エンタープライズ領域のブロックチェーン活用における
インターオペラビリティ実現のための取組みご紹介

2023.5

みずほリサーチ&テクノロジーズ

技術開発本部
先端技術研究部

坂本　健太郎

自己紹介

みずほリサーチ&テクノロジーズ株式会社
技術開発本部
先端技術研究部

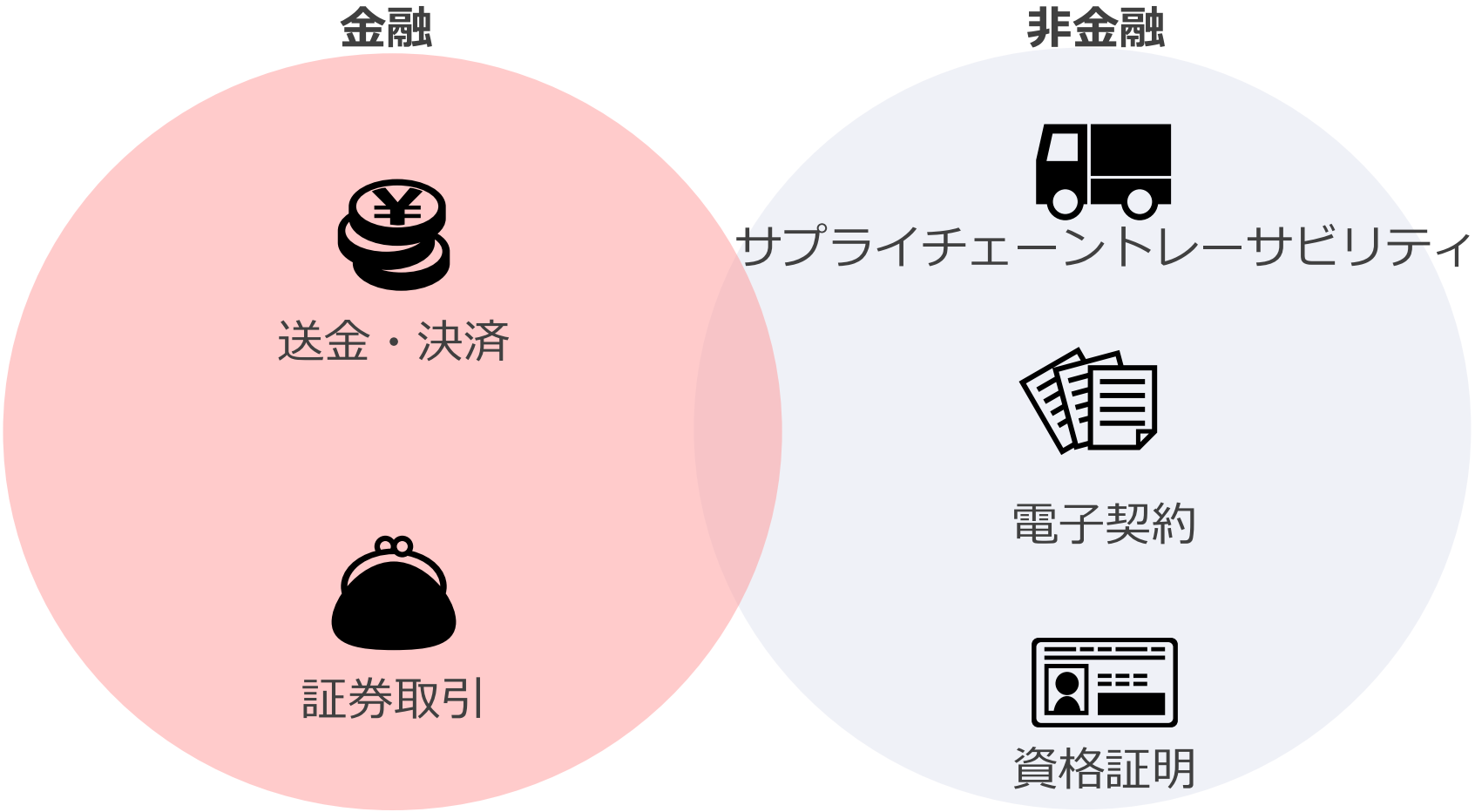
坂本　健太郎

2017年よりブロックチェーンを用いた金融・非金融領域での実証実験、案件立上げ等に参画し、並行してブロックチェーン技術に関する調査・研究や人材育成に従事。

ブロックチェーン技術の活用動向①

- ブロックチェーンは特定の組織等に依存せずに取引やデータ保管が可能になる仕組み。
- 様々なユースケースでの活用が世界中で進行。

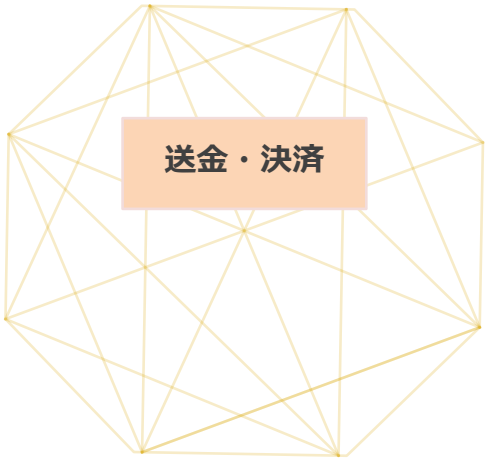
ユースケース例



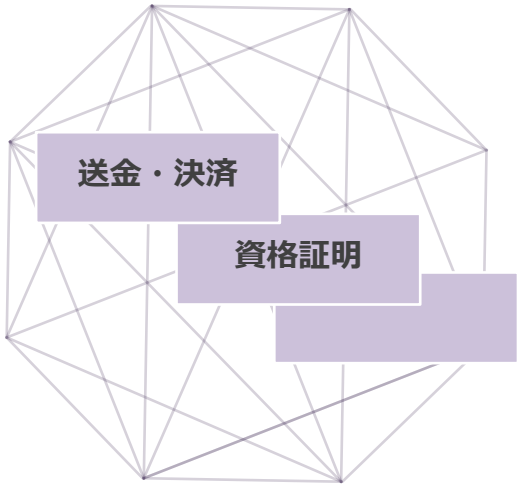
ブロックチェーン技術の活用動向②

■ ブロックチェーン上の各サービスは主に個別のネットワーク内で展開されている状況。

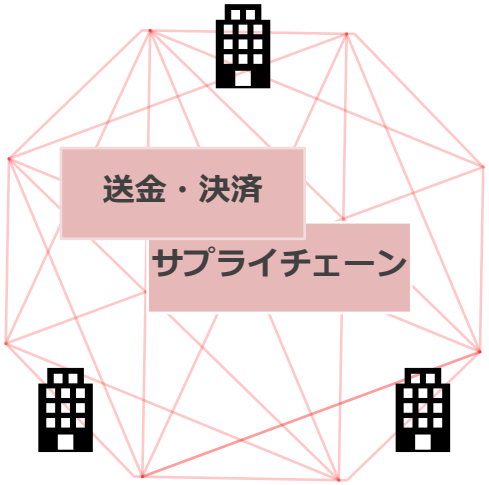
Bitcoin

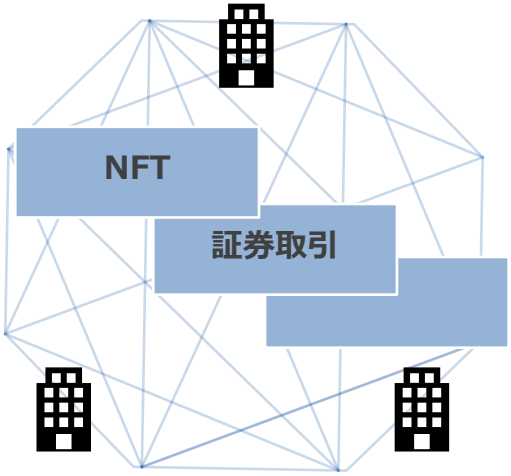


Ethereum等



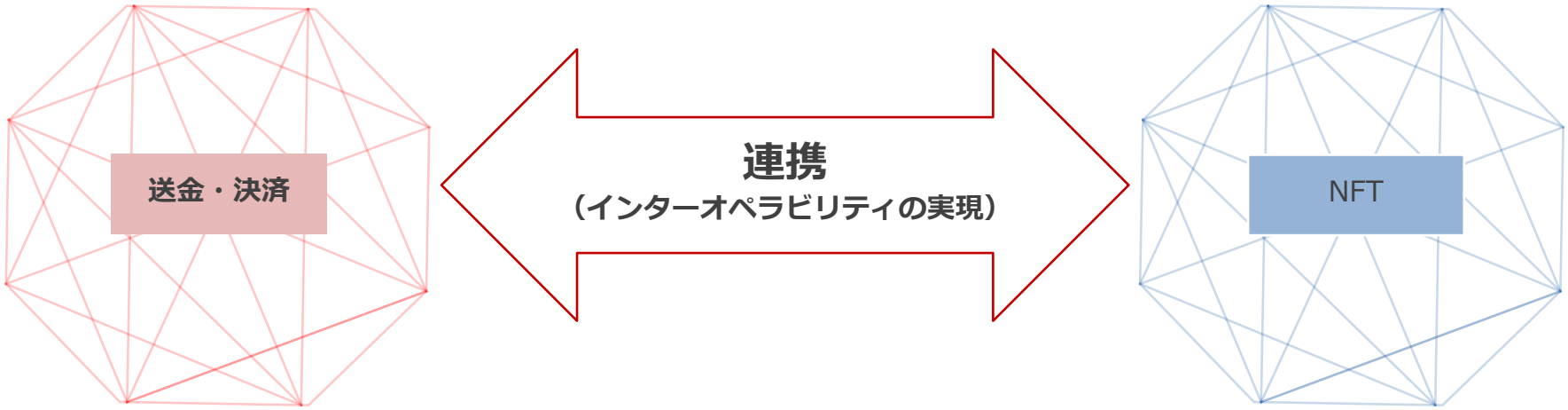
限られたメンバー組織・企業で運営される許可型のブロックチェーン





ブロックチェーン技術の活用動向③

- **異なるブロックチェーン間のインターオペラビリティを実現し高度なサービスを提供すること**の重要性の高まり。
- 既にブロックチェーン間連携のための様々な方法が提唱され稼働も始まっており、今後更なる進展が想定される。



みずほにおけるブロックチェーンの取組み①

■ みずほフィナンシャルグループ各社では2016年頃から金融・非金融の様々なユースケースで実証実験等の取組みを実施。

取組み事例一覧（抜粋）

年	取組み概要	参考URL
2023	「デジタルエンゲージメントプラットフォーム」 の取り扱い開始	https://www.mizuho-rt.co.jp/company/release/2023/r02-d-engage.html
2022	セキュリティトークンに係る実証実験	https://www.mizuho-rt.co.jp/company/release/2022/blockchain0729.html
2021	サプライチェーンファイナンス展開	https://www.mizuhobank.co.jp/release/pdf/20210916release_jp.pdf
2020	サプライチェーンファイナンスや個人向けデジタル社債に係る実証実験	https://www.mizuho-rt.co.jp/company/release/2020/supplychain1228.html https://www.mizuho-rt.co.jp/company/release/2020/sto0221.html
2019	スキル・職歴の管理に係る実証実験(DID)、 MaaSに係る検証	https://www.mizuho-rt.co.jp/topics/2019/pasonapoc0218.html https://news.microsoft.com/ja-jp/2019/07/08/190708-the-theme-in-maas-to-verify-the-usefulness-of-blockchain
2018	サプライチェーン・個品管理プラットフォーム実証実験	https://www.mizuho-rt.co.jp/company/release/2018/lowson0926.html
2017	貿易金融、契約管理、独自通貨等のユースケースに係る 計6件の実証実験	https://www.mizuho-fg.co.jp/release/20170921release_jp.html https://www.mizuho-fg.co.jp/release/20170707_2release_jp.html https://www.mizuho-fg.co.jp/release/20170601release_jp.html https://www.mizuho-fg.co.jp/release/20170426release_jp.html https://www.mizuho-fg.co.jp/release/20170426_2release_jp.html https://www.mizuho-fg.co.jp/release/20170223release_jp.html
2016	国際送金、決済、シンジケートローン、文書記録・管理等の ユースケースに係る計4件の実証実験	https://www.mizuho-fg.co.jp/release/20160719release_jp.html https://www.mizuho-fg.co.jp/release/20160622release_jp.html https://www.mizuho-fg.co.jp/release/20160216release_jp.html https://www.mizuho-fg.co.jp/release/20160216_2release_jp.html

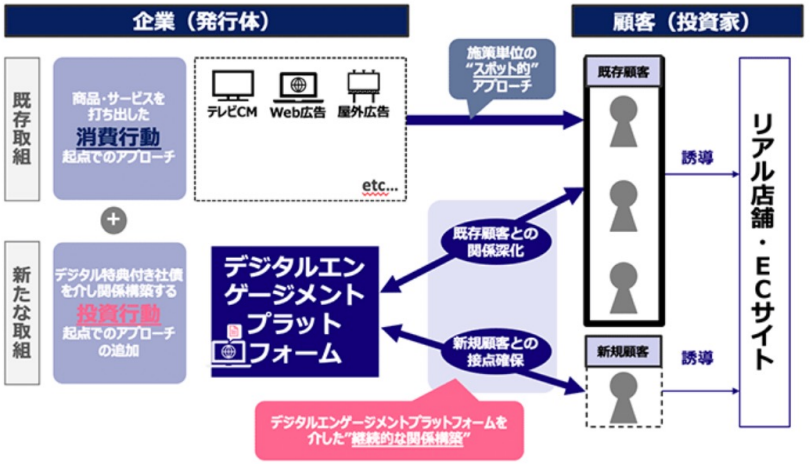
みずほにおけるブロックチェーンの取組み②

事例

■ 社債などの発行体が投資家と直接接点を持つことを可能にするシステム基盤「デジタルエンゲージメントプラットフォーム」の取扱いを2023年2月に開始

ブロックチェーン技術を活用した「デジタルエンゲージメントプラットフォーム」 の取り扱い開始について

2023年2月16日
株式会社みずほフィナンシャルグループ
株式会社みずほ銀行
みずほリサーチ&テクノロジーズ株式会社



株式会社みずほフィナンシャルグループ（執行役社長：木原 正裕）、株式会社みずほ銀行（取締役頭取：加藤 勝彦）、およびみずほリサーチ&テクノロジーズ株式会社（取締役社長：吉原 昌利）は、このたび、ブロックチェーン技術を活用し、発行体が投資家と直接接点を持つことを可能にするシステム基盤「デジタルエンゲージメントプラットフォーム」（以下、「本プラットフォーム」）の取り扱いを開始しました。

https://www.mizuho-rt.co.jp/company/release/2023/r02-d-engage.html

ブロックチェーンインターオペラビリティへの取組み

- 金融・非金融の様々なユースケースでブロックチェーンへの取組みを行うなかで「異なるブロックチェーン間のインターオペラビリティを実現し高度なサービスを提供すること」の重要性を認識。
- 株式会社Datachain様、SBI R3 Japan株式会社様と連携し2022年度にクロスチェーン技術に関する取り組みを実施。

MIZUHO
みずほリサーチ&テクノロジーズ

Datachain

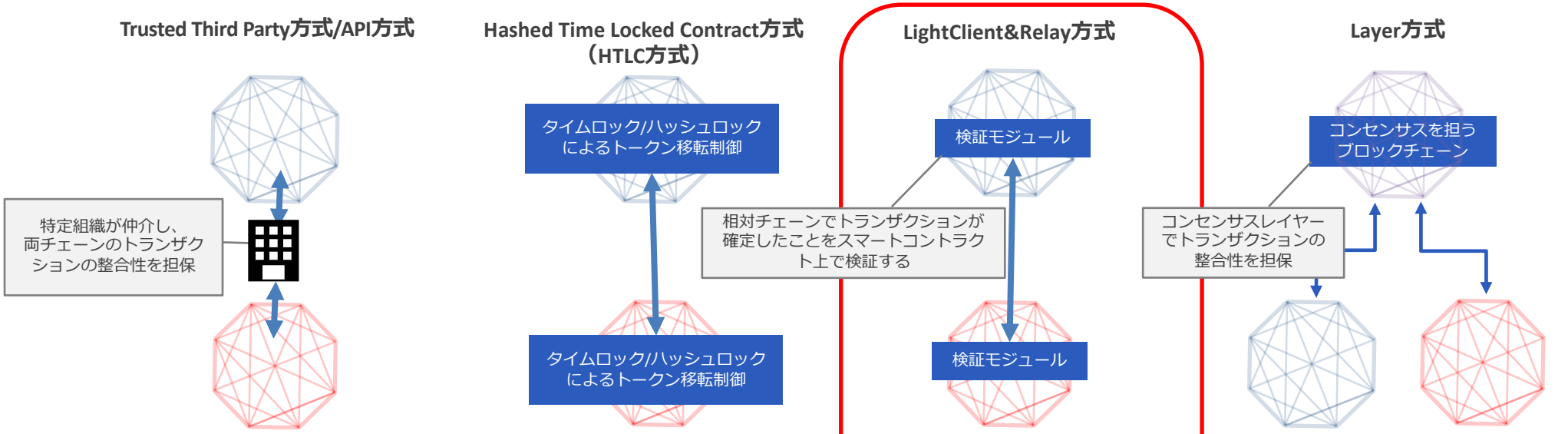
SBI R3 Japan

取組み概要

- 主要エンタープライズブロックチェーン基盤（以下、BC基盤）間のインターオペラビリティを念頭に、特にGoQuorum、Corda間のインターオペラビリティについて金融・非金融の想定ユースケースを設定し、機能・非機能要件の実現方法を検討。
- 機能・非機能要件は各開発プロジェクトにより水準が異なるものの、本取組みによって得られた一般的なプラクティスを2023年6月に公開予定。

取組み対象のインターオペラビリティ実現方式

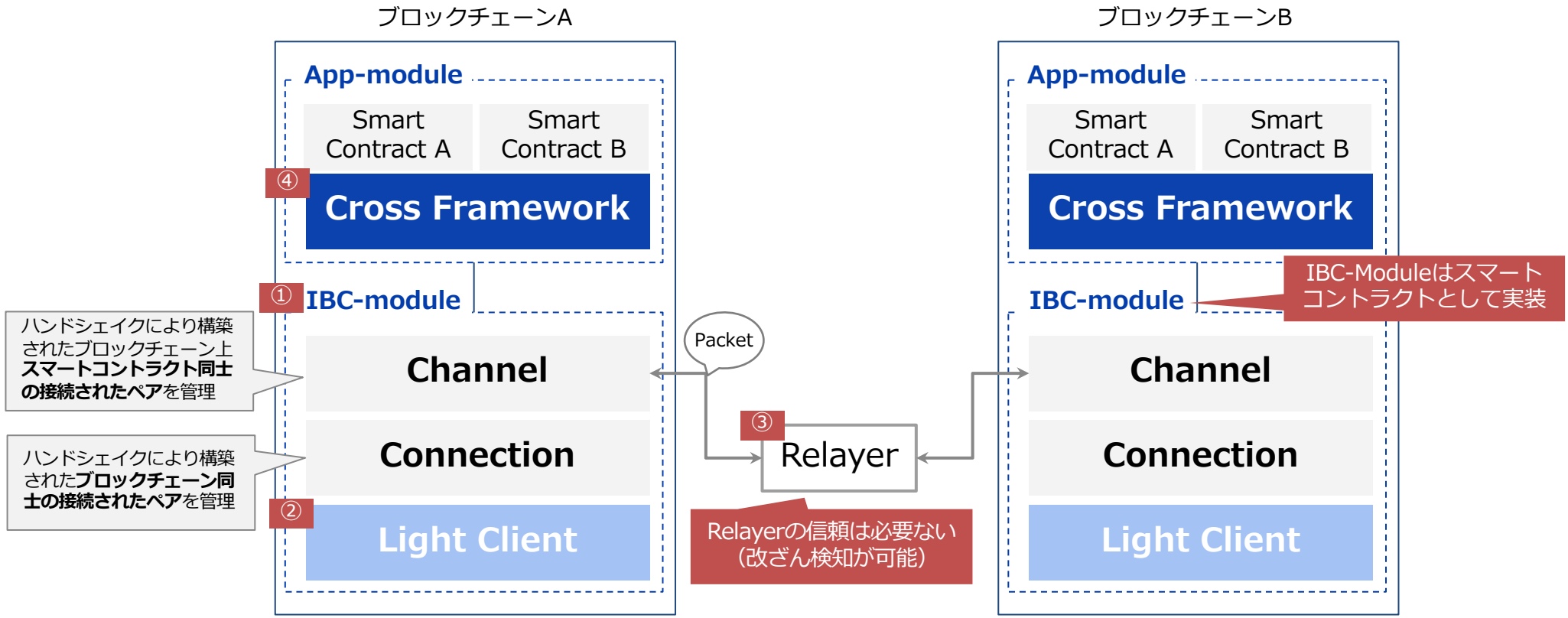
- 複数のインターオペラビリティ実現方式のうち、**特定の組織等に依存せずに取引やデータ保管が可能になるブロックチェーンの特性を損なわないRelay方式**を取組み対象に選定。
- Relay方式を採用する技術のうち、Cosmosプロジェクトにて活用が進んでいるIBC Module(Inter Blockchain Communication Module)をベースとし**エンタープライズBC基盤にも対応**しているHyperledger YUIを本取組みで対象とする実現方式に選定。



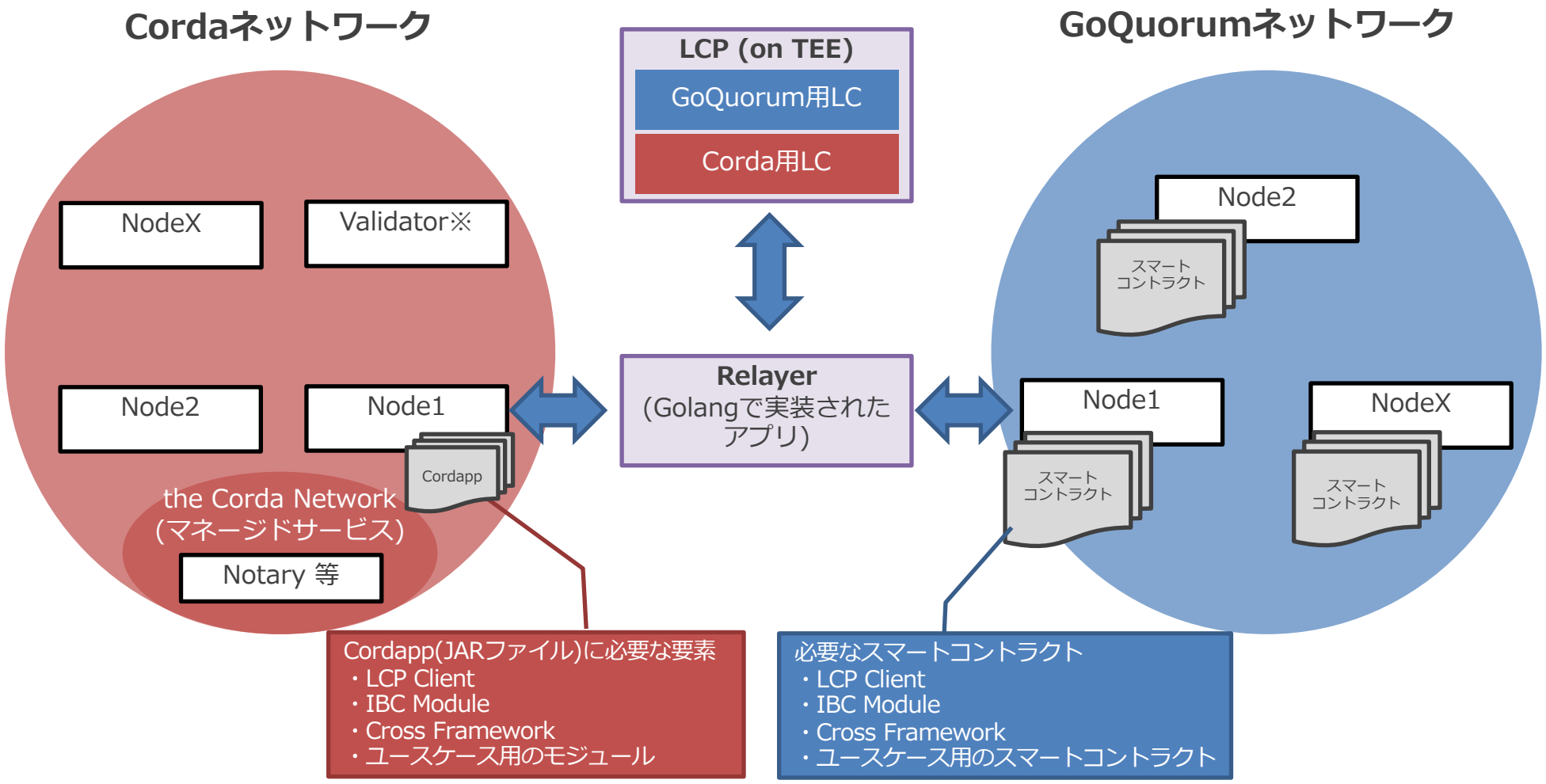
	Trusted Third Party方式/API方式	Hashed Time Locked Contract方式（HTLC方式）	LightClient&Relay方式	Layer方式
メリット	• 実現が容易	• 特定組織等への信頼が不要	• 特定組織等への信頼が不要 • 汎用性が高い	• 特定組織等への信頼が不要 • 汎用性が高い
デメリット	• 特定組織等への信頼が必要 • 信頼維持のために、システム/組織ガバナンスのコストが想定される	• ユースケースが限定的（例：トークン移転のユースケース）	• 技術的に発展途上・実装難易度が高い	• 特定組織等に依存しないようにコンセンサスチェーンを管理する工夫が必要 • コンセンサスレイヤーのチェーン停止が全チェーンに波及するリスクが想定される • コンセンサスレイヤーのチェーンに接続するためにコストが掛かるケースあり

Hyperledger YUIによるRelay方式のインターオペラビリティの特徴

- IBC Module(下図①)をベースとしたプロジェクト。
- 相手方のチェーンを検証するためのLight Client (LC、下図②)を両チェーンのIBC Moduleで持ち合うことで、通信仲介役となるRelayer(下図③)を通じて信頼できる第三者を設置せずにトランザクションを実行可能。
- 各チェーン上のスマートコントラクトからクロスチェーントランザクションを容易に実行するためのフレームワーク（Cross Framework、下図④）がYUI関連のOSSとして別途公開されている。



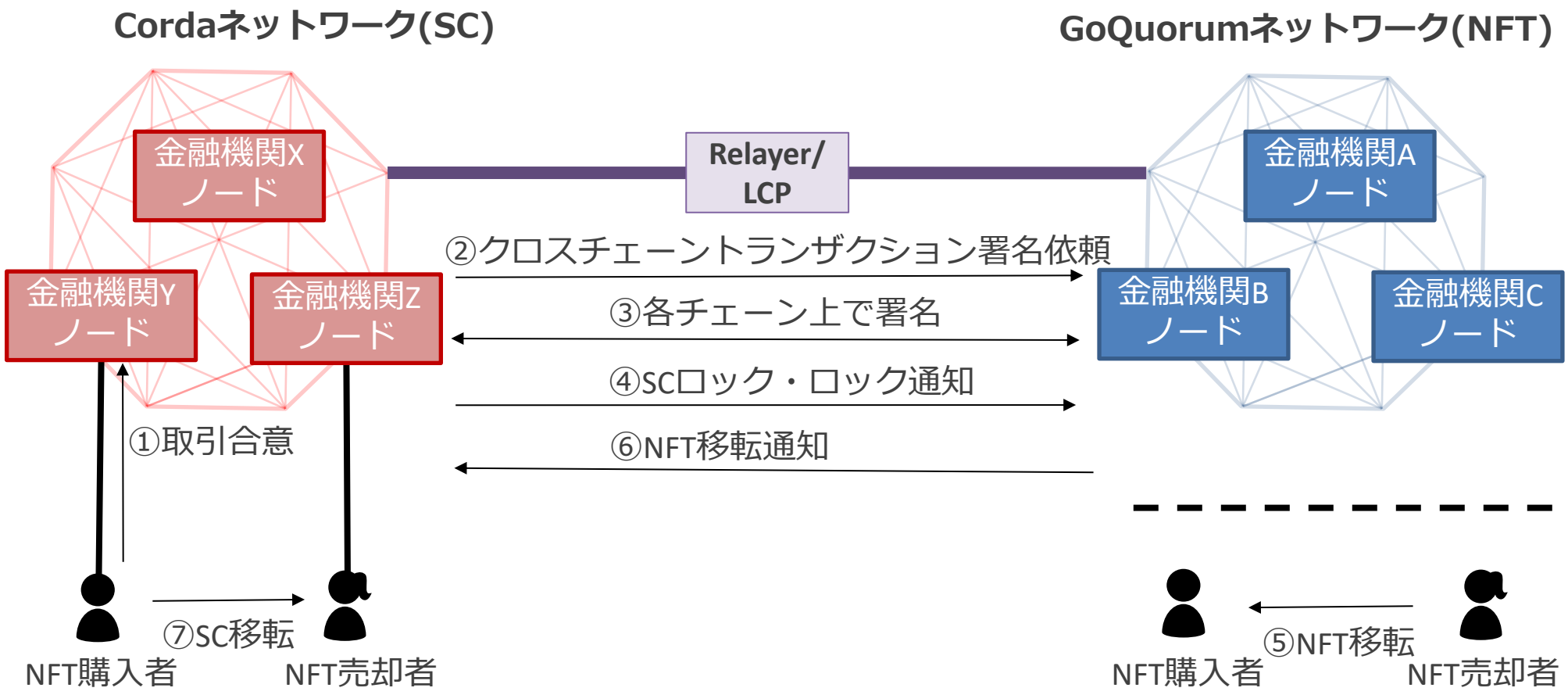
想定アーキテクチャ



※このValidatorは、クロスチェーントランザクション実行時のCorda側トランザクションの正当性を強化するために、
取引当事者ノードとは別に設置される第三者のノードを指す。（取引当事者ノード間のトランザクションに対して第三者として署名を行う）

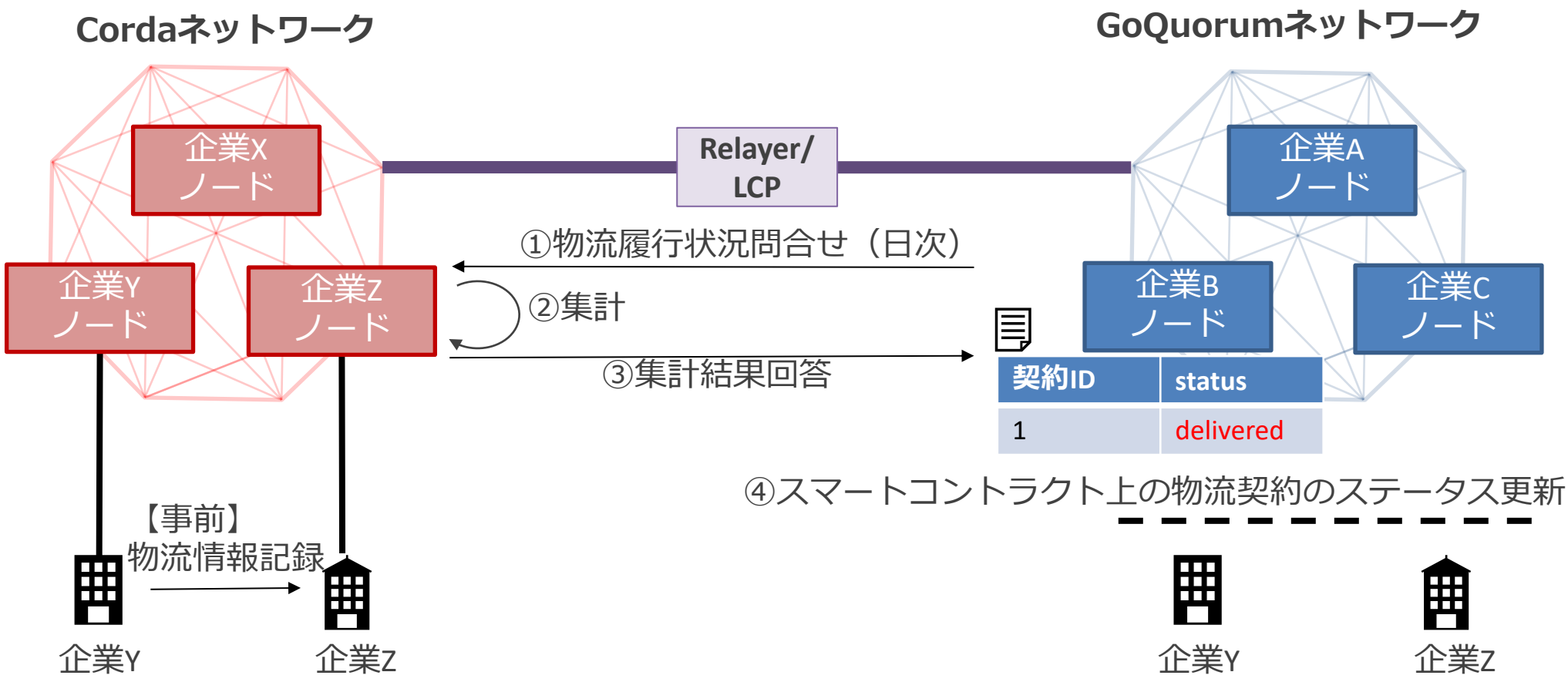
想定ユースケース①（金融）

- Corda上で発行・管理されているステーブルコイン(SC)とGoQuorum上で発行・管理されているERC721準拠のトークン（NFT）を用いたDVP決済を行う。



想定ユースケース②（非金融）

- Corda上で管理されている物流情報を参照して、GoQuorum上で管理されている契約情報を日次で更新する。



機能・非機能要件を実現するプラクティスのご紹介

- 想定ユースケースで設定されうる機能要件や非機能要求グレードに基づく一般的な非機能要件のうち、**クロスチェーントランザクションにおいて特別な考慮が必要と考えられる以下機能・非機能要件**について重点的に検討。
- 本日は得られたプラクティスの一部(赤枠)を抜粋してご紹介。（全量は2023年6月公開予定の資料ご参照）

機能要件	両ブロックチェーンでのアトミックな更新（想定ユースケース①）
	他方ブロックチェーンへの参照（集計）を伴う更新（想定ユースケース②）
	プライバシー
	アイデンティティ指定
非機能要件	可用性（耐障害性）
	可用性（回復性）
	性能
	運用・保守性(監視・異常検知時対応)
	運用・保守性(リリース運用)
	セキュリティ

機能・非機能要件を実現するプラクティスのご紹介

- 想定ユースケースで設定されうる機能要件や非機能要求グレードに基づく一般的な非機能要件のうち、**クロスチェーントランザクションにおいて特別な考慮が必要と考えられる以下機能・非機能要件**について重点的に検討。
- 本日は得られたプラクティスの一部(赤枠)を抜粋してご紹介。（全量は2023年6月公開予定の資料ご参照）

機能要件	両ブロックチェーンでのアトミックな更新（想定ユースケース①）
	他方ブロックチェーンへの参照（集計）を伴う更新（想定ユースケース②）
	プライバシー
	アイデンティティ指定
非機能要件	可用性（耐障害性）
	可用性（回復性）
	性能
	運用・保守性(監視・異常検知時対応)
	運用・保守性(リリース運用)
	セキュリティ

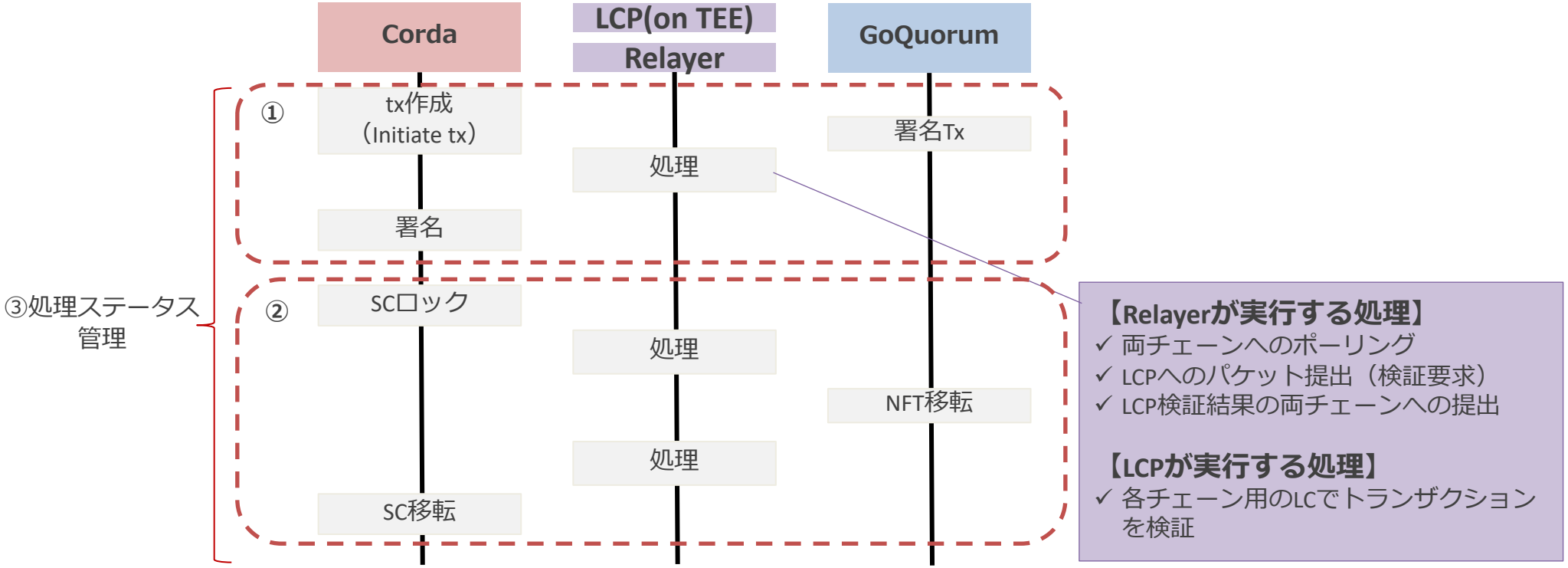
【機能要件】両ブロックチェーンでのアトミックな更新（想定ユースケース①）

ポイント

- ✓ Corda上で発行・管理されているステーブルコインとGoQuorum上で発行・管理されているNFTとのDVP決済のような両ブロックチェーンでのアトミックな更新には、Cross Frameworkが具備する機能を活用することで効率よく開発が可能。

Cross Frameworkがサポートする処理

① エンドユーザーによる認証・署名管理
② Simple Commitフローによるアトミックなトランザクションの管理
③ 処理フロー全体の処理ステータス管理



機能・非機能要件を実現するプラクティスのご紹介

- 想定ユースケースで設定されうる機能要件や非機能要求グレードに基づく一般的な非機能要件のうち、**クロスチェーントランザクションにおいて特別な考慮が必要と考えられる以下機能・非機能要件**について重点的に検討。
- 本日は得られたプラクティスの一部(赤枠)を抜粋してご紹介。（全量は2023年6月公開予定の資料ご参照）

機能要件	両ブロックチェーンでのアトミックな更新（想定ユースケース①）
	他方ブロックチェーンへの参照（集計）を伴う更新（想定ユースケース②）
	プライバシー
	アイデンティティ指定
非機能要件	可用性（耐障害性）
	可用性（回復性）
	性能
	運用・保守性(監視・異常検知時対応)
	運用・保守性(リリース運用)
	セキュリティ

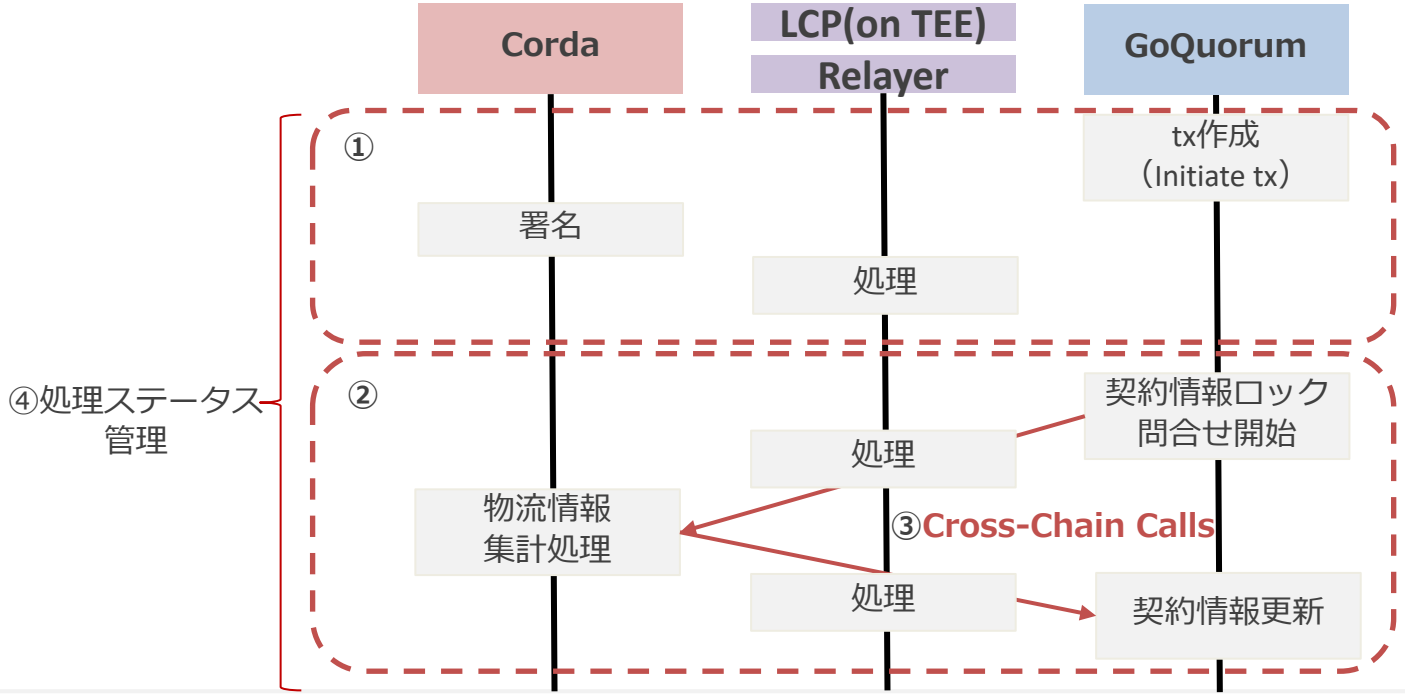
【機能要件】他方ブロックチェーンへの参照（集計）を伴う更新（想定ユースケース②）

ポイント

✓ Corda上で管理されている物流情報を参照してGoQuorum上で管理されている契約情報を日次で更新するような他方チェーンへの参照（集計）を伴う更新処理においても、Cross Frameworkが具備する機能を活用することで効率よく開発が可能。

Cross Frameworkがサポートする処理

① エンドユーザーによる認証・署名管理
② Simple Commitフローによるアトミックなトランザクションの管理
③ Cross-Chain Callsによる他チェーンへの参照処理
④ 処理フロー全体の処理ステータス管理



機能・非機能要件を実現するプラクティスのご紹介

- 想定ユースケースで設定されうる機能要件や非機能要求グレードに基づく一般的な非機能要件のうち、**クロスチェーントランザクションにおいて特別な考慮が必要と考えられる以下機能・非機能要件**について重点的に検討。
- 本日は得られたプラクティスの一部(赤枠)を抜粋してご紹介。（全量は2023年6月公開予定の資料ご参照）

機能要件	両ブロックチェーンでのアトミックな更新（想定ユースケース①）
	他方ブロックチェーンへの参照（集計）を伴う更新（想定ユースケース②）
	プライバシー
	アイデンティティ指定
非機能要件	可用性（耐障害性）
	可用性（回復性）
	性能
	運用・保守性(監視・異常検知時対応)
	運用・保守性(リリース運用)
	セキュリティ

【機能要件】プライバシー①

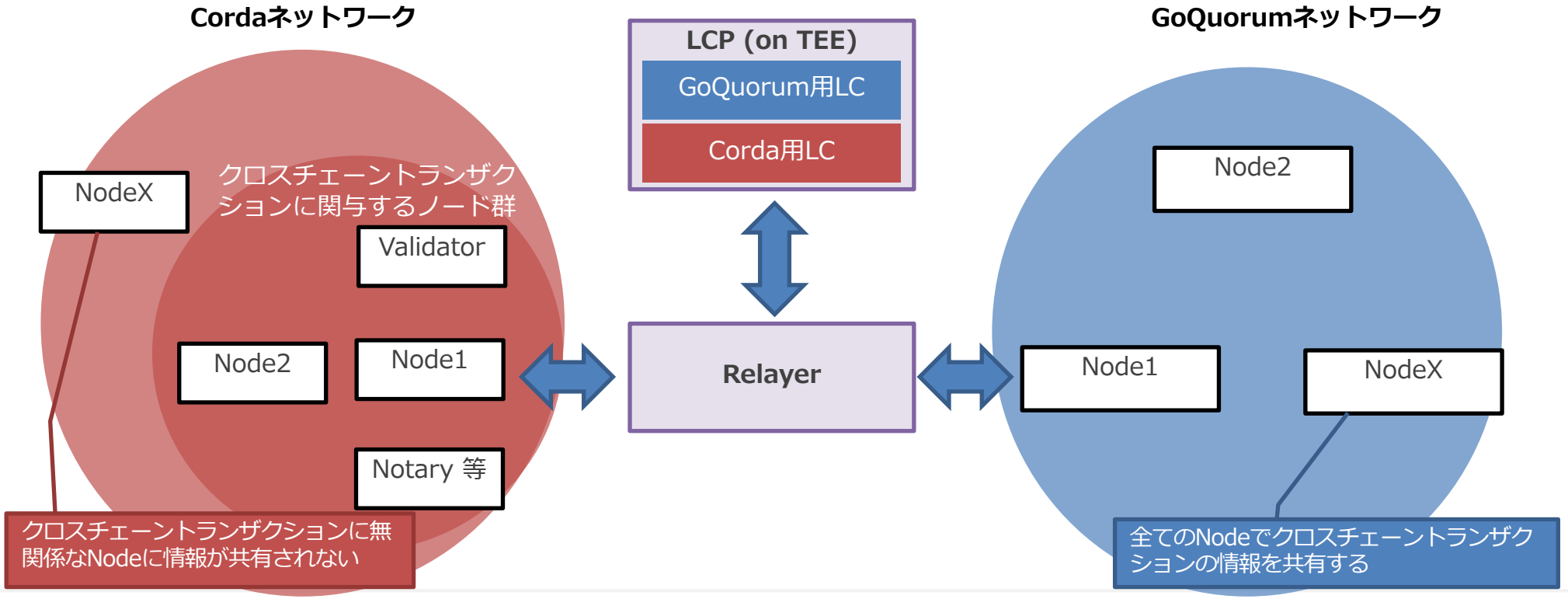
ポイント

- ✓ 情報の取扱いに関するチェーン間差異を把握し、以下観点を踏まえてプライバシー要件を設計する。
  - ① 伝播した情報に関する他方チェーン内での共有範囲
  - ② 他方チェーンへ伝播させる情報

伝播した情報に関する他方チェーン内での共有範囲

■ BC基盤毎の情報共有範囲の差異を踏まえ他方チェーンへ伝播させる情報を設計する必要がある。

- ✓ Corda: トランザクションに関与するノードのみで情報を共有
- ✓ GoQuorum: プライベートトランザクションを除き全ノードで情報を共有



【機能要件】プライバシー②

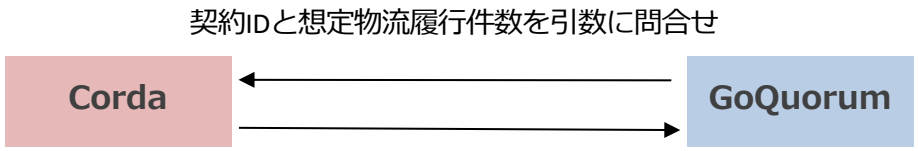
他方チェーンへ伝播させる情報

■ IBCプロトコルにおいて他方チェーンに伝播する情報は以下の2種類である。
① IBCの通信に係る制御用データ（非業務データ)
② クロスチェーントランザクションのデータ

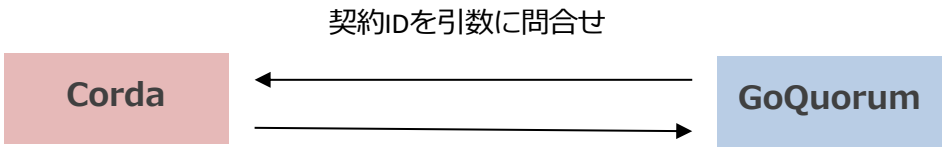
■ 上記②に関して、Cross-Chain Calls実行時の引数・レスポンス結果は任意の形態をとれる。
→レスポンスに含まれる回答の信頼性、プライバシー要件のバランスを踏まえた設計が可能。
※信頼性、プライバシー要件以外にもパフォーマンス等は考慮が必要

想定ユースケース②における設計例

設計例①
伝播する情報を限定しプライバシーを高めるパターン



設計例②
伝播する情報を増やし回答の信頼性を高めるパターン



機能・非機能要件を実現するプラクティスのご紹介

- 想定ユースケースで設定されうる機能要件や非機能要求グレードに基づく一般的な非機能要件のうち、**クロスチェーントランザクションにおいて特別な考慮が必要と考えられる以下機能・非機能要件**について重点的に検討。
- 本日は得られたプラクティスの一部(赤枠)を抜粋してご紹介。（全量は2023年6月公開予定の資料ご参照）

機能要件	両ブロックチェーンでのアトミックな更新（想定ユースケース①）
	他方ブロックチェーンへの参照（集計）を伴う更新（想定ユースケース②）
	プライバシー
	アイデンティティ指定
非機能要件	可用性（耐障害性）
	可用性（回復性）
	性能
	運用・保守性(監視・異常検知時対応)
	運用・保守性(リリース運用)
	セキュリティ

【非機能要件】性能①

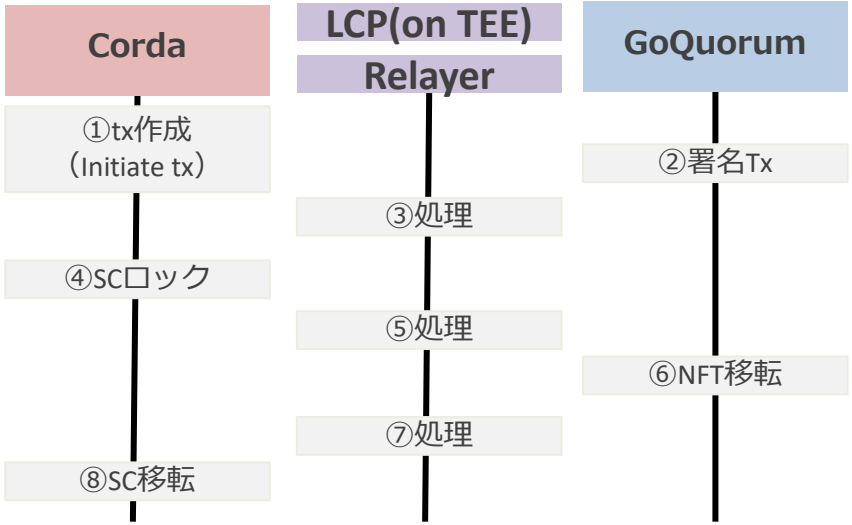
ポイント

- ✓ 各想定ユースケースにおけるラウンドトリップタイムは以下式となる。（NWの伝送時間含まず）

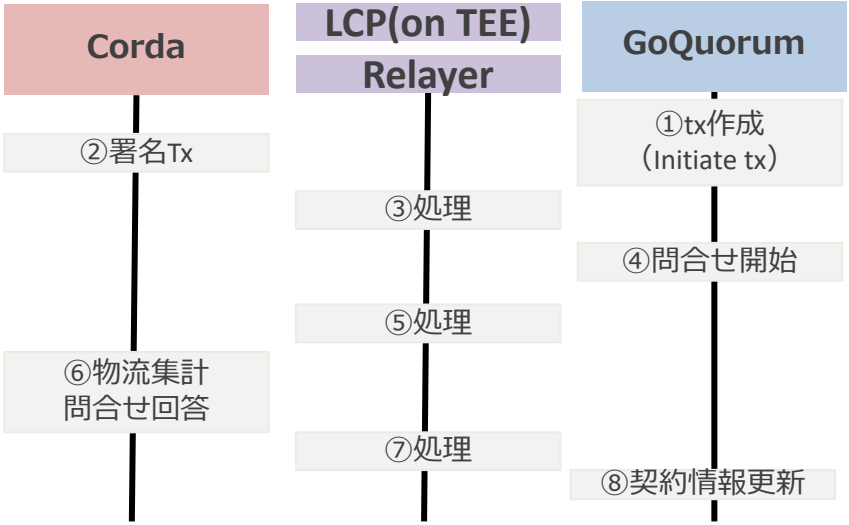
  ユースケース①：(Cordaトランザクション実行時間×3回) + (GoQuorumトランザクション実行時間×2回) + (Relayer・LCP処理時間×3回)
  ユースケース②：(Cordaトランザクション実行時間×2回) + (GoQuorumトランザクション実行時間×3回) + (Relayer・LCP処理時間×3回)

- ✓ 各構成要素における処理性能向上の工夫が有効。また、中長期稼働において各構成要素の性能劣化を低減させることも有効。
- ✓ 想定されるラウンドトリップタイムを踏まえ、エンドユーザーへのトランザクション完了通知を非同期で行う等のUX向上の工夫が考えられる。

ユースケース①ラウンドトリップタイム
Cordaトランザクション実行時間(①,④,⑧)
＋ GoQuorumトランザクション実行時間(②,⑥)
＋ Relayer・LCP処理時間(③,⑤,⑦)



ユースケース②ラウンドトリップタイム
Cordaトランザクション実行時間(②,⑥)
＋ GoQuorumトランザクション実行時間(①,④,⑧)
＋ Relayer・LCP処理時間(③,⑤,⑦)



【非機能要件】性能②

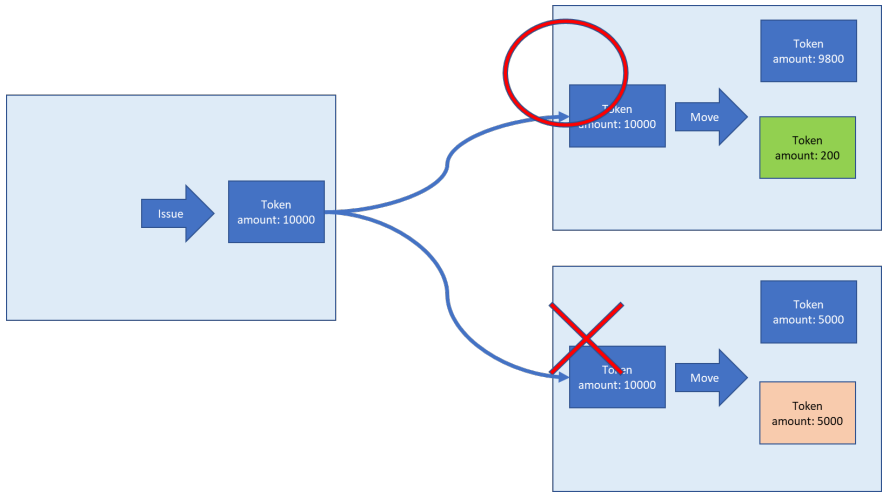
処理性能向上の工夫

- 各チェーンの処理性能の向上がクロスチェーントランザクション全体のラウンドトリップタイム短縮に有効。
- 各チェーンの処理性能向上はクロスチェーントランザクション固有の要素ではないが、工夫の一例としてCordaでは以下のような対応が可能。
  - ✓ マルチスレッド処理
  - ✓ トランザクションに含まれるStateを事前分割することによる並列処理容易性の向上。（下図イメージ）
  - ✓ ノードに含まれるRDBのインデックスメンテナンスや、 Corda Enterpriseの機能（Archive service） を用いたRDBレコードの安全な削除による中長期の性能劣化低減。

State事前分割イメージ

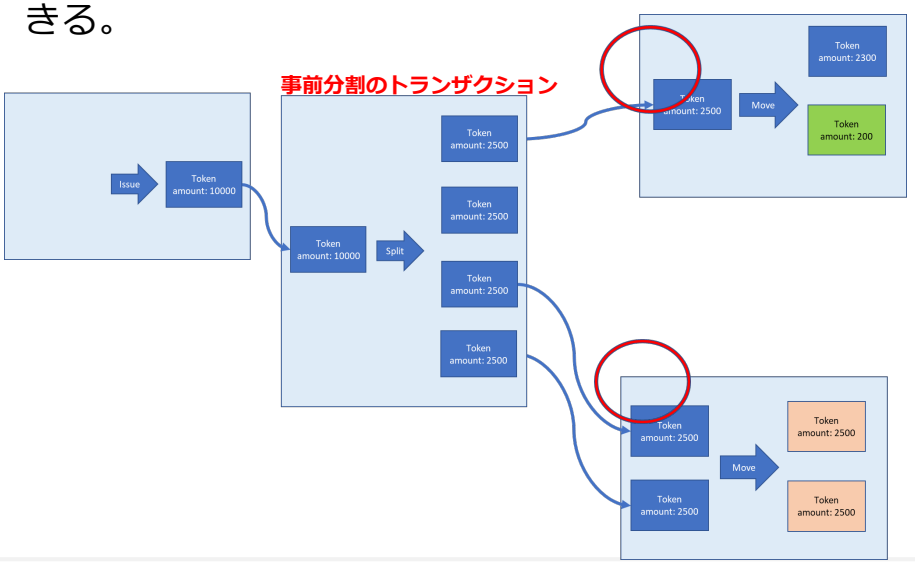
事前分割を実施しない場合

CordaはUTXOモデルを採用しており、同タイミングで同じStateを使うことができない。



事前分割を実施する場合

Stateを事前に分割しておくことで並列でStateを使用できる。



おわりに

- 異なるブロックチェーンのインターオペラビリティ実現はビジネス拡大やユースケース進展において重要な検討テーマ
- インターオペラビリティ技術や各ブロックチェーン技術は技術進展が続いているため以下が重要と思料
  - ✓ インターオペラビリティ導入時点の技術水準を踏まえた機能・運用の設計
  - ✓ 各技術のアップデートの取り込み
  - ✓ 上記を実施できる体制

Corda観点での本取組みの振り返り

- 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対応可能
- プライバシーの高さに特徴
  - ✓ クロスチェーントランザクションで受領した情報についても関係者のみで共有
- スケーラビリティ
  - ✓ Cordappチューニング、インフラレベルのチューニング（スケールアップ・スケールアウト）、中長期稼働を見据えた性能維持が可能
- プロフェッショナルサービスを通じて得られるノウハウ・知見

本取組みで得られたプラクティスを2023年6月に公開予定ですので、各社HP等より是非ご覧ください。

本資料は情報提供のみを目的として作成されたものであり、商品の勧誘を目的としたものではありません。

本資料は、当社が信頼できると判断した各種データに基づき作成されておりますが、その正確性、確実性を保証するものではありません。また、本資料に記載された内容は予告なしに変更されることもあります。

本資料記載の製品、サービス名は各社の商標または登録商標です。