京証券取引所の 2015 年における株式の一日平均売買代金は 3 兆 573 億円。

タル通貨については、世界各国の中央銀行や CPMI[2015][21]をはじめとした国際的なコミュニティにおいて議論が行われているが、前述の 2 つの対応案と比較して、考慮すべき事項は圧倒的に多いと考えられることから、今後、更なる議論や調査・研究が望まれる。

図 9 DLT 上で資金決済を行う対応案



(3) 大規模ポストトレード処理への適用における留意点

DLT の基盤技術としての特性を踏まえると、金融市場のポストトレード分野との親和性が高い技術であると考えられる。また、少量のポストトレード処理については、現状の DLT 技術で大きな問題は生じないと考えられる。一方で、長期的な課題として、大規模ポストトレード処理を円滑に行うために既存インフラが備えている機能については、DLT 上で検証した例はほとんど公表されていないことから、適用に向けて考慮すべき事項について検討した。

ポイント 1：処理プロセスの変化による流動性への影響

ビットコインは取引（約定）と決済（受渡）をほぼリアルタイムで処理していることから、DLT を金融インフラに適用することにより、取引から決済までをシームレスに処理する事が出来るとの指摘がある。

仮に証券決済をリアルタイムで処理することとし、DVP 決済を行うこととした場合、必要な証券及び資金があらかじめ口座内にあるかを確認し、必要な残高があることをリアルタイムで厳密に確認する事となる。

一方で、現在の証券市場においては、取引と決済がシームレスになっていない事から、信用取引や貸株制度、預かり資産に応じた買付可能額の設定により、流動性を向上させている。決済処理のリアルタイム化とシームレス化により、こうした効果は失われる可能性がある。

ポイント 2：ネッティング

証券のポストトレード処理においては、複数の当事者間で債権と債務を相殺し、その差分を決済

[21] http://www.bis.org/cpmi/publ/d137.htm

するネッティングが行われており、これにより、オペレーションコストの削減や決済資金所要額の削減による流動性の節約につながっている。

対象とする取引や商品の性質によっては、リアルタイムでグロス決済処理を行うのではなく、DLT にネッティング機能を持たせる等により、決済効率を確保する仕組みの構築が必要である。

ポイント 3：セーフティーネットの整備

金融市場における既存の大規模な決済インフラにおいては、円滑な決済の実現のために、フェイル慣行[22]や決済上の「すくみ」を防ぐセーフティーネットが用意されている。取引時に必要な証券及び資金があらかじめ口座にあるかを確認しない場合、これらのセーフティーネットを整備しておく必要がある。

フェイルへの対応については、DLT のみで技術的に解決することは困難であり、現行の証券決済で行っているのと同様に、清算機関のような中立的第三者を制度的に設け、フェイル解消までの間における、売方から買方への遅延損害金の支払いや、受渡対象証券の強制買付け（バイイン）等の処理を行うことにより、フェイル発生抑止及び早期解消を行うことが出来ると考えられる。また、DLT におけるフェイル慣行を市場参加者の間で合意することも対応のひとつである。

次に、決済上の「すくみ」を防ぐためのセーフティーネットとしては、①コンセンサスアルゴリズムの工夫、②第三者機関による流動性供給、の 2 つの方法が考えられる。

まず①について、実際の決済制度においては、「すくみ」を防ぐためのセーフティーネットが用意されている。例えば、日銀ネットにおいては、待ち行列機能[23]と複数指図同時決済機能[24]を設けている。我々の知る限り、主要な DLT のコンセンサスアルゴリズムでは、同一ブロックに含まれるトランザクションの処理順番については特段の制御をしていない。トランザクションの組み合わせを見ながら、決済効率が高まるよう、処理順序を適切に変更するようなコンセンサスアルゴリズムが開発されれば、決済上の「すくみ」を技術的に解決できる可能性がある。

次に②については、中央銀行における決済の場合、資金の受けと払いのタイミングのズレから生じる一時的な資金負担の軽減策として、中央銀行が流動性を供給する仕組みを用意している。このように、「すくみ」が生じる場合には、第三者機関が一時的に流動性を供給することにより、決済のファイナリティをつけ、事後的に「すくみ」が解消された際に決済資金を第三者機関に返すという形で対応することも考えられる。

[22] 当初の決済予定日が経過した時点で証券の受渡しが行われていなくても、そのことのみをもって債務不履行（デフォルト）とはせず（契約を解除せず）、これを容認する市場慣行。
[23] 資金不足のため直ちに決済できない場合、当該支払指図を日銀ネット内の待ち行列に待機させておく機能。
[24] 日銀ネットが受付けた支払指図や、日銀ネット内で待機している支払指図の中から、同時に決済すれば資金不足とならない組合せを探索し、当該決済を実行する機能。

V. まとめ

本稿では、DLT に係るこれまでの調査・分析等から得られた知見を踏まえ、金融市場インフラに対する DLT の適用に係る可能性及び技術的な制約等について検討した。その結果、DLT を金融市場インフラに活用した場合、いくつかの課題があるものの、新たなビジネスの創出、業務オペレーションの効率化、コストの削減等に寄与し、金融ビジネスの構造を大きく変革する可能性の高い技術であることが分かった。

短期的な課題

金融市場における DLT の活用に際して、技術的課題の中でとりわけ重要度が高いと考えられるのは、スマートコントラクトにおける非決定的要因の解決及び情報の秘匿性の実装である。

期日の到来をトリガーとしたイベント処理、外部フィードの取得及び乱数の発生といった非決定的要因を含む処理をスマートコントラクトで実行する場合、検証ノード間で実行結果の完全な一致が得られない事により、認証処理を妨げる可能性がある。いずれも証券取引においては一般的かつ頻繁に発生する処理であるため、DLT 上で取り込めるか否かが金融市場における普及にあたってのポイントとなる。

また、現在の証券取引等の実務を考慮すると、取引内容等のデータが全て公開されることが利用者に受け入れられるとは考えにくく、このため取引等の当事者以外に対する情報の秘匿性が重要になってくる。現状では DLT 自体で情報の秘匿性を実現できる規格が少ないため、今後、多くの規格において対応が進む事を期待する。

中長期的な課題

将来的に DLT が金融市場インフラのコア技術として採用される場合の課題も記しておきたい。

まず、大量の取引を安定して処理できるスループット性能が重要であるが、今回の実証実験において得られた結果からは、残念ながら現状ではまだ適用範囲を限定せざるを得ない水準である。スループット性能について、DLT 規格の開発元によるデモンストレーション等では高い水準が示される場合もあるが、それらはユースケースやノードの地理的な分散状況等、測定に際しての前提が必ずしも明確ではない。金融市場インフラとして必要な要件を考慮した上で、更なる技術改善を期待する。

また、ビットコインはリアルタイム決済を前提とした仕組みであると考えられるが、ネッティング、キュー管理及び流動性供給といった、既存の金融市場インフラが備えている機能を DLT 上で検証した例はほとんど公表されていない。利用者の利便性、決済安定性の確保及び DLT の特性などを念頭に置いた上で、清算機関の活用を含め、適切な方式が DLT 上で実現できる必要がある。さらに、本格的な適用においては DVP 処理の実現は必須であるが、より安全に大量処理を行うためには、資金決済のファイナリティが DLT 上で実現できることが望ましい。

金融ビジネス変革の可能性

実証実験を通じて幾つかの制約や注意事項は発見されたものの、DLT をインフラ技術として見た場合、可用性の高さ、改ざん不可能、障害時のデータ復元が容易、相対的に低コストといった点は極めて魅力的である。また、こうした技術的な特性に加えて、DLT の導入を契機としてビジネスプロセスの見直しを行うことにより、金融サービスの革新や業界全体として大幅なコストの削減

が実現する可能性がある。

例えば、過去データの断面取得が容易という特性を活かし、証券の保有者名簿をリアルタイムで作成することが可能になる。議決権行使や配当金処理も含めた株主管理プロセスが効率化すれば、発行企業にとって大きなメリットになるとともに、例えば証券取引において売買単位ではなく金額単位指定で取引する事も可能となる。もちろん法律を含めた実務面での課題は多いが、金融サービスデザインの自由度が向上する事により、市場利用者に利便性をもたらすイノベーションが起こしやすくなる。また、複数の主体間で行われる取引内容の照合、データの共有・参照といったプロセスを DLT 上に実装する中で業務の自動化・効率化が進めば、大きなコスト削減が得られる可能性がある。さらに、暗号化技術等による秘匿性の確保が大前提ではあるが、システム障害発生時やデータロスト時に他の金融機関が保有するノードからデータをリカバリーする事も可能であり、相互依存型の BCP の実現によりシステムの冗長化コストを削減するといった効果も考えられる。

DLT は、ある利用者グループ間でインフラを共用するのに有効な技術である。分散されたノードの一つ一つが維持・運営に与える影響力を等しくしたままでインフラを共有する事ができるため、業界共通基盤として使いやすい。中央集権的な存在を設置する場合でも、主にインフラの調整者や安全弁としての役割に重点を置く事になるため、民主的なインフラ共有が可能となる。

今回の実証実験では金融機関に限定したインフラ共有を想定したが、上場会社や投資家まで範囲を広げる事で、より効率化の範囲を広げる事が出来る。また、各国のインフラを繋げる事で国際的なインフラ共有にも繋がる可能性がある。近年のシェアリングエコノミーというトレンドの中で、DLT はインフラシェアの可能性を大きく広げる技術という事ができる。

最後に、今回の検証にあたって、テクノロジーの利用者の立場から注意した点について述べたい。

まず、DLT はいくつかの技術要素が相互に関係しており、その上に構築する具体的なビジネスによって、それらの技術要素の最適な構成は異なる。ビットコインは仮想通貨というユースケースにおいて非常にバランスの取れた技術要素の組み合わせを実現しているが、DLT を金融市場インフラに適用する場合には、本稿が述べた様々な要件等を踏まえ、新たな最適バランスの模索が必要であると考えられる。また、今回の実証実験では「コンソーシアム型」の DLT 規格を採用したが、秘匿性が求められないデータだけを取り扱うのであれば「パブリック型」の利用が相応しい場合もある。どちらが優れているかという優劣の議論になりがちだが、ユースケースに応じて適切な規格を採用することが望ましい。こうした最適バランスの探索はまだ始まったばかりであり、机上検証のみで達成し得るものではない。世界中で行われる実証実験等を通じて、こうしたチューニングが加速していくと考える。金融市場インフラの運営者としての知見を活かしながら、今後も最適なバランスの探索を継続していきたい。

また、DLT の適用によるイノベーションは、その技術的特性を可能な限り活かしつつ、既存の業務プロセスを見直すことで初めて得られるものと考える。金融市場インフラにおける DLT の適用においては、既存の業務プロセスに精通した主体を中心に検討が進むと思われるが、既存プロセスに拘りすぎて DLT の利点を損なうことがないよう注意が必要である。

2009 年から現在に至るまで実際に運用されているビットコインと異なり、金融市場インフラに対して DLT を適用した実績は現時点では乏しく、DLT が金融市場インフラの基盤技術として成熟するためには、今後も多くの実験と改善を繰り返す必要がある。本稿を通じて、DLT の金融市場インフラ適用に向けたオープンイノベーションが促進されれば幸いである。