証券市場からみたDLT活用可能性の検証

2018年2月7日

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

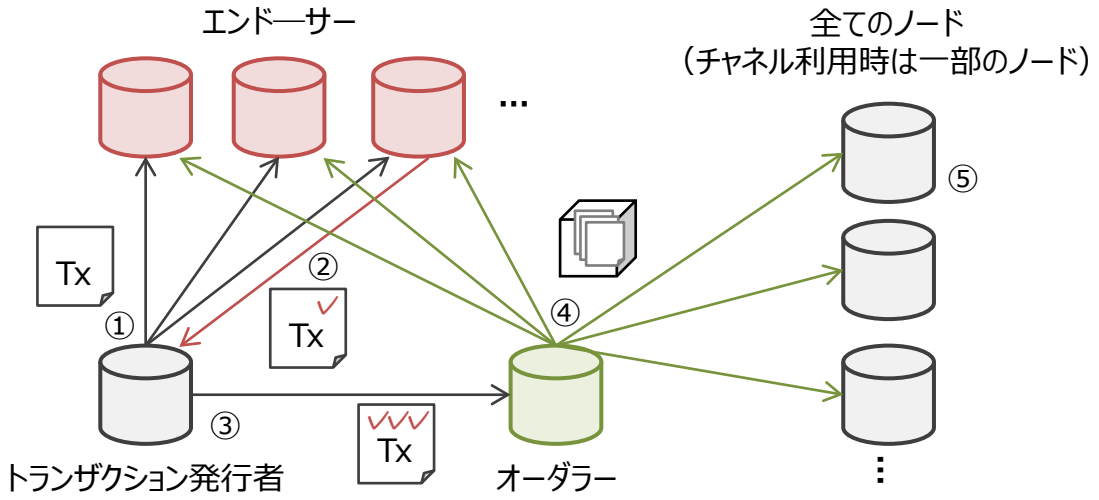
これまでの取組み

	2015	2016	2017
実証実験	内部調査/机上検証	Hyperledger Fabric V0.6 with IBM Ethereum系 with NRI/Currencyport	Hyperledger Fabric V1.0 with IBM
ワーキングペーパー			
コンソーシアム		**6** 金融機関	**36** 金融機関 (+金融庁，日本銀行，証券業協会)
業界プロジェクト			**2** プロジェクト提案 (大和証券、SBI/NEC)

個別技術の特徴①：Hyperledger Fabric

- 昨年7月にver1.0正式リリース (従来版(～ver.0.6)と比較して仕様が大きく変更)
- エンドースメントポリシーとチャネル機能により、合意形成ルール及び情報の秘匿性を柔軟に設定することが可能

【参考】Hyperledger Fabric ver.1.0におけるトランザクションの処理フロー



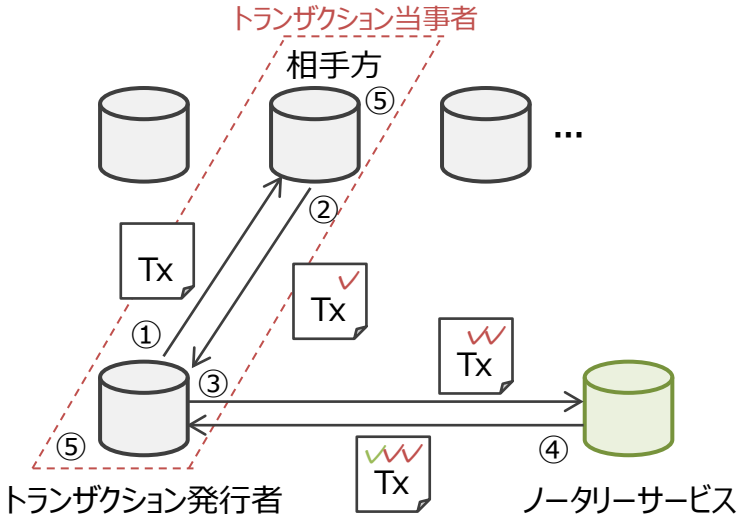
□エンドーサー (Endorser)
トランザクションを実行し、署名を付して実行結果と共にトランザクションの発行者に返す役割のノード
□オーダラー (Orderer)
トランザクションを1つないし複数まとめて順序を決め、ブロックとしてネットワーク全体にブロードキャストする役割のノード
□エンドースメントポリシー (Endorsement Policy)
どのノードがエンドーサーとなるか、トランザクションが承認されるために何台のエンドーサーからの署名が必要か、などについての設定
□チャネル (Channel)
ネットワーク上で台帳を共有するノードの範囲についての設定

① トランザクション発行者はトランザクションをEndorserに送信する
② Endorser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Endorsement Policy(EP)で定める必要な数のEndorserからの署名を集めた後、Ordererにトランザクションと集めた署名を送信する
④ Orderer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EP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

個別技術の特徴②：Corda

- 昨年10月にver1.0が正式リリース
- データモデルとしてUTXOを採用(ビットコインと同様)、当事者間でしかデータを共有しない
- 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

【参考】Cordaにおけるトランザクションの処理フロー



UTXO(Unspent Transaction Output)のイメージ

トランザクション

インプット	処理内容	アウトプット
口座A 100円 ※実際には、過去のトランザクションを指定	口座Aから口座Bに10円を入金	口座B 10円 口座A 90円

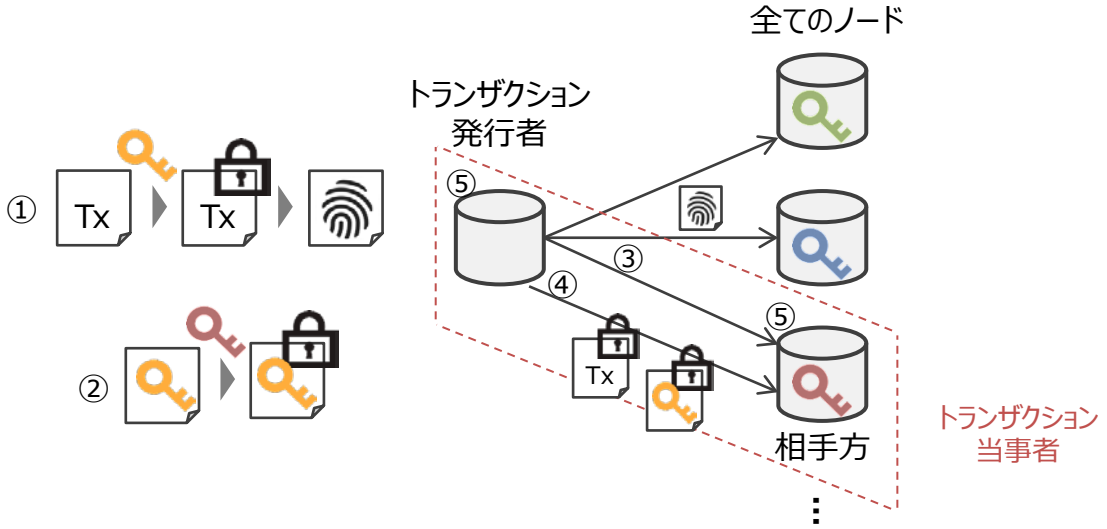
新たに発行するトランザクションにおいて、処理内容で対象となるデータをアウトプットに有する過去のトランザクションをインプットとして指定する

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、実行して結果を台帳に格納する

個別技術の特徴③：Quorum

- JPモルガンが当初開発して一昨年10月にオープンソース化した、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
- 昨年3月に発足したEnterprise Ethereum Allianceにおいて参照規格とされている
- 特殊な権限のノードをネットワーク上に一切持たずにデータの秘匿性を実現している

【参考】Quorumにおけるプライベートトランザクションの処理フロー



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

比較まとめ

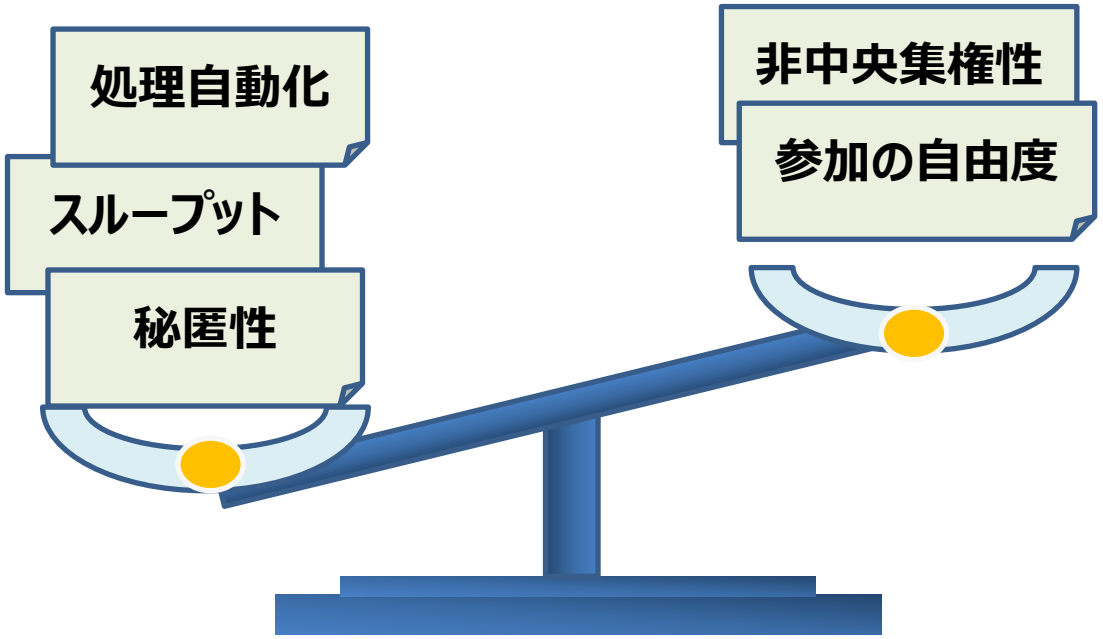
- 主要なコンソーシアム型DLTは、金融業界の要望を取り込みながら、ブロックチェーンの当初のコンセプトからは異なる方向性へと変容

	【参考】ビットコイン	Hyperledger Fabric	Corda	Quorum
情報の秘匿性	なし	チャネル機能	当事者間のみで情報共有	プライベートトランザクション、ゼロ知識証明
単一障害点	なし	オーダラー	ノータリーサービス	なし
ビザンチン障害耐性	あり	なし	- ネットワーク全体で共有する情報がない	なし※
スループット	低	データベースの設定次第では 高	- JPXグループではテスト未実施	- JPXグループではテスト未実施

※ ビザンチン障害体制のあるコンセンサスアルゴリズムの導入を検討中

正しい変化の方向性なのか？

- ブロックチェーン/DLTは複数の技術要素の組み合わせであり、利用者が最も成し遂げたい便益に応じて、バランスが変化する事は自然
- 現時点では、技術の利用者としての金融機関は、「情報共有の効率化」と「処理の自動化」に魅力を感じており、結果としてブロックチェーンの当初コンセプトから乖離



仮想通貨とは異なるアプローチで金融の効率化を実現しようとする挑戦

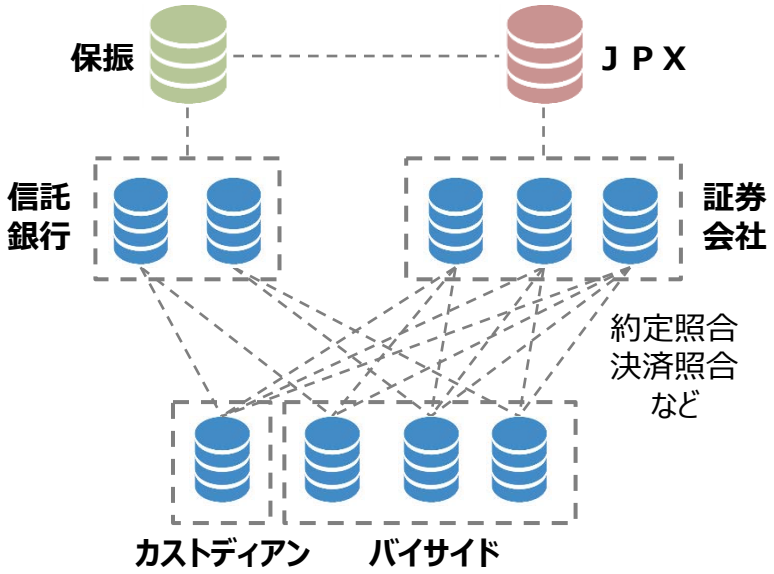
スループット向上へのチャレンジ

- 合意形成プロセスを分解して並列処理可能な部分を増やす
- 重たい処理のオフチェーン化、オフチェーン処理との組み合わせ
- 情報配布・確認範囲の限定（秘匿性向上の副産物？）
- そもそも何を並列処理してもいいのか？
  - 同一IDの同一資産は二重使用を防ぐ、かつ、逐次ファイナリティの確保
    ⇒ ここは並列処理できない
  - 異なる資産なら（たぶん）並列処理可能
    ⇒ でも、DVP, PVP, 組み合わせ取引どうする？
    ⇒ スループット性能のカタログスペックの魔法

どんなユースケースが議論になっているのか？

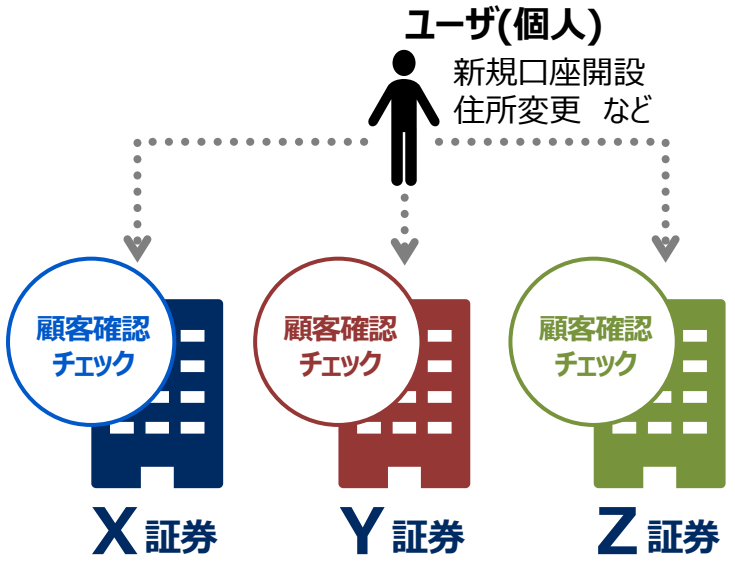
業界連携型実証実験に提案されているプロジェクト

パターン①：ポストトレード照合



・金融機関サイドは多対多の構造
⇒確認のため何重もの”照合”が必要
※クロスボーダーの場合はより複雑

パターン②：顧客確認(KYC/AML)

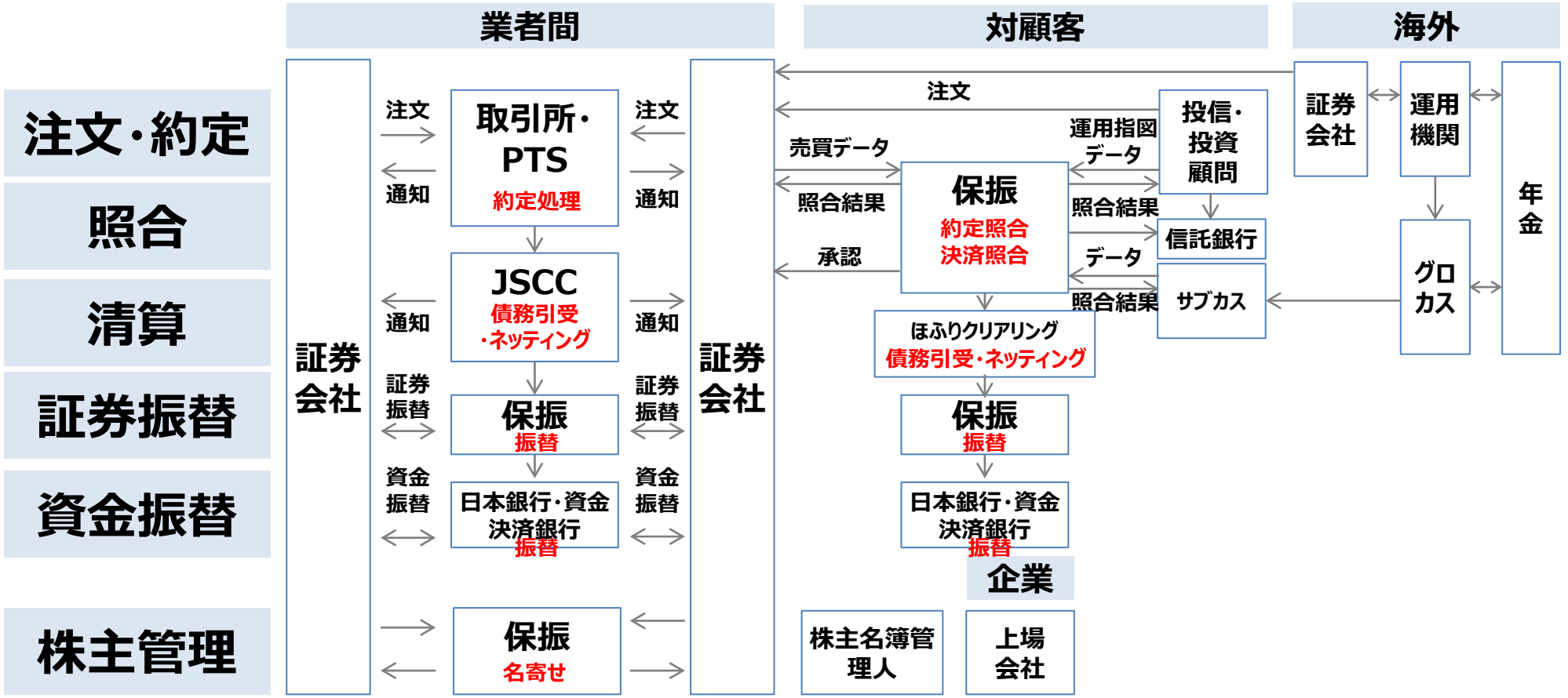


・業者間でのデータ共有の枠組みがない
⇒ユーザにとって大きな手間

情報(データベース)の分散・分断　＆　複雑なオペレーション

（参考）株式の処理プロセス

- 業者間、対顧客（国内、海外）で、多くの主体が関わっている事により、主体間での無数の照合処理が発生しており、多くの非効率性が存在。
- 非効率性の原因の一つは、「複数の競合する法人間」で「単一の合意形成」を「システム的に効率的で安全性の高い方法」で実現するのが難しいため



10

分散台帳技術でないと実現できないのか？

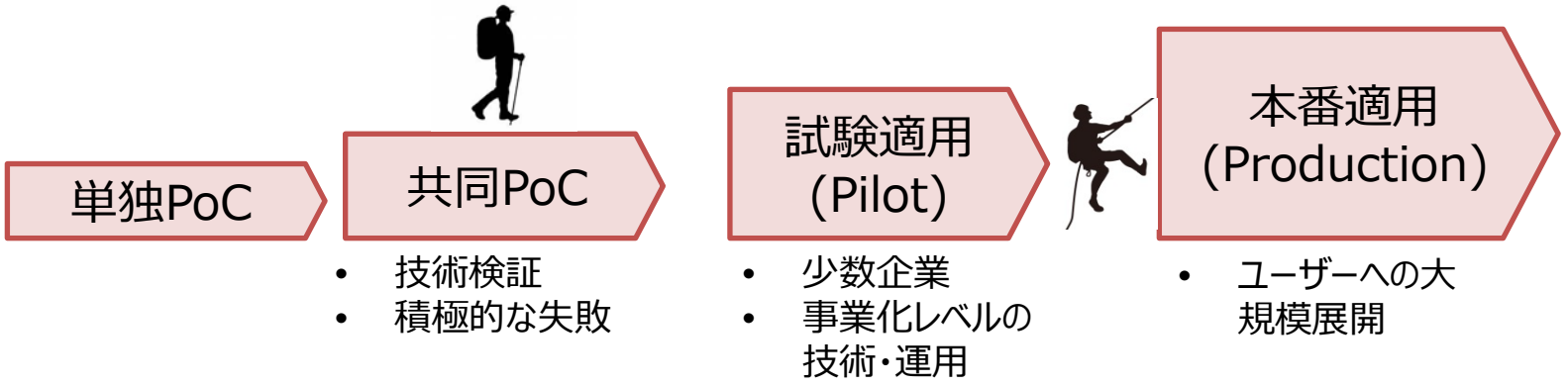
- 分散台帳技術は魔法の杖ではなく、既存技術で実現できる事も多い
- 一方で、既存技術だけで、十分に情報共有の効率化や処理の自動化が達成できてきたとは言い難い（なぜか？）

- 業界全体で新たな金融サービスのデザインにチャレンジできるのは新規技術の特権

- **分散台帳技術(DLT)のユーザー視点での特徴**
  - **サービスの集合体としてのパッケージシステムである**
    - スマートコントラクト（アプリ）、合意形成のための通信プロトコル、データベース等
  - **単独企業ではなく複数企業で基盤共有が可能**
    - Decentralized
      ⇒ 圧倒的強者を作らない技術　…　ビジネス競合による‘すくみ’の解消
  - **複数企業をまたがる処理自動化と単純化が可能**
    - 単純なコスト効率だけでなく、新規商品/サービスのデザインが容易に

本当にできるのか？

- DLTが業界全体として十分大きな課題を解決する可能性があったとしても、実ビジネスで適用するために超えなくてはいけない壁は大きい

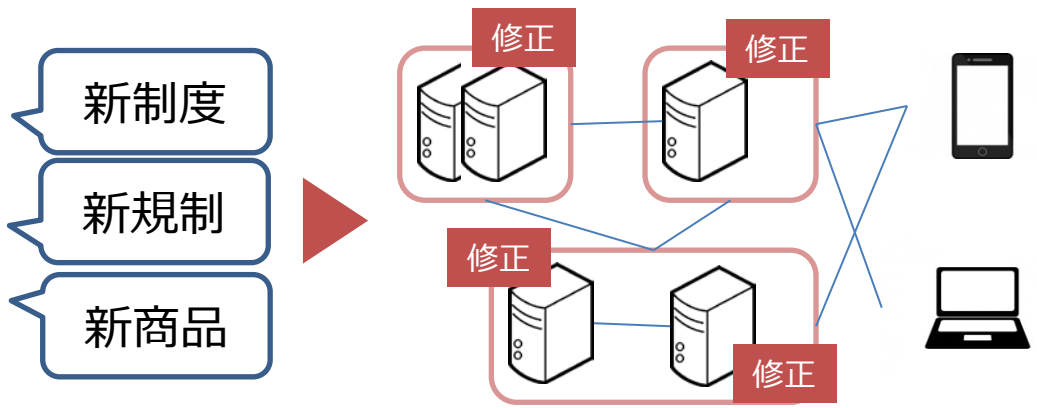


- とても参考になる検証
  - 技術課題の検証
    - Project Stella報告書(2017/9, 日本銀行, ECB)
    - Project Ubin Phase2 報告書(2017/10, MAS)
  - 法的課題の検証
    - 「証券取引における分散台帳j技術の利用を巡る法律問題研究所」報告書, 日本銀行金融研究所
  - 現実的な実装方法の提案
    - 約定照合業務におけるブロックチェーン(DLT)適用検討ワーキングペーパー, 大和証券グループ　プロジェクトチーム

‘効率化‘の本質

自社を効率化すればコストが下がる
業界全体を‘効率化‘すれば世界が変わる

- 企業経営者の目線では、効率化＝自社事業のコスト削減
- しかし、DLTによる効率化が目指すのは、より高い視点での業界(業種)横断的な効率化
- スマートコントラクトによる処理の自動化や情報共有の効率化は、新商品・新制度・新規制導入への摩擦をゼロに近づける試み
- 管理コストの摩擦をゼロに近づける事ができれば、サービス/トランザクションの極小化も可能になり、世界が変わる



- 現在は軽微な修正であっても、複数企業の複数システムに修正が必要で、時間もコストもかかる
- 管理コストの問題でサービス/トランザクションサイズの引き下げは限界がある

【本資料に関する注意事項】

- 本資料は情報提供のみを目的としたものであり、投資勧誘や特定の証券会社との取引を推奨することを目的として作成されたものではありません。
- 万一、本資料に基づき被った損害があった場合にも、（株）日本取引所グループは責任を負いかねます。
- 本資料で提供している情報は万全を期していますが、その情報の完全性を保証しているものではありません。
- 本資料に記載されている内容は将来予告なしに内容が変更される可能性があります。内容等について、過去の情報は実績であり、将来の成果を予想するものではありません。
- 本資料のいかなる部分も一切の権利は（株）日本取引所グループに属しており、電子的または機械的な方法を問わず、いかなる目的であれ無断で複製、または転送等はできません。
- 資料には、講演者の個人的意見も含まれておりますので、全てが（株）日本取引所グループの公式見解ではありません。

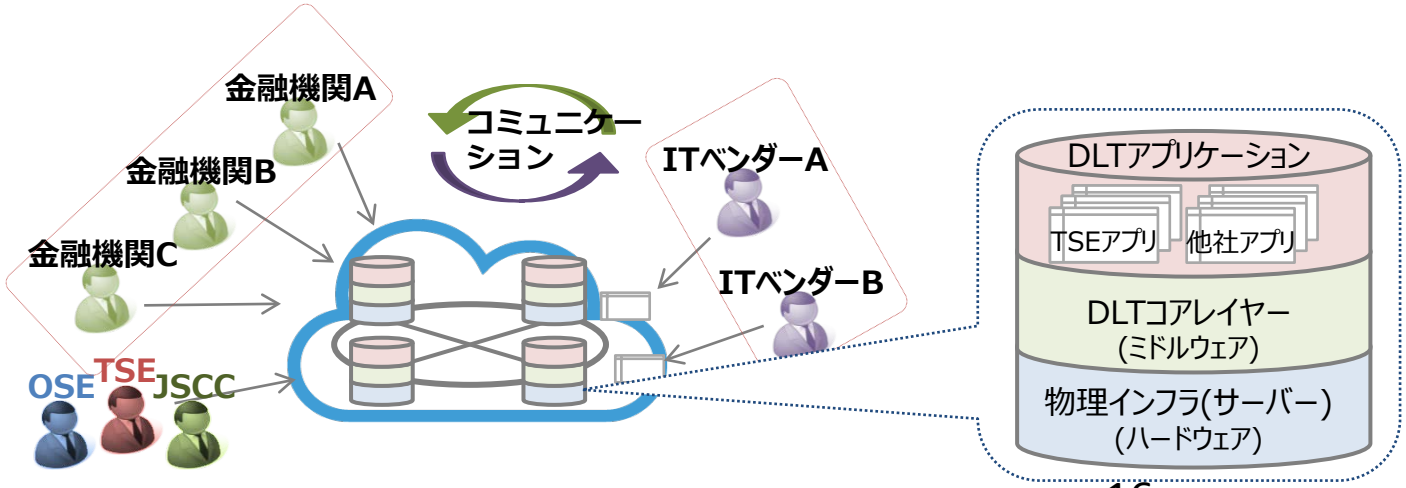
参考

業界連携型実証実験やってます

- 新規技術の探求は、関心があったとしても、人も予算も必要で、単独社で進めるには相当なパワーが必要
- 少しずつ負担をシェアし合えば、もっと効率的に進められるはず
- ブロックチェーン/DLTは、分散ネットワーク上で動くという技術的特性もあり、連携しないと期待される効率化の効果も小さくなる

⇒ 業界連携型の実証実験を開始。
⇒ TSE提供アプリ on Hyperledger fabric V1.0
⇒ 金融機関・ベンダーから2件のプロジェクトが提案され進行中
⇒ JPX Working paper　2本、デモアプリの動画がHPにて公開中

http://www.jpx.co.jp/corporate/research-study/dlt/index.html



16