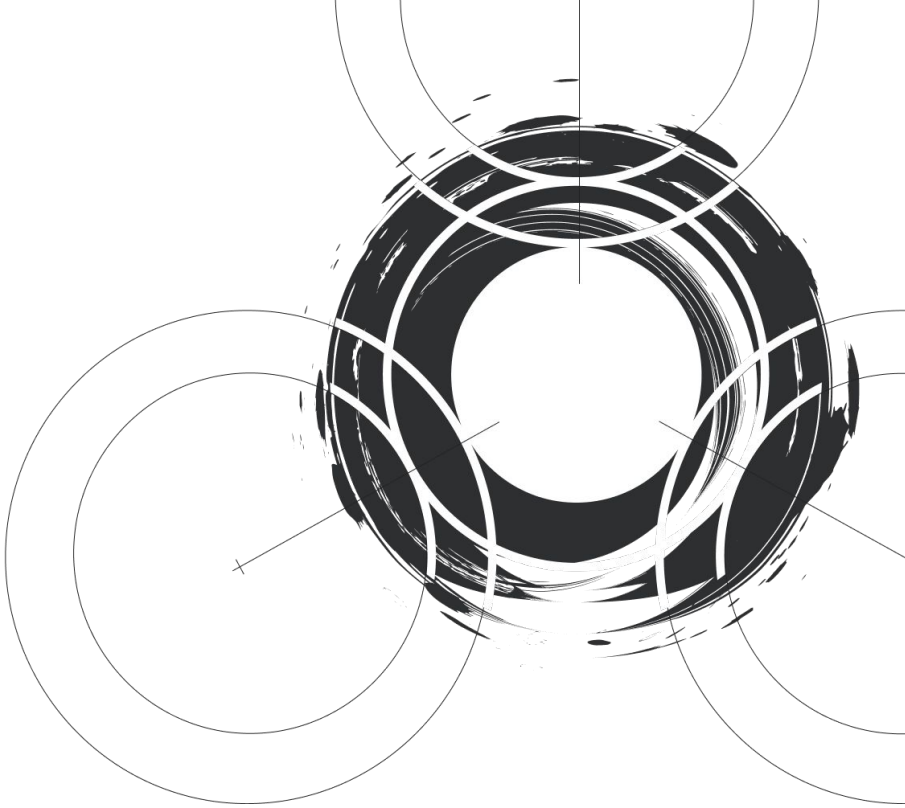
Datachain

日本銀行　CBDCフォーラム　WG4

【新たなテクノロジーとCBDC】

株式会社Datachain



サマリ

- **異なるシステムを接続し、連携させるインターオペラビリティ（相互運用性）は様々なトークン化プラットフォームでのユースケースにおいて重要であり、今後、CBDCシステムでも重要となることが見立てられる**
  - 特にDLT（分散型台帳技術）を用いたデジタルアセットプラットフォームでは、アセット転送やDvP、オラクルなどに利用され、DeFiを支えている

- **スムースなインターオペラビリティを実現することで、様々なアセットプラットフォームや外部データの利用が可能になり、支払の自動執行 等、価値の円滑なやりとりに寄与することが出来る**

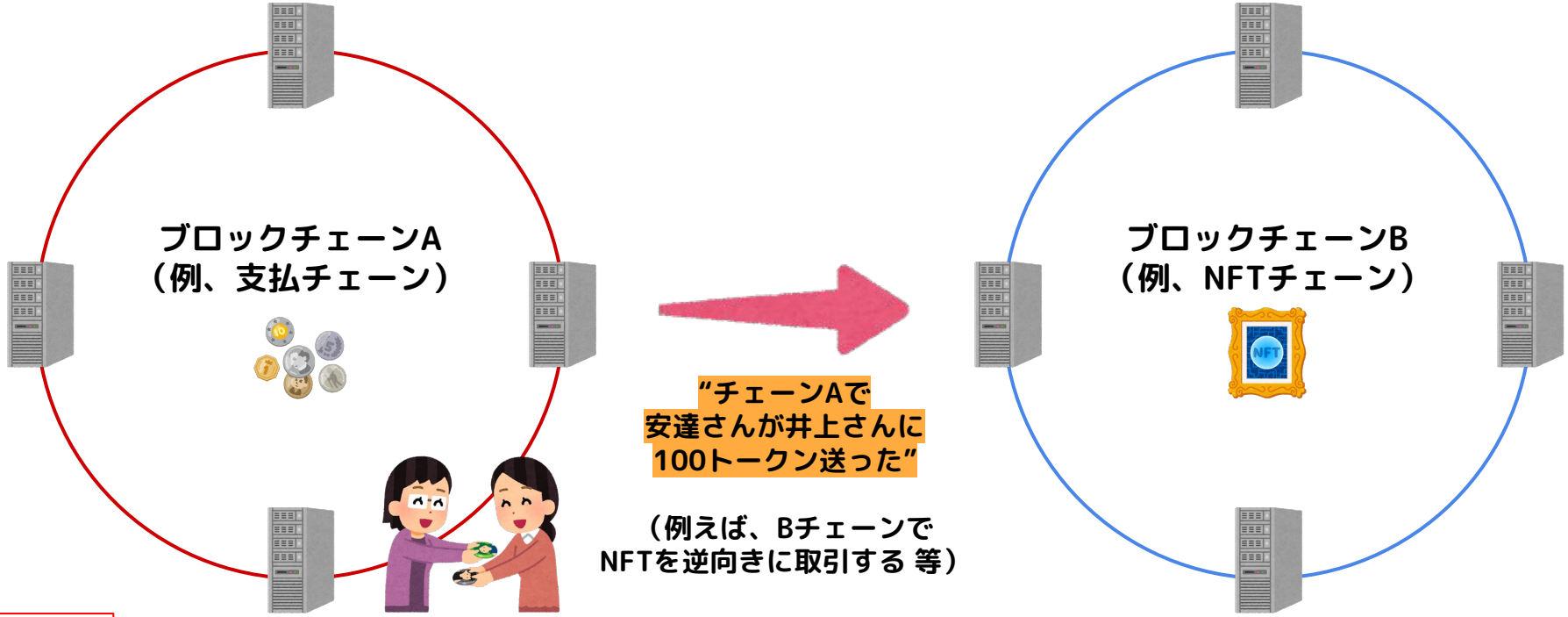
- **現状、RWAのトークン化の進展 等と併せて、様々なインターオペラビリティプロトコルの利用が広がっており、各方式の長所・短所を踏まえた検討や、標準化の議論を進めていくことが肝要と想定**
  - 伝統的金融機関においても、実用化されているブリッジの棚卸しや先端技術の適用を含め、検証が進んでいる

インターオペラビリティ（相互運用性）

Datachain

インターオペラビリティとは複数のシステムを安全に接続し、連携するためのメカニズムである

例）ブロックチェーンシステム間のインターオペラビリティ



CONFIDENTIAL

インターオペラビリティのユースケース

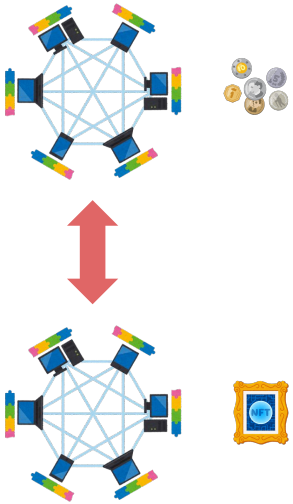
Datachain

トークン化アセットに関連するインターオペラビリティのユースケースとしては、DeFi領域を中心に様々なユースケースが存在。例えばトークン転送やDvP（Delivery-versus-Payment）、オラクルなどが存在

トークン転送

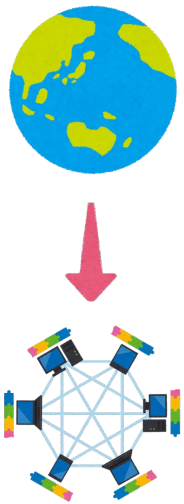
例）BitcoinをEthereum上でWBTCとして扱うEthereum上でのDeFi等でトークンとして利用可能

DvP



例）Ethereum上でUSDCを送り、AvalancheでNFTを受け取る

オラクル



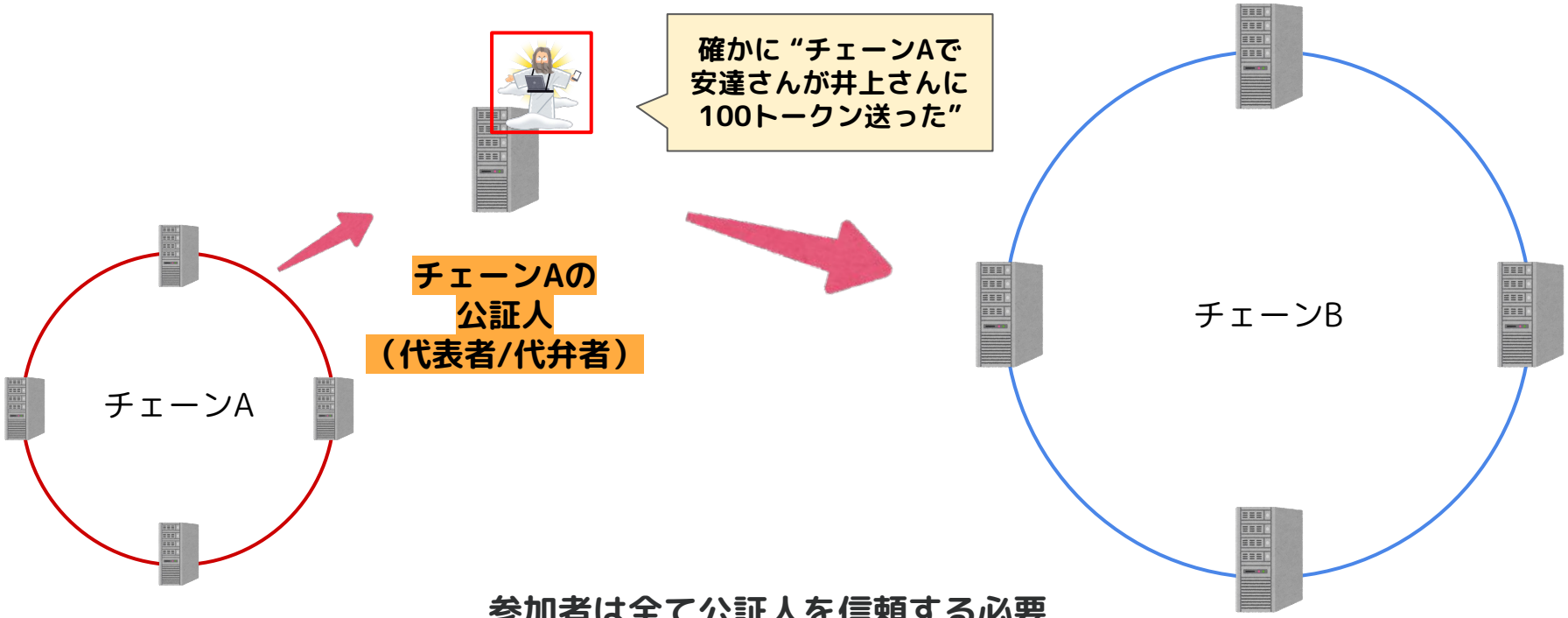
例）選挙結果などをブロックチェーンに書き込み、予測市場に利用

CONFIDENTIAL

インターオペラビリティの（Trivialな）実現方式

Datachain

二つのシステムにインターオペラビリティをもたらす上では、双方のシステムにアクセスできる「公証人」（Notary）が情報をやりとりする方式が考えられる



参加者は全て公証人を信頼する必要
（i.e. 公証人が嘘をつくと、安全性は損なわれる）

CONFIDENTIAL

インターオペラビリティの類型化

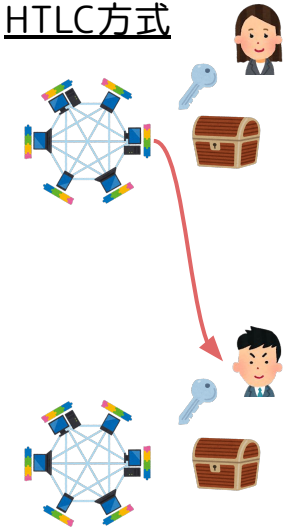
Datachain

先のTrivialなやり方に加え、HTLC（Hashed Time-Locked Contract）方式やシステムのコンセンサスを検証するLight Client検証方式がインターオペラビリティの実現方式として挙げられる

Notary方式

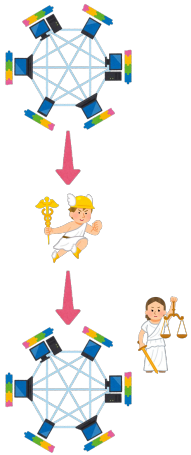
信頼できる公証人がメッセージを伝達

HTLC方式



アセットを渡すための「箱」を用意し、DvPを実現

Light Client検証方式



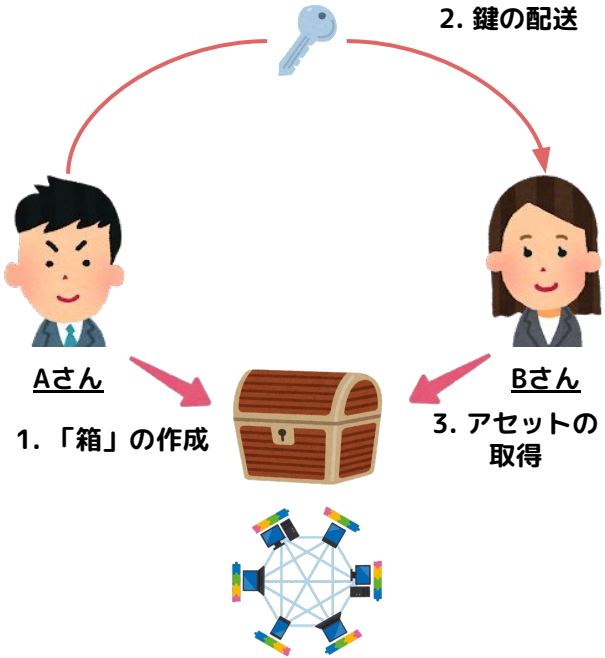
信頼を必要としないリレーヤー（Relayer）がメッセージを伝達し、受け手側のシステムで検証を行う

CONFIDENTIAL

HTLC（Hashed Time-Locked Contract）方式

Datachain

HTLCでは、アセットをロック可能な「箱」を介してやりとりすることで、システムをまたいだアセットのやりとりを可能とする。仕組み上、ユースケースは限定される



「箱」を作ってアセットを渡す

- 「箱」はBさんが正しい鍵を提示するとアセットをBさんに渡す
  - Hash（鍵）＝ある値
- 時間切れになるとAさんがアセットを取り戻せる

通常は鍵を配送する必要があるが、工夫をすることで、DvPが実現可能

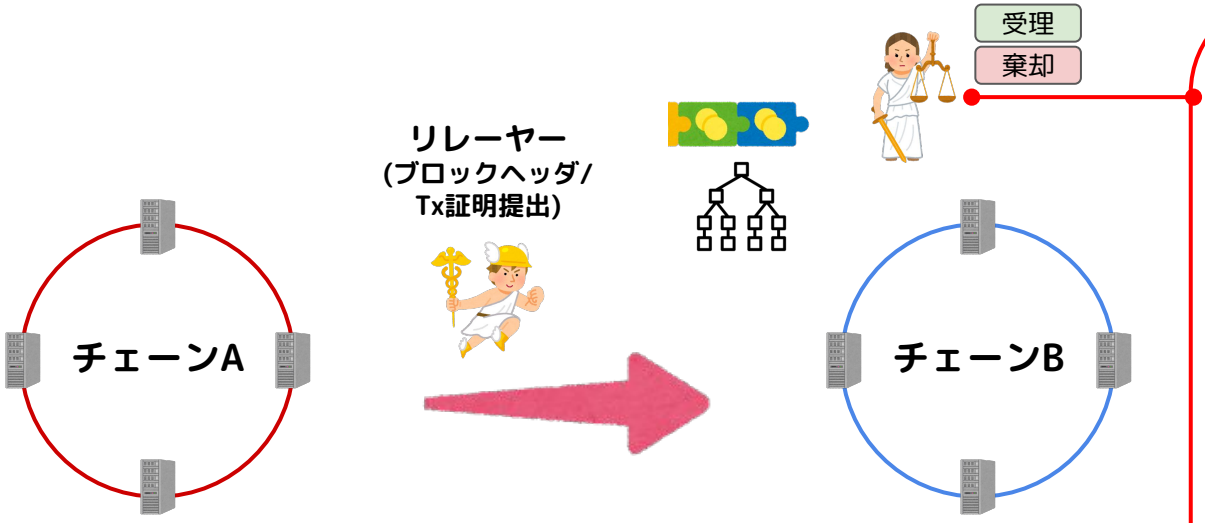
- 「箱」をAさんが作る
- 別の「箱」を「ある値」の設定値はそのままでBさんが作る
- Aさんは、Bさんの箱を自分の鍵で開ける
- Bさんは、ブロックチェーンの透明性を利用し、Aさんの鍵を知れる→Aさんが作った箱を開けられる

「箱」を用いており、アセットの譲渡にユースケースは限られる

CONFIDENTIAL

Light Client検証方式

システムのコンセンサスを検証することで、システムと同程度の強度の安全性を目指す方式
（Don’t Trust, Verify）



オンチェーン・ライトクライアント
（スマートコントラクトと
してすべてのノードで実行）

- 提出されたヘッダが正当であることを検証する
  - バリデータセットの署名 等
- Tx証明を用いて、メッセージが正当であることを検証
  - Merkle証明 等

チェーンB内で外部に依存せず検証

＊チェーンAのバリデータセットが結託すると任意の攻撃が可能

Datachainでも
Light Client検証方式に準ずる方式を提供（後述）

インターオペラビリティの類型化：各方式の長所・短所

Datachain

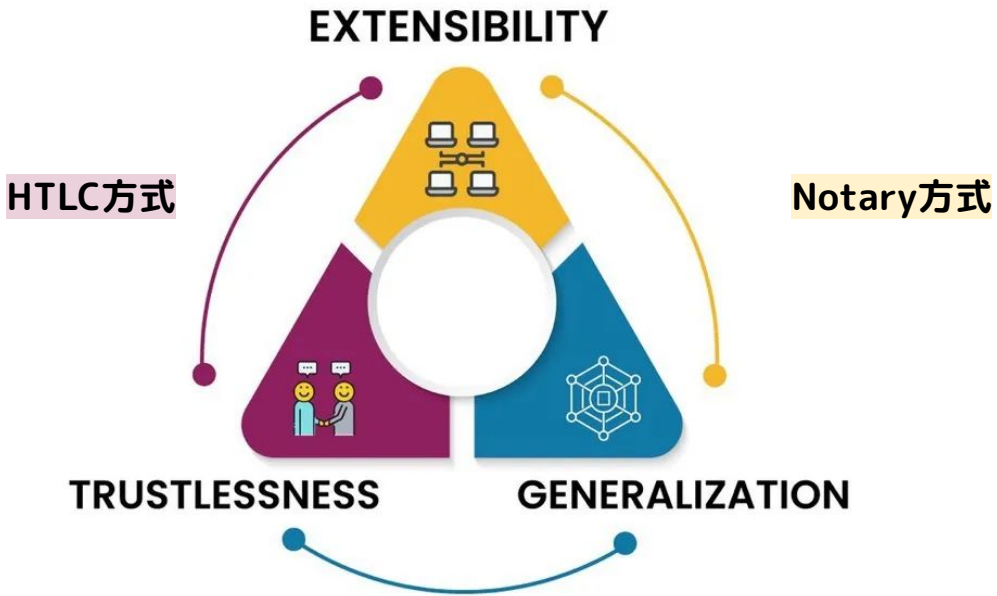
全ての方式について、良い点と悪い点が存在し、各々の要素がトレードオフの関係になっている

	Notary方式	HTLC方式	Light Client検証方式
利点	**公証人が存在すれば、システムがシンプル** ● 拡張性に富む	**アセットを渡すためのプロトコルとしてはシンプル**	**接続するシステム以外には信頼仮定が小さい（Trust-minimized）**
課題	**公証人を仮定しづらい可能性** ● ネットワーク数が増加すると特に難しくなる可能性 **公証人が攻撃対象となり得る**	**一般的なメッセージの送受信は出来ない** **システムに複数回アクセスする必要があるため、オンライン性が重要**	**検証を行うLight Clientを構成する必要が存在** ● コンセンサスを検証する場合、コンセンサスアルゴリズム毎に必要 **オンチェーンでの検証にコストがかかる**

CONFIDENTIAL

Refs：インターオペラビリティ方式のTrilemma

安全性（Trustlessness）・ユースケースの広がり（Generalizable）・ネットワーク拡張性（Extensible）の全てを高いレベルで実現することが出来ない



Ref) A Brief History of Blockchain Interoperability, Communications of the ACM, Volume 67, Issue 10

インターオペラビリティプロトコル

足許で稼働するインターオペラビリティプロトコルとしては、Notary方式をベースとして、Trustlessnessを強化する方向性で拡張を加えたプロトコルが多い。近年、TradFiとの結びつきを強化している

LayerZero.

70+ネットワークに対応、これまでに50+B$の転送を実施

Project GuardianのJPMorganの取り組みで、OnyxとAvalancheを接続

AXELAR

75ノードで構成されたブリッジチェーンを提供。これまでに10+B$の転送を実施

左記のJPMorganとの取り組みではOnyxとProvenanceを接続

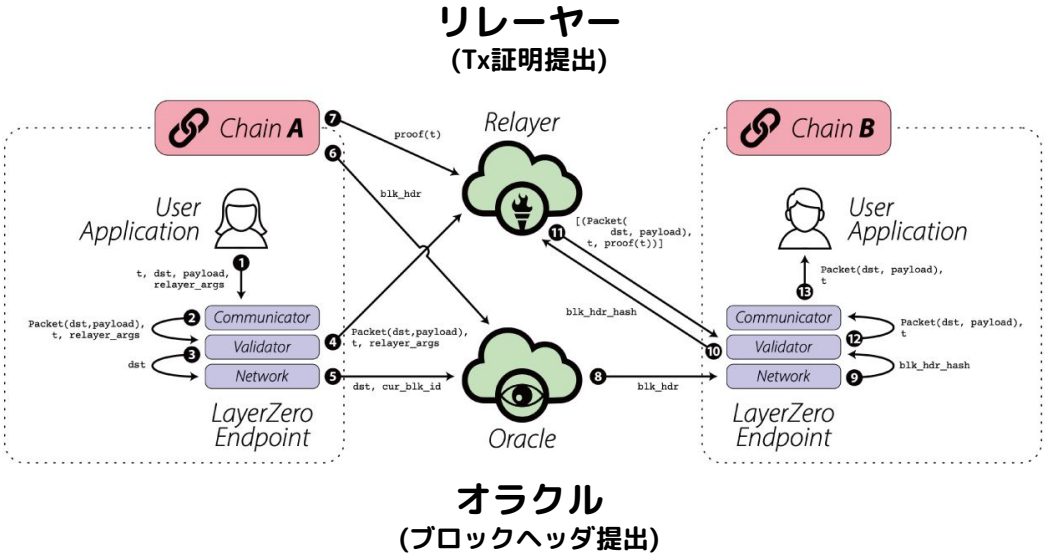
Chainlink CCIP

Oracleプロトコルである Chainlinkが、Oracleネットワークを利用し、ブリッジを提供

Project Guardianに参加 また、SWIFTとDvPの実証も実施

IETF(Internet Engineering Task Force)にて議論されているデジタルアセットシステム間でのプロトコル

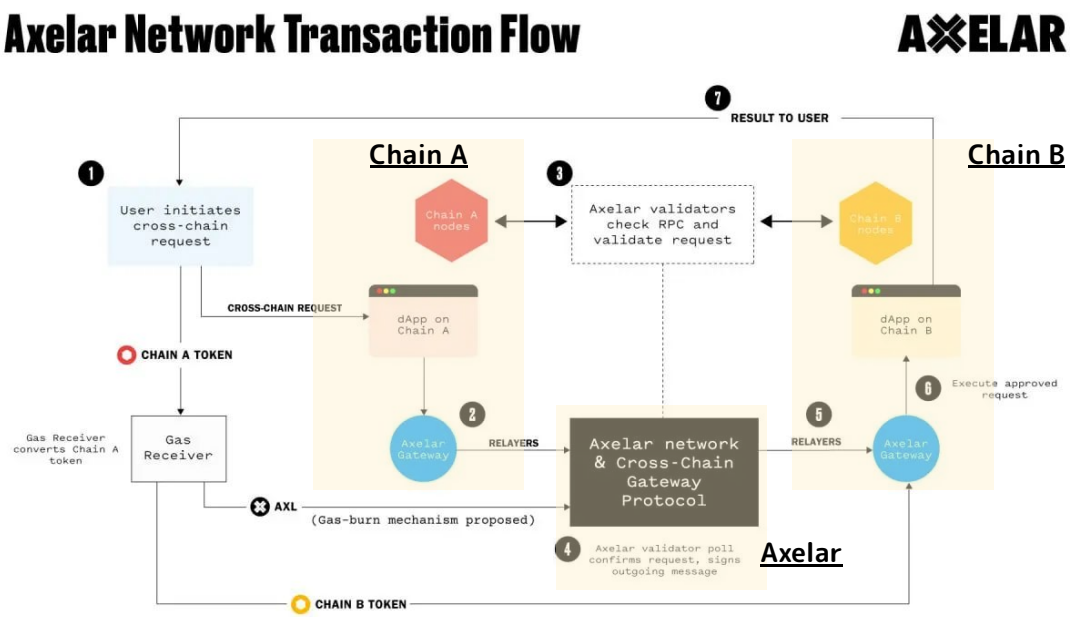
LayerZero（の初期のバージョン）では、Notaryを二つの役割を果たすエンティティに分割し、単一の障害点を防ぐ方式を採用。現在（v2）は「DVNs」という形で中間層を抽象化し、利用者が選択可能な形に移行



- **ブロックヘッダとTx証明を割符の様に利用してインターオペラビリティを実現**
  - 正しいブロックヘッダとTx証明を組み合わせると、送信元チェーンであるTxが合ったことを軽量で検証可能
- **デフォルト設定では下記のような運営体制（利用アプリが設定可能）**
  - オラクル: Industry TSS Oracle (Polygon, Sequoia) → Google Cloud に変更
  - リレーヤー: LayerZero Labs
- **（初期バージョンでは）オラクルとリレーヤーが結託しないことをセキュリティの根拠とする**

Ref) LayerZero v1 whitepaper

Axelarは、分散化されたノードで構成される「ブリッジチェーン」を構成し、ブリッジチェーンを介して情報をやりとりする



- 基本的にはL1チェーンの参加者がAxelar Networkに情報を連携
  （『チェーンAからチェーンBに、ある情報を送りたい』）
- 多数決の仕組みで、Axelar Networkがその情報に合意→チェーンBにAからの情報を書き込み
- 分散化とインセンティブがセキュリティを支える
  - 75バリデータ
  - 総ステーク量：700M AXL(~= 450M$)

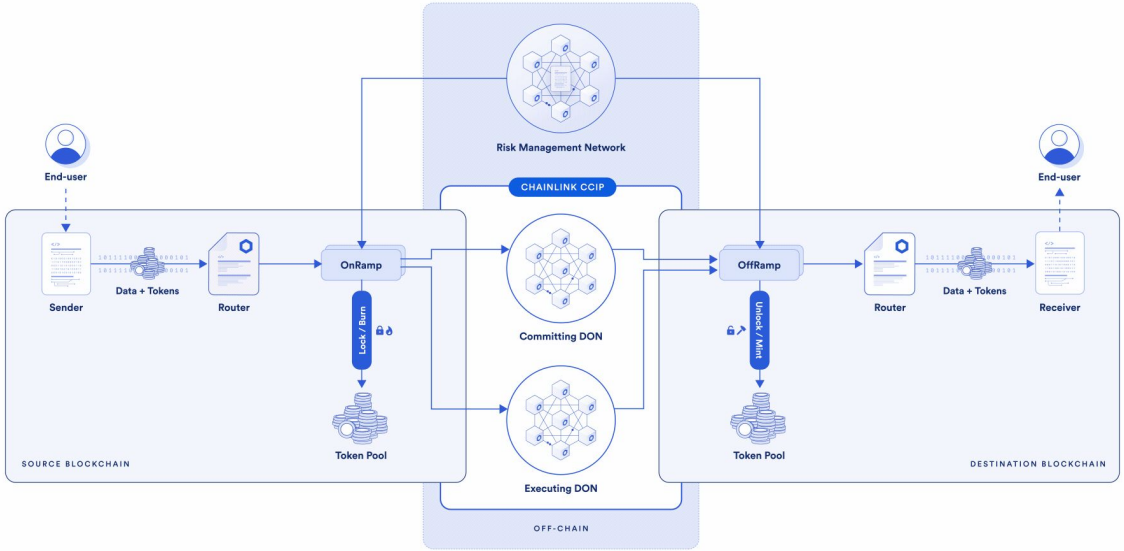
Ref) Axelar blog, Axelarscan

CONFIDENTIAL

インターオペラビリティプロトコル：Chainlink CCIP（Cross-chain Interoperability Protocol）

Datachain

Chainlinkは分散化オラクルのインフラをベースとして、役割分担やインセンティブのメカニズムを導入することでブロックチェーン間のインターオペラビリティを実現



Ref) Chainlink CCIP Docs

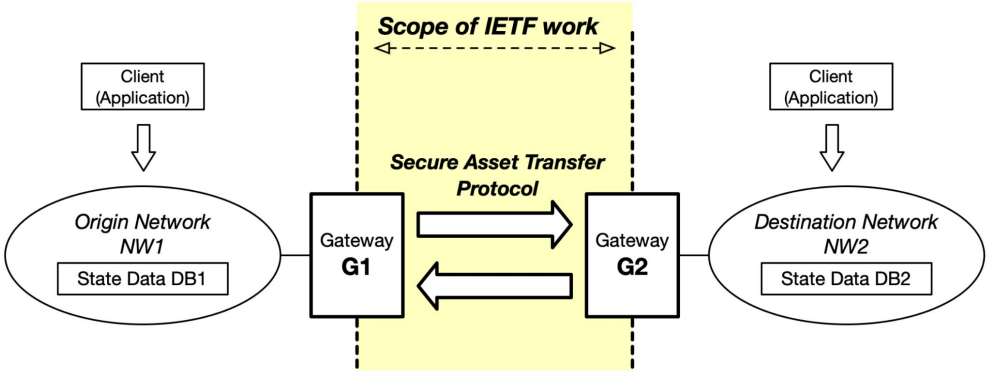
- **分散化されたノード群（Chainlink）を用いてチェーン間の連携を行う**
- **分散化されたOracle Networkを3つの役割に分割**
  - Committing DON
  - Executing DON
  - Risk Management Network（RMN）
- **Committing DONが提出したサマリをRMNが承認し、その上でExecuting DONが実行**
  - 役割を分担したDONによる二重のチェック

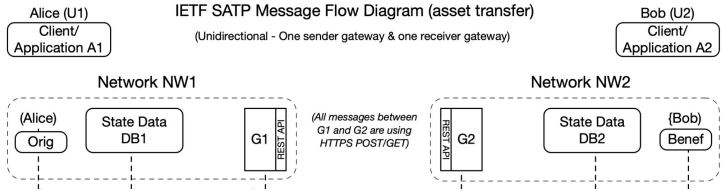
CONFIDENTIAL

インターオペラビリティプロトコル：SATP（Secure Asset Transfer Protocol）

Datachain

標準化の議論としては、IETF（Internet Engineering Task-Force）において、SATPという2 Phase Commitをベースとしたプロトコル方式が検討されている





Stage 0: 実行前準備
- ネットワークの発見など

Stage 1: Propose
- セッション開始のためのHandshake

Stage 2: Lock
- Src NetworkでのAsset Lock

Stage 3: Commit
- Dest NetworkでのCreate/Assign
- Src NetworkでのDelete

一部金融機関などで、SATPをベースとした検討が実施されている模様

Ref) https://github.com/ietf-satp

CONFIDENTIAL

Refs：Northern Trustによる分析

Datachain

Northern Trustがインターオペラビリティに関する調査・実証を実施。Privateなど独自チェーンを用いる場合、既存のPublicチェーンでのブリッジ利用に課題があることが浮き彫りとなった

	LayerZero	Axelar	Chainlink CCIP
利点	**Deployが一定容易であり、Privateチェーンでも実行できた**	**Publicチェーンのデータを連携する75 validatorsのセキュリティは十分高いといえる**	**DONを3つの役割に分割している点などは評価でき、これらの中では最もセキュアといえる**
課題	**DefaultのDVN設定が脆弱** ● 2 of 3 signatures **Defaultから設定を変更するのは難しい。一定OSS化されているものの開発者サポートは3つの中で最も少ない**	**必ずしも75ノードの分散化が実現できるわけではない** **Privateチェーンにおいては利用が難しい**	**Axelar同様、必ずしもDONは分散化されない可能性** **Privateチェーンにおける利用はAxelarよりさらに難しい** **サポート対象のチェーンが少ない（現状9チェーン）**

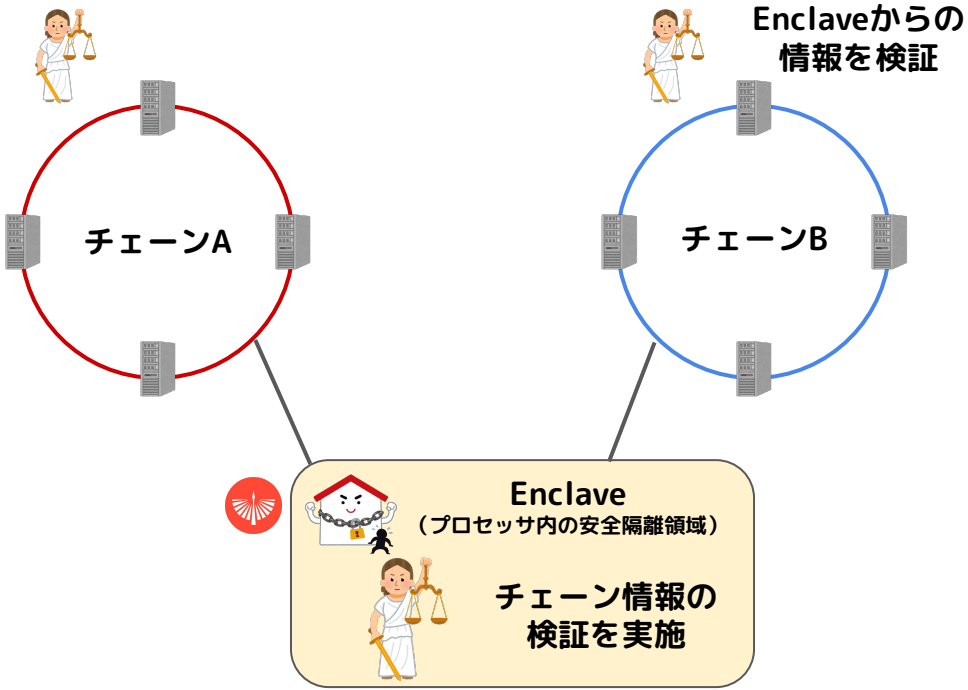
Ref) Interoperability of Tokenized Assets: Towards a Secured and Unified Future in the Financial Industry

CONFIDENTIAL

インターオペラビリティプロトコル：LCP（Light Client Proxy）

Datachain

Datachainでは、Light Client検証方式として、IBC（Inter-blockchain Communication Protocol）に則ったプロトコルを開発し、DvPやPvPの実活用に向けて導入を進めている



Light Client検証方式に伴う課題をTEEと呼ばれるプロセッサ技術を用いることで一定解消

- オンチェーンでの検証コストを低減
- 開発環境の複雑性を低減

Enclaveと呼ばれる保護領域でLight Client検証をオフロード

- プロセッサ 等の完全性が保たれていれば、スマートコントラクトと同様に、透明性が担保

IBCに規定される通信プロトコルをサポートし、任意のメッセージ送受信が可能

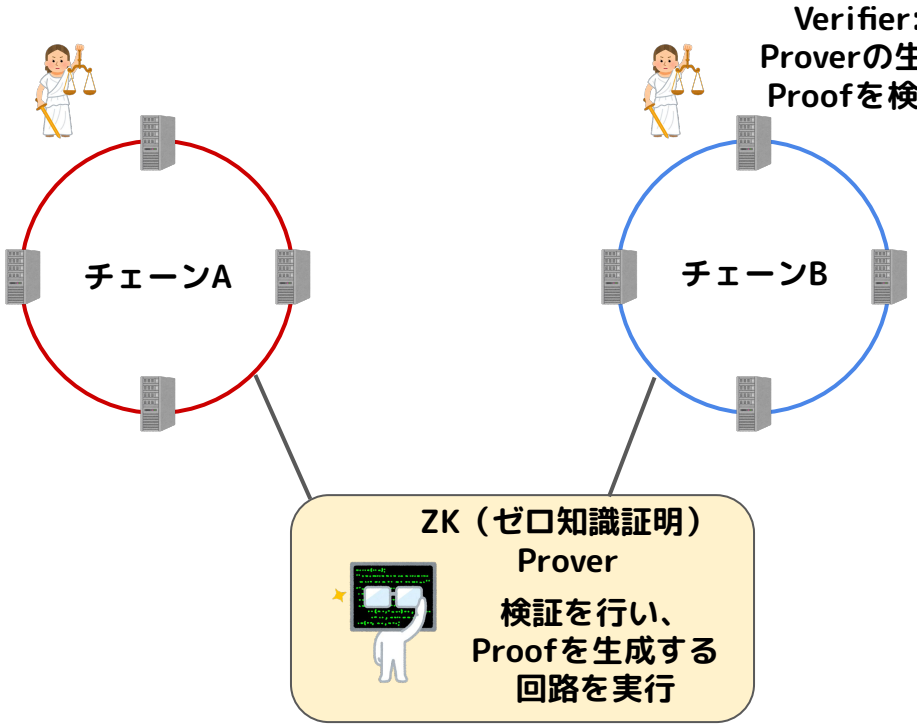
デジタルアセットのDvPやStablecoinのPvPへの活用を図る

CONFIDENTIAL

インターオペラビリティ方式における研究開発

Datachain

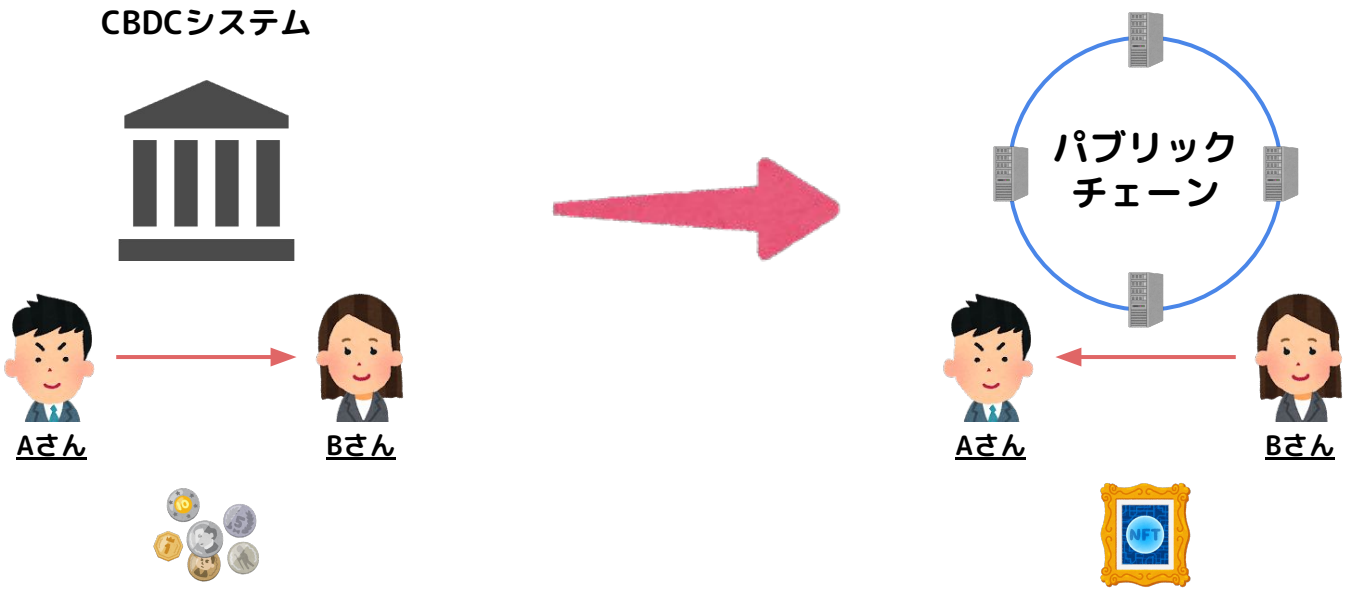
特に、ゼロ知識証明を利用したプロトコルの研究開発がブリッジやオラクルの領域で進展している。具体的な方法としてはLCPに近いが、Light Client検証を実行し、その証明を検証する形になる



- **オフチェーンでチェーンAのコンセンサスを検証し、簡潔なProofを生成**
- **チェーン上のVerifierは簡潔なProofの検証を実施**
  - 基本的には楕円曲線上の複数の点がある性質を満たすかをチェック
- **ここ数年で、実用化・実用化に近い段階まで技術が進展し、実証なども進む**
  - （やや文脈が異なるが）Project Mandala、Web Proofなど

CBDCを絡めたインターオペラビリティのユースケース：シナリオ

例えば、CBDCシステムとパブリックブロックチェーン上のトークン化アセットを接続し、DvPを行うシナリオが想起できる。インターオペラビリティの類型化に沿って、各方式での具体的な構成を考える

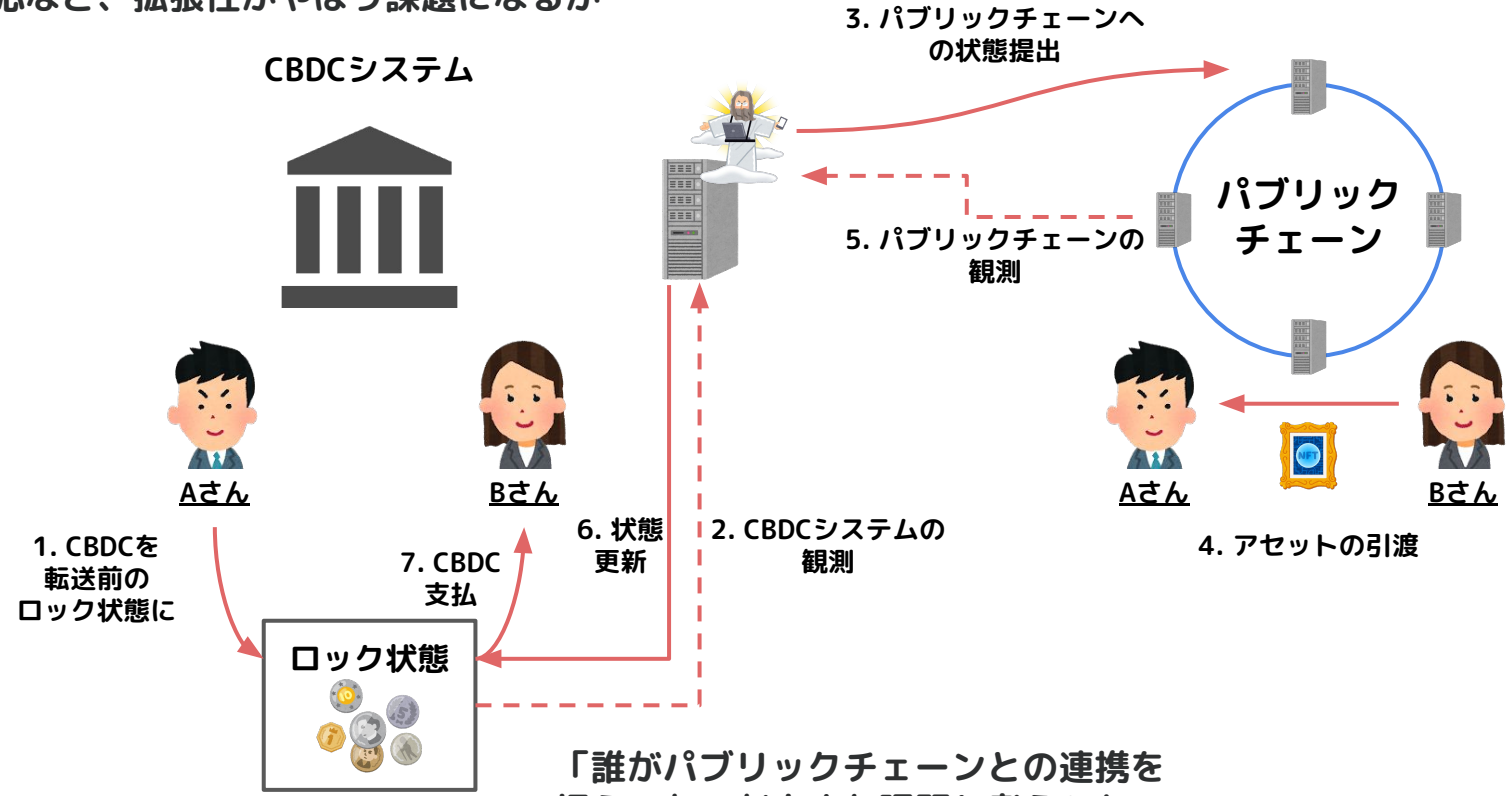


1. CBDCシステムでのAさんからBさんへの支払・
2. パブリックチェーンでのBさんからAさんへのアセット引渡をセットで行う

CBDCを絡めたインターオペラビリティのユースケース：Notary方式の例

Datachain

ある信頼できる機関（例えば日本銀行）を介して情報をやりとりする形になる。新たなネットワークへの対応など、拡張性がやはり課題になるか



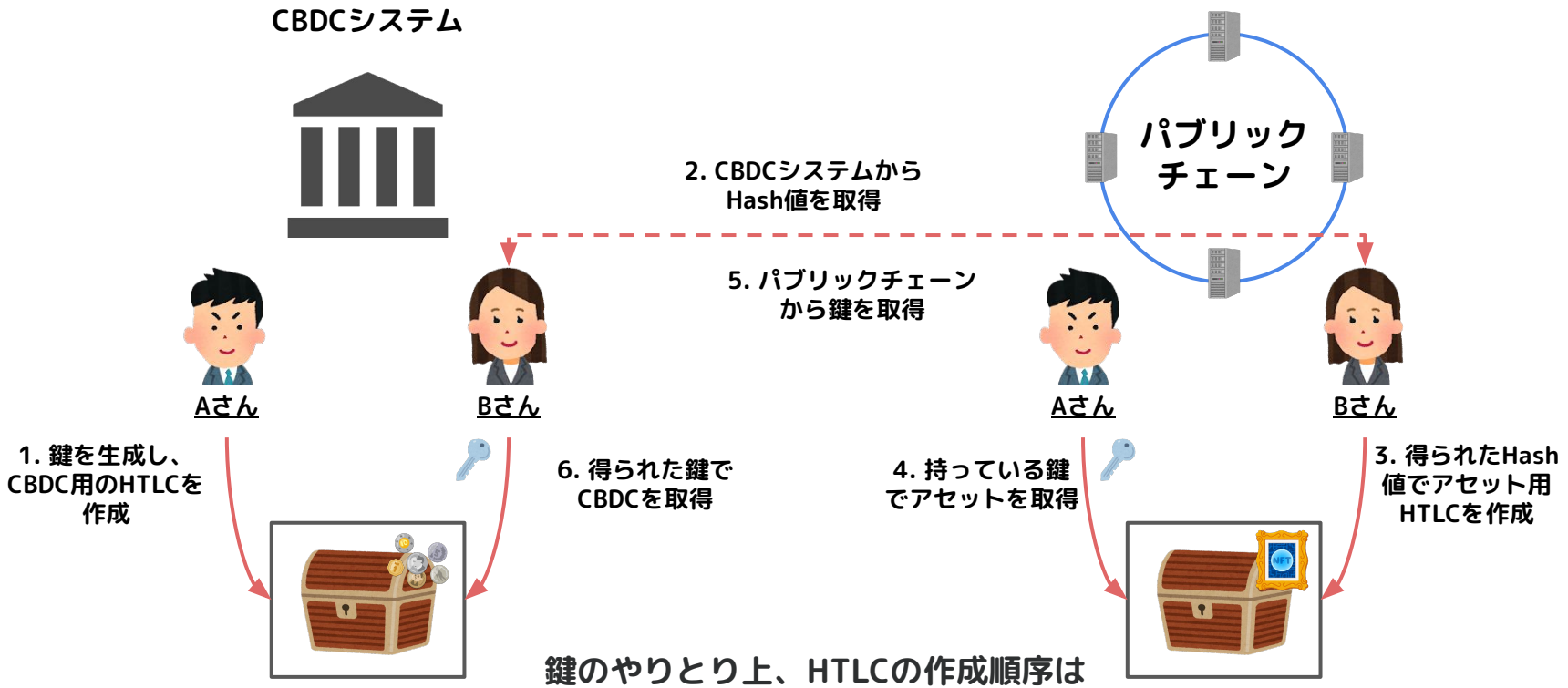
「誰がパブリックチェーンとの連携を担うのか」が大きな課題と考えられる

CONFIDENTIAL

CBDCを絡めたインターオペラビリティのユースケース：HTLC方式の例

Datachain

HTLC方式では、CBDC側台帳での方式や鍵（Preimage）のやりとり、参加者のオンライン性が課題になる可能性



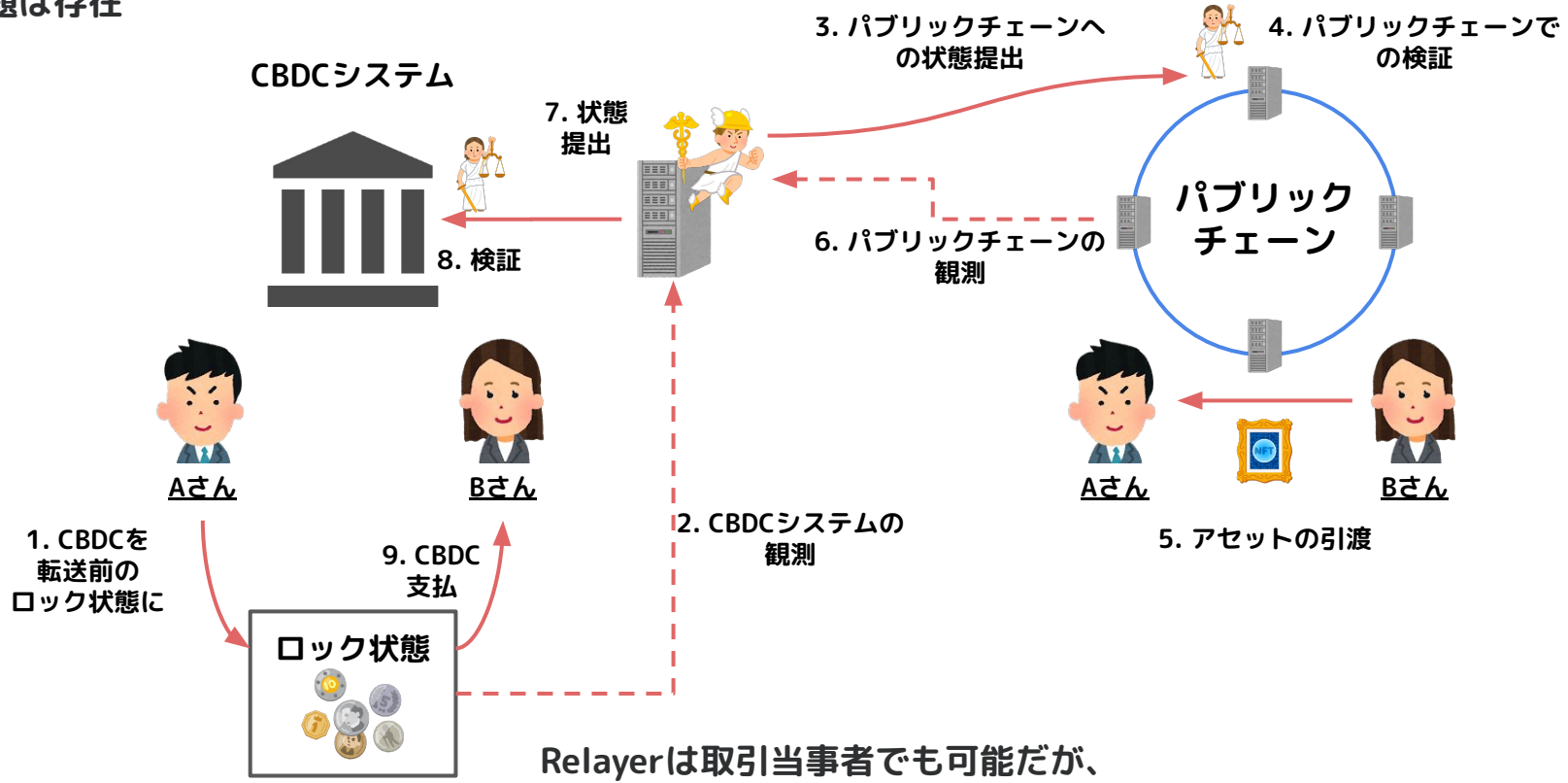
鍵のやりとり上、HTLCの作成順序は基本固定される

CONFIDENTIAL

CBDCを絡めたインターオペラビリティのユースケース：Light Client検証方式の例

Datachain

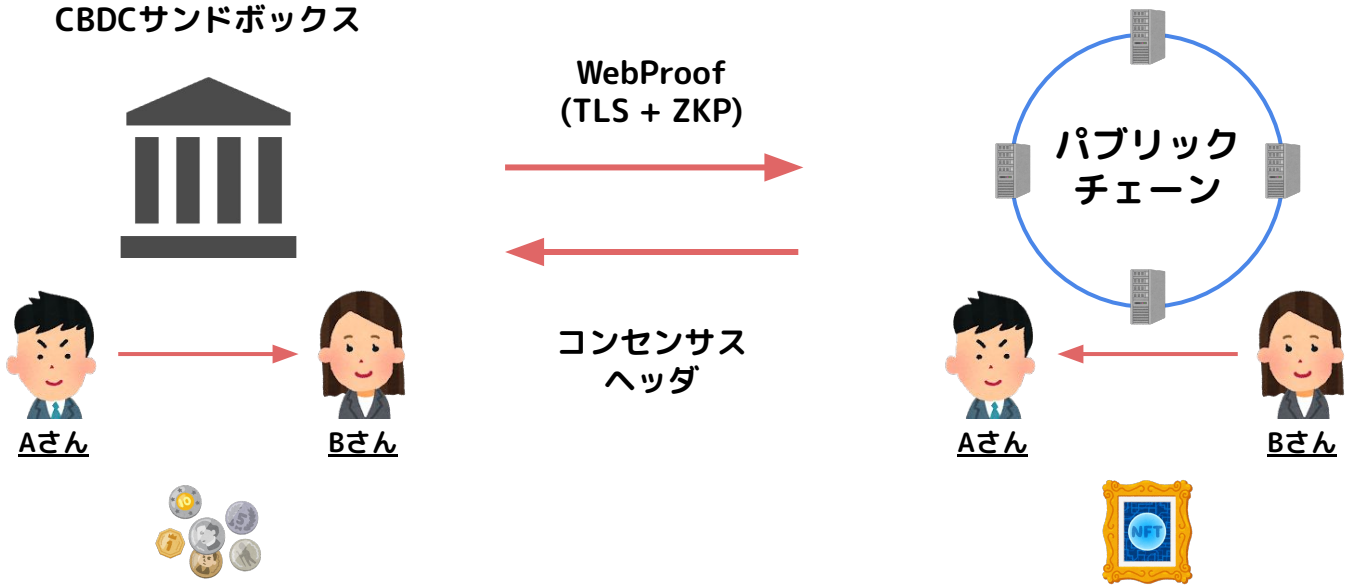
一度仕組みを構築すれば、信頼を置く必要のあるNotaryが不要となるが、双方のシステム改修などに伴う課題は存在



Relayerは取引当事者でも可能だが、
(4)で何を検証するかが不明瞭（Web Proofなど?）

CONFIDENTIAL

前ページに近い設定で、CBDCサンドボックスを用いてパブリックチェーンとの間での、ユースケースも含めた実証を進めていきたい



別の主題になるが、TIS様ともクロスチェーン文脈で実証予定であり、
上記のようなインターオペラビリティの実証を、サンドボックスを用いて進めていきたい

議論トピック（あくまでもご参考として）

- 先のシナリオを想定した場合においても各方式に一長一短が存在しており、現実のプロトコル同様、設定・ニーズに即したプロトコルの拡張が必要と考えられる

- CBDCシステムに求められるインターオペラビリティ方式について、以下のような切り口を例として議論させていただきたい
  - 安全性・信頼仮定
  - 対象とするユースケースの広がり
  - ネットワーク拡張性