CBDCフォーラム
【新たなテクノロジーとCBDC】WG（WG4）
第12回会合 事務局説明資料

カナダ中銀ディスカッションペーパー
“A Retail CBDC Design for Basic Payments: Feasibility Study”

2025年12月22日

日本銀行 決済機構局

ポイント

- WG4の初回会合で紹介したHamilton Phase1の拡張モデル
  - ✓ Hamiltonのコンセプトを踏襲：高性能、高プライバシーのUTXOモデル
    ※Hamilton同様、本DPはあくまで技術検証の一環との位置づけ。
  - ✓ Hamiltonからの拡張：TradFiで求められる機能の実装可能性を検討

- 本DPも議論の材料の一つとしながら、最後にCBDCの将来的なデザインの可能性に関してディスカッション。

Project Hamilton Phase1の振り返り：概要

- ボストン連銀とMITメディアラボデジタル通貨イニシアティブが共同でProject Hamiltonを実施、2022年2月にフェーズ1報告書を公表。
- 実験システムの価値情報はUTXOモデルで表現。ローカル検証をするSentinelと、存在性検証をするUHSデータベースで構成。UHSデータベースの設計はAtomizerと2PCの２種類。

トランザクションプロセッサ

UHSデータベース (実行エンジン)

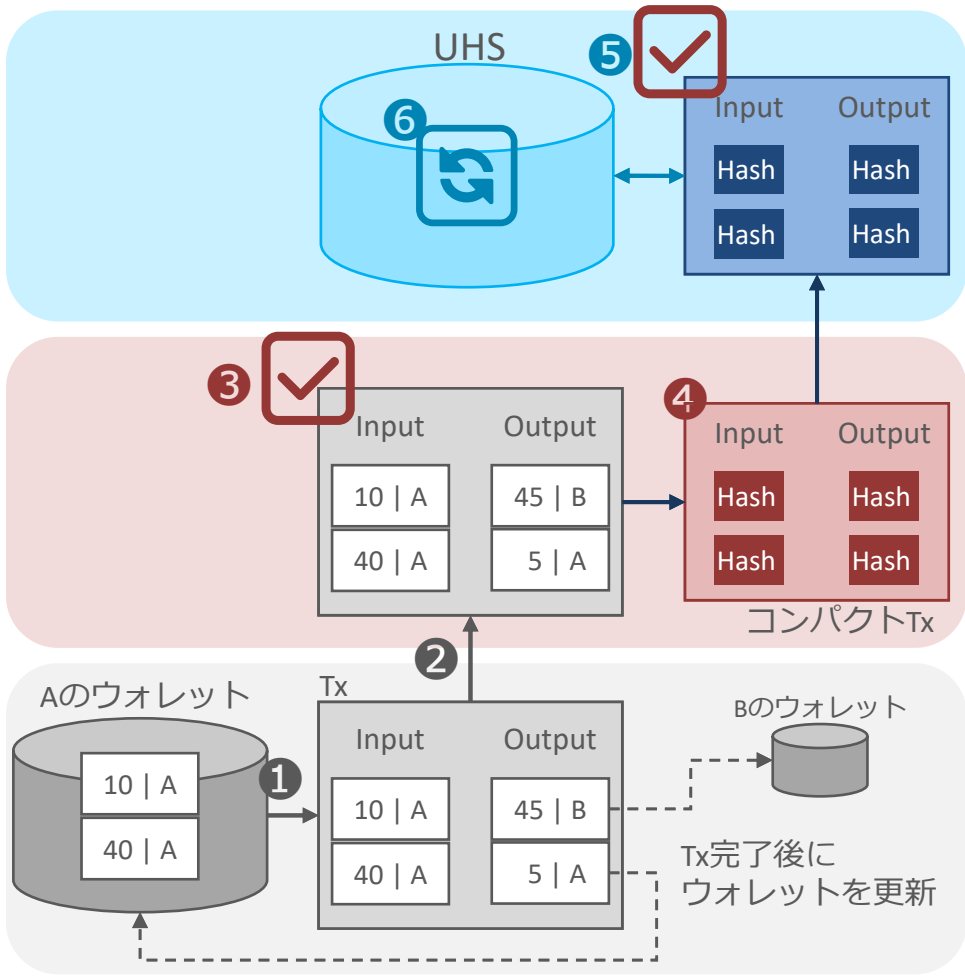
❺Sentinelから送信されたコンパクトTxの
存在性検証を実行
❻UHSを更新
※2種類の実装：Atomizer / 2PC

Sentinel

❸ユーザウォレットから送信されたTxの
ローカル検証を実行
❹TxをコンパクションしてUHSデータベースに送信
※ステートレスで動作 (永続的な情報の保持は行わない)

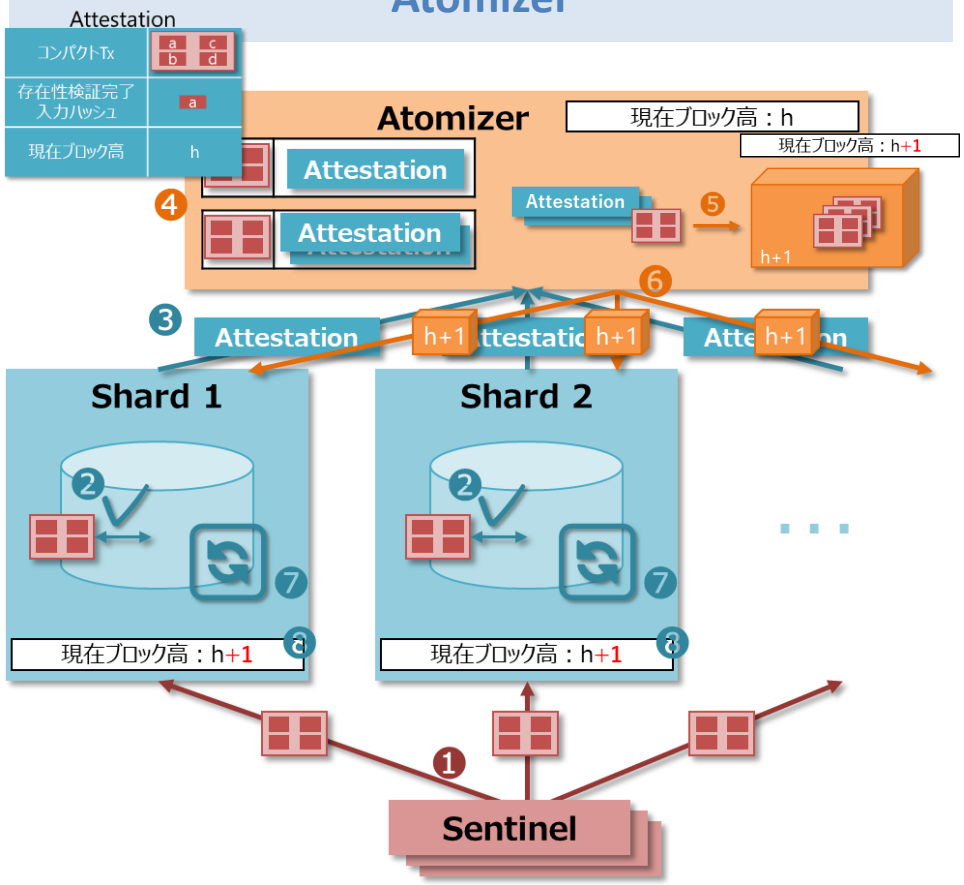
ユーザウォレット

❶所有するUTXOと秘密鍵を使ってTXを作成
❷作成したTxをSentinelに送信
※**所有者のデジタル通貨の実態 (UTXO) を唯一保持**



Project Hamilton Phase1の振り返り：DB設計

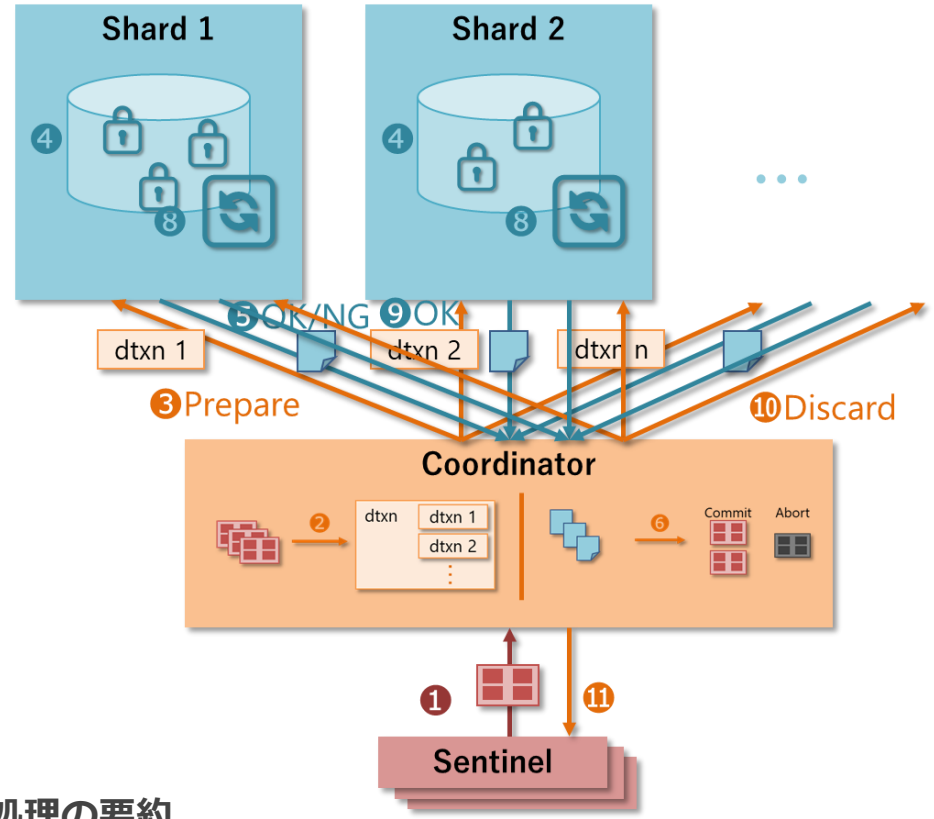
Atomizer



処理の要約

- **各Shard**がコンパクトTxを受信し担当範囲の検証
- **Atomizer**が検証結果(Attestation)を総括しブロックを生成
- **各Shard**がAtomizerから受け取ったブロックをもとにコミット（＋Archiver、 Watchtower）

2-phase commit (2PC)

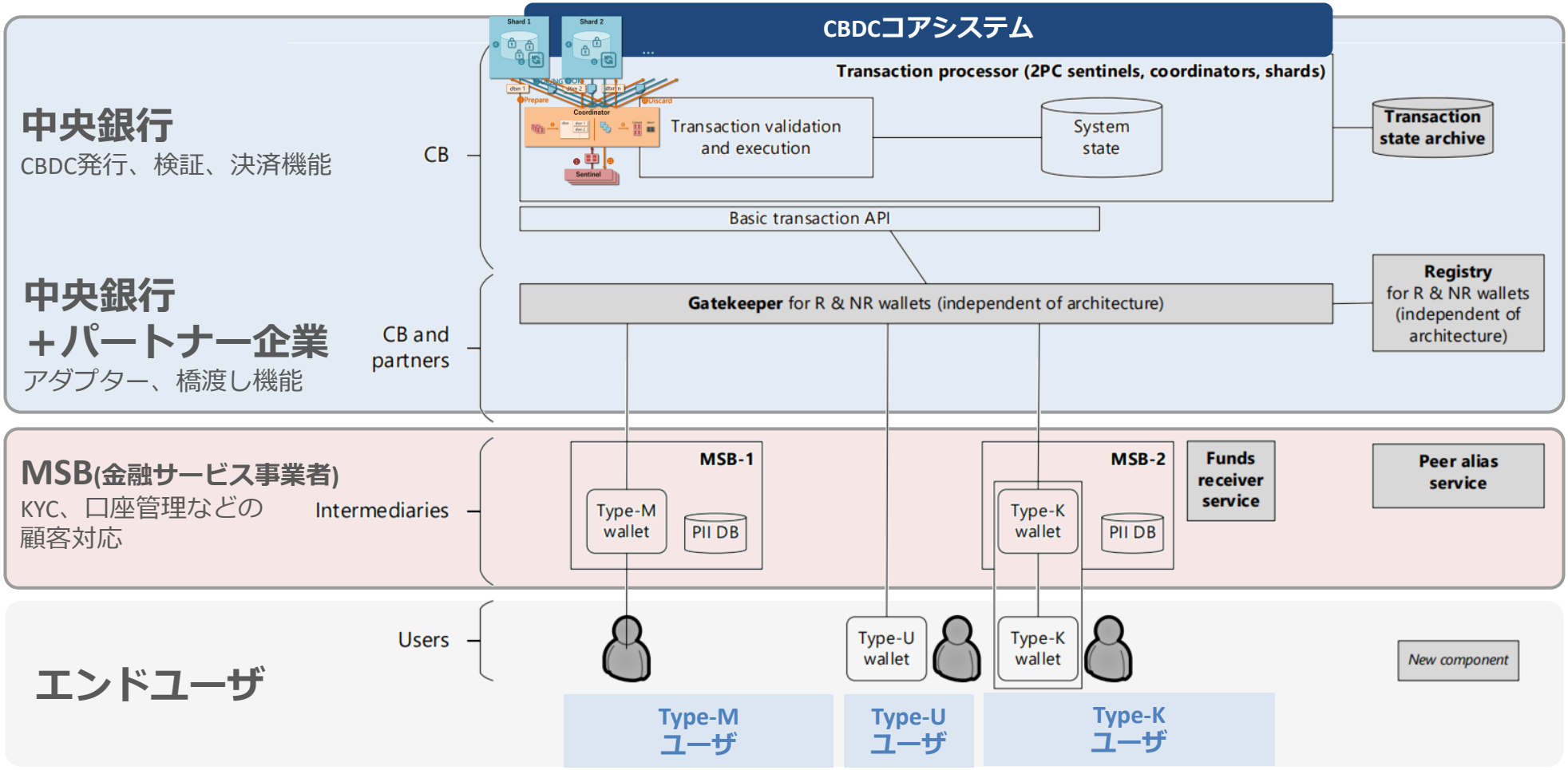


処理の要約

- **Coordinator**がコンパクトTxをまとめ、各シャード向けの分散Tx(dtxn)を作成
- **各Shard**が分散Txを受信し入出力ハッシュをロック
- **Coordinator**がロック可否を受信しコミットするTxを確定
- **各Shard**がコミットを実行しロック開放
- **Sentinel**がコミット結果を受信

アーキテクチャ全体像

- **Project Hamiltonの2PC**をトランザクションプロセッサとして採用
- 大きく中央銀行、MSB（金融サービス事業者）からなる**二層構造**を提案
  - MSB仲介の有無により多様なユーザ体系をサポート（下図Type-U/M/K）



※ユーザ、ウォレットの種類については後述

不正取引の防止

取引データの改ざん、不正取引の防止を行うため、Sentinelが複数の署名により連鎖的な確認を行う

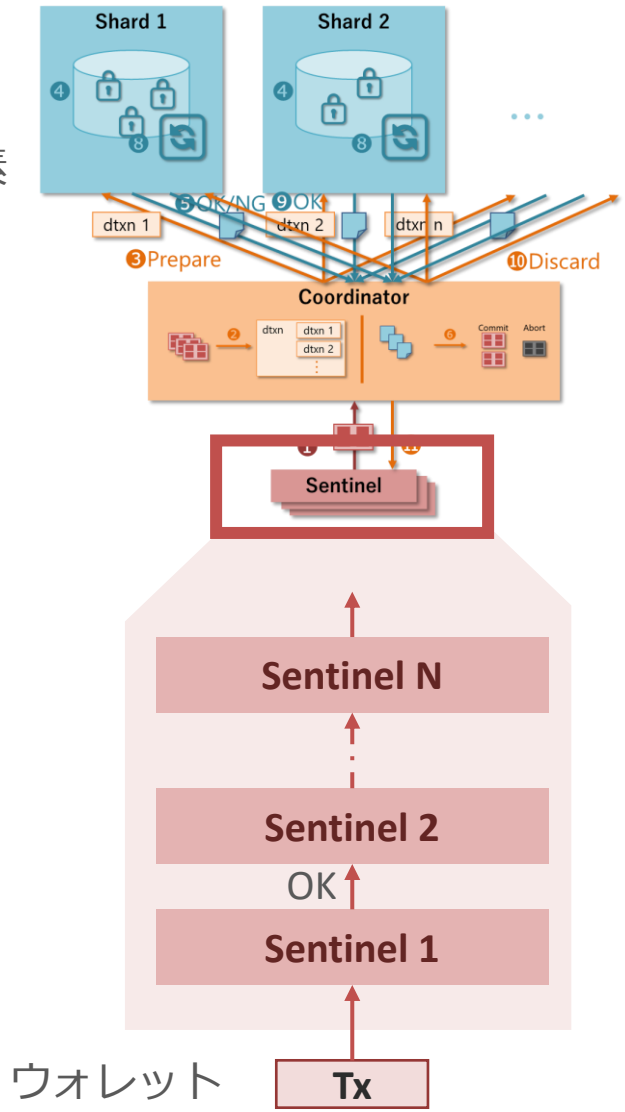
- SentinelはウォレットでTxを受け取る最初の部分であり、入出力の検証（ローカル検証）を行える唯一の構成要素
→ 確実な検証が必要

Sentinel認証の仕組み

- 各Sentinelが取引内容を検証、署名
- パラメータn（>0）：Sentinelの数
  - n=0：認証無効
  - n=1：Txを受け取る単体のSentinelが検証と署名を実施
  - n>1：複数Sentinelによる連鎖的な確認で冗長性・安全性を強化

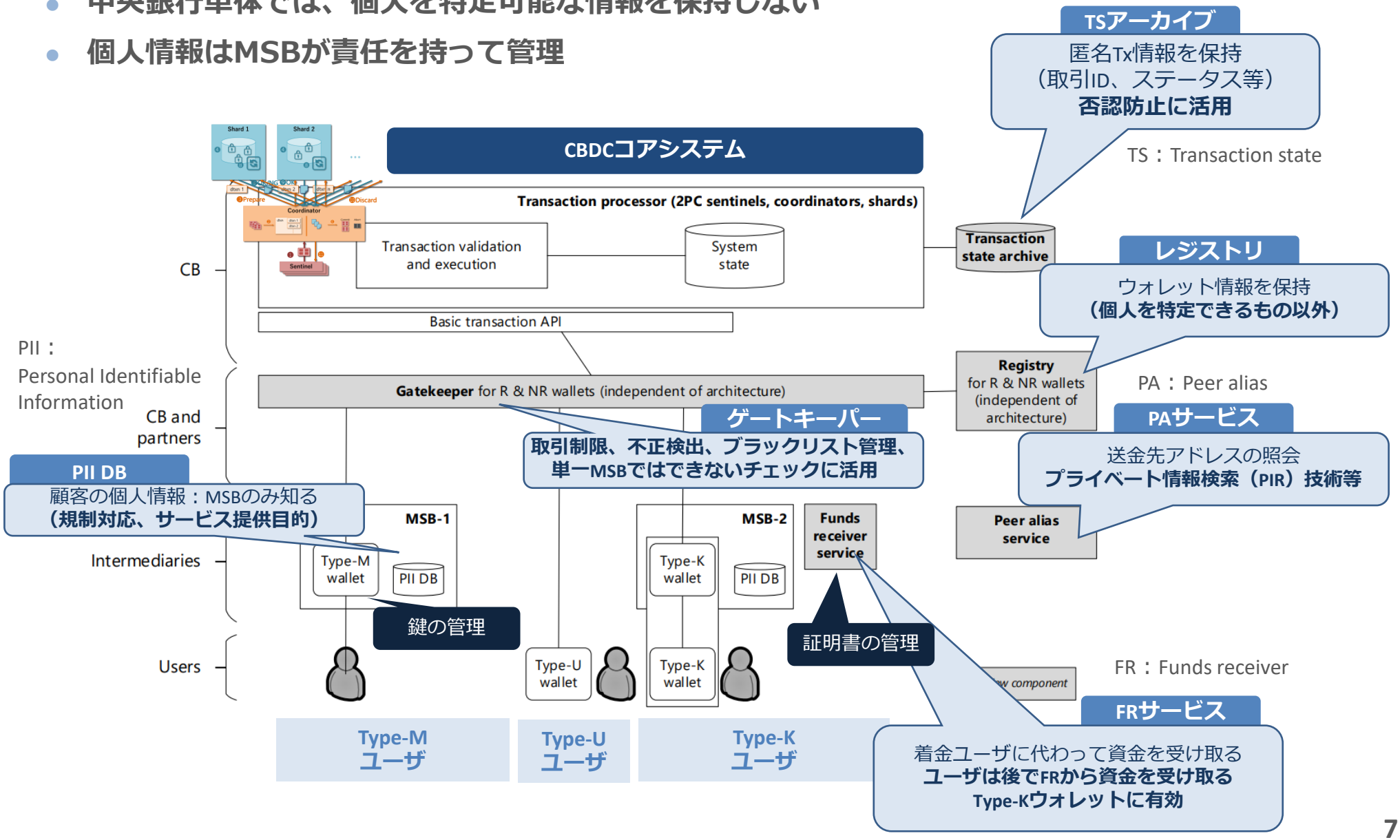
rCBDCのユースケースでは、セキュリティ上少なくともn=2以上

- Sentinelが攻撃を受けた際に不正にTxがコミットされることを防ぐためには、最低限２個のSentinelによる連鎖的な承認プロセスが必要



各構成要素の役割

- 中央銀行単体では、個人を特定可能な情報を保持しない
- 個人情報はMSBが責任を持って管理



サポートするウォレットの種類

Type-Uウォレット（セルフカストディ）

- **ユーザが資金と秘密鍵を完全に管理**
- **デバイス紛失時には資金も失われる**
- MSBの管理外となり**最高レベルのプライバシー**

高匿名性
高消失リスク

Type-Mウォレット

- **MSBが資金と秘密鍵を完全に管理**
- 端末紛失時もMSBのバックアップとリカバリで保護可能
- ユーザはMSBを信頼する必要がある（秘密鍵・資金管理）
- ユーザがMSB提供のインターフェイスにアクセスして利用

Type-Kウォレット

- **ユーザ**が秘密鍵を、**MSB**が資金を分割管理
- 両者の共同承認なしには支払い不可
- 端末紛失時も資金の実態は保護
- 支出権限はユーザが保持（秘密鍵）

共通事項

- 提案した構造であればこれら３タイプを同時にサポート可能
- **MSBは資金・Tx履歴・所有者情報を保持し、各種法令義務を履行**
  - 身元確認の規制がない場合、NR/SRユーザにもサービスを提供可能

（補足表）ユーザの種類

ユーザタイプ	
R（登録）	MSBにおいてKYC済みのユーザ
SR（準登録）	電話番号、メールアドレス等最低限のユーザ情報を登録したユーザ
NR（非登録）	匿名ユーザ

表. ウォレットの種類

ウォレット	秘密鍵	資金	Tx履歴	Rユーザ	NR/SRユーザ
U	ユーザ	ユーザ	ユーザ		●
M	MSB	MSB	MSB	●	●
K	ユーザ	MSB	MSB	●	●

流通金額監査の技術的実現性

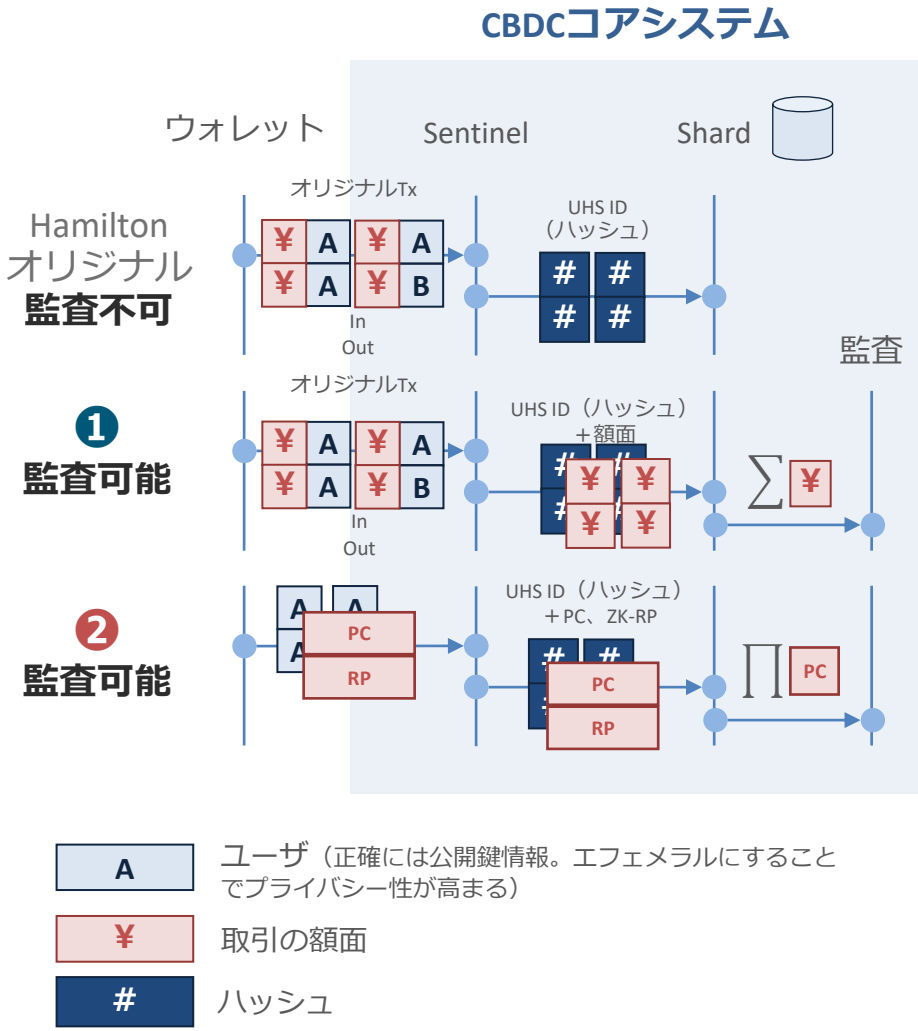
UHSに保存するデータのバリエーション

- Hamiltonオリジナル：<hash(UHS ID)>のみ保存（ベースライン）→**監査不可**
- ❶**Variant-values**：<hash(UHS ID), value>を保存。額面がそのままShardに保持される

暗号処理は不要で計算が単純だが
プライバシーが一部犠牲になる

- ❷**Variant-PPA**：<hash, Pedersen commitment(PC), range proof(RP)>を保存。
  - 数学的な暗号技術・証明技術を活用
  - PC：Txプリイメージ（資金実態データ）から計算し金額を隠すことが可能
  - RP：PCから計算。不正な資金（負値あるいは巨大な値）を防止する。

計算コスト・ストレージ占有量を犠牲にして
プライバシー保護を強化



PPA：Privacy-preserving audit (プライバシー保護監査)
Pedersen Commitment: **入出力の合計が一致することを保証**（金額は隠蔽）
Range Proof: **値が0 ≦ v ＜ 2^nであることを保証（ゼロ知識証明で担保）**

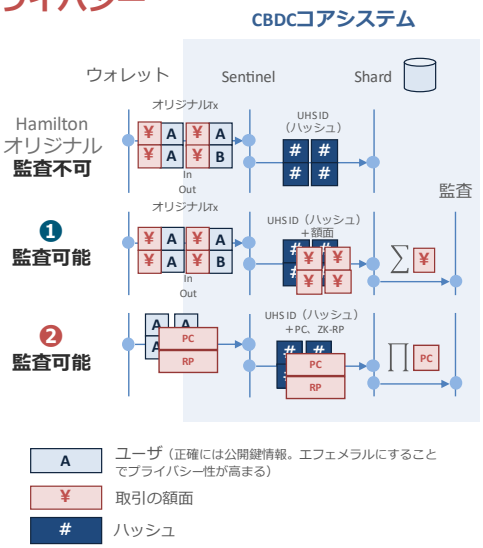
プライバシー

- **匿名性を重視したID設計**：ユーザ情報（PII）は、Txに暗号識別子を使うことで切り離される
- **コアにおけるデータの最小化**：Sentinel、Coordinator、Shardは非PIIデータしかアクセスできない
- **一度きりの使い切り鍵を採用**：プライバシー保護を強化
- **セルフカストディ型ウォレット**（Type-Uウォレット）のサポート：特にNRユーザの高プライバシーを保証
- **PPAによる金額の秘匿化**：ベースライン以上のプライバシーを実現（下図赤枠）
- **プライバシー・バイ・デザイン**：補完的なコンポーネント（ゲートキーパー、TSアーカイブ、レジストリ）が連携し、最小限かつ秘匿性を担保する形でデータを保管する設計

高プライバシー

3：可視性なし・保存不要
2：可視性あり・保存不要
1：可視性あり・要保存

低プライバシー



ベースライン：**額面の可視性を持っているが保存はされない** → 2
Variant-values：**額面の可視性を持ち、UHSに保存される** → 1
Variant-PPA：**額面はCBから一切見えず、保存もされない** → 3

Table 5: OpenCBDC 2PC visibility ratings for the three var

Solution	Wallet type	Central bank					Payer MSB					Payee MSB				
		H		T			H		T			H		T		
		O	B	S	R	A	O	B	S	R	A	O	B	S	R	A
OpenCBDC 2PC baseline variant	U	3	3	2	2	2	3	3	3	3	3	3	3	3	3	3
	K/M	3	3	2	2	2	1	1	1	1	1	1	1	1	1	1
OpenCBDC Variant-values ❶	U	3	3	2	2	1	3	3	3	3	3	3	3	3	3	3
	K/M	3	3	2	2	1	1	1	1	1	1	1	1	1	1	1
OpenCBDC Variant-PPA ❷	U	3	3	2	2	3	3	3	3	3	3	3	3	3	3	3
	K/M	3	3	2	2	3	1	1	1	1	1	1	1	1	1	1
Cash		3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

Note: MSB is money services business. H means users' holdings, and T means transactions. O is the owner, B is the balance, S is the sender, R is the receiver and A is the data amount. A rating of 3 indicates the entity has no visibility and stores no data, rating 2 indicates the entity has visibility but has no storage requirement and rating 1 indicates both visibility and storage are required.

スケーラビリティ

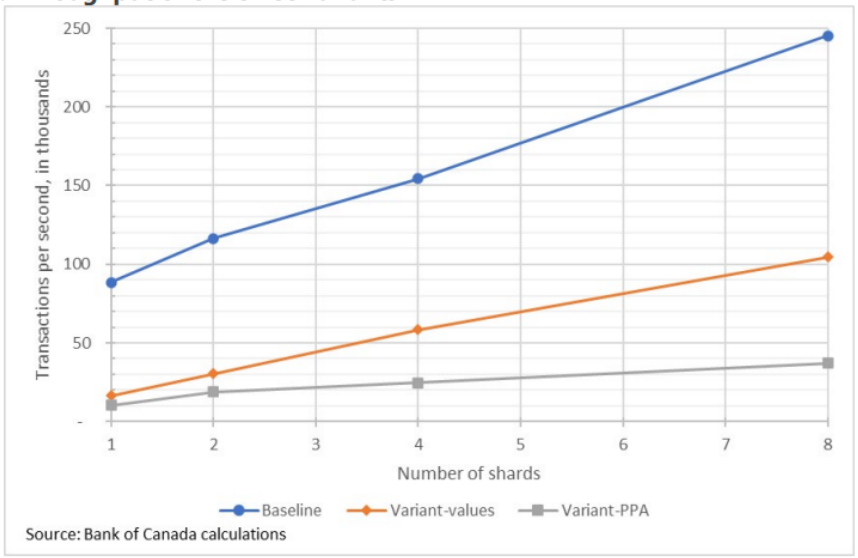
実験条件

- ３つのバリエーション比較：Baseline（Hamiltonオリジナル・監査なし）、Variant-values（額面の平文保存による監査）、Variant-PPA（暗号技術の活用によるプライバシー保護監査）
- 実験対象：**ウォレット間の資金移動は含まず、コアシステム内の決済処理に限る**

スケーラビリティの実験結果（TPS vs Shard数）

- Baseline：1～8で線形にスケーリング。最大**約250,000TPS**達成
- Variant-values：監査処理によってスループットが低下したが、ほぼ線形
- Variant-PPA：最低でも10,000TPSを達成したが、**暗号演算の負荷が高く、スケーラビリティが不十分。線形とはほど遠い**

Chart 2: Throughput of the three variants



レイテンシー

実験条件

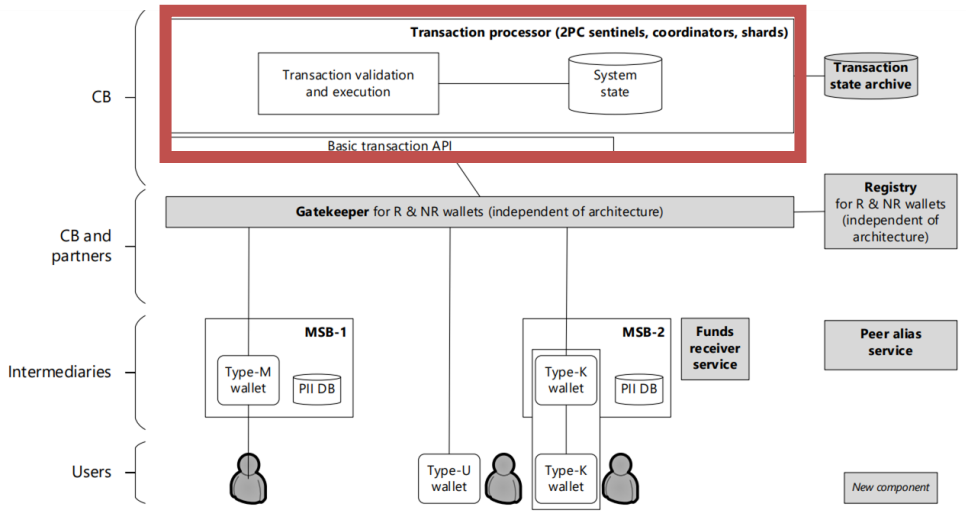
- **Txがコアシステムに提出された時間を起点とし、更新が完了するまでの時間（下図赤枠）**
  - **ウォレット間の資金移動を含んでいないことに注意**

実験結果

- **レイテンシ平均：**プライバシー保護技術有無によらず**数百ミリ秒**（～1秒）付近で推移
- **99p（パーセンタイル）最大：4.3秒**　（サンプルを小さい順に並べた際99%にあたる値。統計学的には、「残り１％＝例外として考えた場合、現実的に普段起こりえる値」と解釈できる）

→ リテール決済における許容範囲目安（平均：1秒未満、99p：5秒未満）に収まっていると主張

- しかし特に計算負荷の高いPPA、Sentinel認証を導入するほど顕著に性能が低下する傾向



コンプライアンス・法令遵守

各MSBは、ユーザデータ管理とAML/CFT 法に準拠したコンプライアンス確保の責任を負う

ユーザのオンボーディング

- 二層モデルにおいては**MSBがKYCの設計を行い、コンプライアンス確保の全責任を負う**
  - 既存のKYCサービスを利用しても自社で開発してもよいが、新規顧客獲得には利便性が重要
- Type-UウォレットをもつNRユーザは、MSBにID情報を提供することなくウォレットを取得

ルールに基づいたコンプライアンス

- **具体的な振る舞いや行動**を記述したルールに基づく (**プロセス**重視)
  - 例：１万ドルを超える取引は当局に報告が必要
- Type-M/KウォレットをもつRユーザのルール違反があった場合には、トランザクションとIDを確認できる**MSBが当局に報告する責任を持つ**（CBはこれらのデータにアクセスできない）
- ルールに反するNRユーザからのトランザクションは、トランザクションプロセッサへの提出前にゲートキーパーが拒絶

原則に基づいたコンプライアンス

- 具体的な振る舞いや行動を指定せずに、行動や意思決定のもととなる**目的自体を重視** (**結果**重視)
- パターンや異常性に基づいて疑わしい取引を検知するために、**機械学習モデルなどの技術も利用可能**
  - MSBが管理する過去の取引データを分析に利用することで、不正な取引の傾向やパターンを検出
  - 潜在的なリスクや不正行為をリアルタイムで特定し、迅速かつ適切な対応が可能
- Type-Uウォレットを持つNRユーザには、原則に基づいたコンプライアンスを適用不可

回復力（レジリエンス）

資金とウォレットの回復力

- Type-M/Kウォレットの資金を管理するMSBは、
  顧客のウォレットを保護するためにバックアップや復元の仕組みを導入すると見込まれる
- Type-Uウォレットの資金はユーザが管理し、自身で紛失を防がなければならない
  - スマホ向けウォレットアプリベンダは、**ユーザ自身のクラウドアカウントへの暗号化バックアップ機能**を提供可能
  - 資金と支出キーを異なる場所にバックアップすることで、資金盗難リスクを最小化

システム障害からの回復力

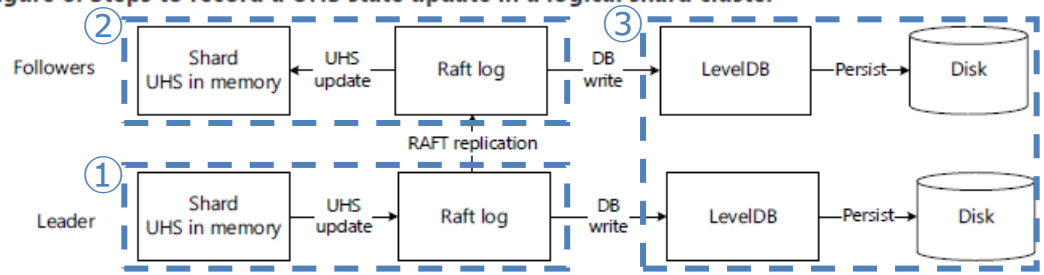
① UHSをディスクではなく、高速に更新できる**Shardインスタンスのメモリ上**に保持

② 論理ShardクラスタへのUHSの同期
  - リーダーShardからフォロワーShardへRaftログを複製し、インメモリUHSを同期
  - この時点で決済完了とみなされる

③ 各ShardのDBへ書き込み（永続化）

- 部分的/完全なシステム停止からの復旧

Figure 8: Steps to record a UHS state update in a logical shard cluster



Note: UHS is the hash set of all unspent transaction outputs. Raft is a replication protocol, and LevelDB is a database.

この間には新規のトランザクションを
受け付けられない時間あり（要再送）

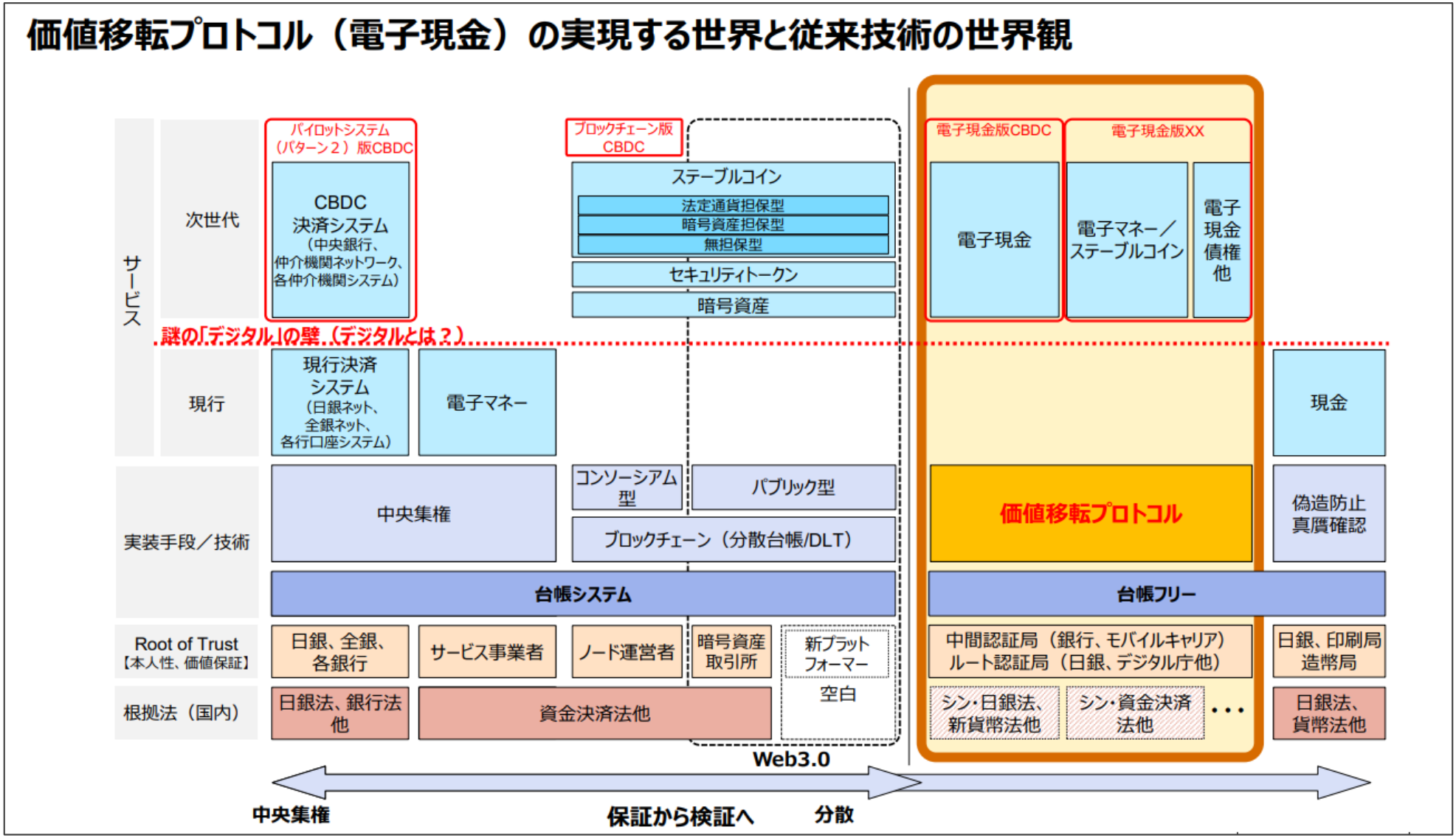
	RPO（目標復旧時点）	RTO（目標復旧時間）
部分的なシステム停止	0 (状態を失うことなく回復)	数秒から数分程度
完全なシステム停止	ディスク書き込み待ちの状態が失われる恐れあり	上限なく増加（スナップショットの取得で短縮可能）

留意点、示唆

- 留意点
  - 性能テストの測定範囲はコアシステム内のみ。各種制限処理は想定されていない（UTXOの並列処理性は、各種制限処理が想定されると低下する可能性）。
  - 匿名性と消失リスクの存在、一つの対応策としての仲介機関の関与。
  - 具体的なエラーハンドリングの定義や対処法は明示されていない。店舗目線として、対応するPOS端末の導入・開発コスト、既存リテールインフラとの統合の仕方は考慮されていない。

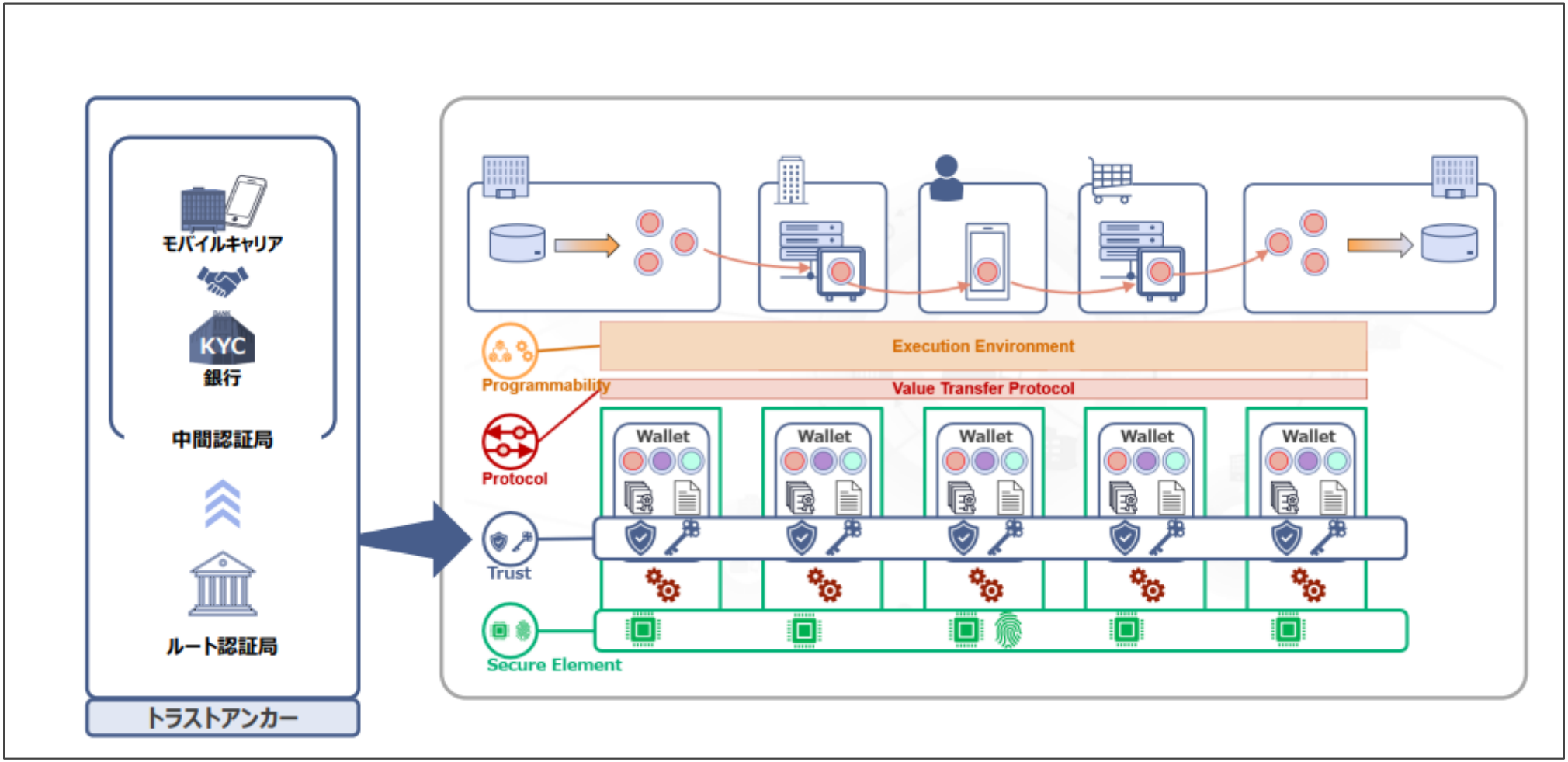
- 示唆
  - 大胆なコンセプトから出発しているデザインだが、TradFiで必要とされる機能や既存システムとの連携を検討していくと、既存システムと似たようなシステム対応が必要となってくる？
  - WG4で紹介のあった価値移転プロトコルの発想と近い？
  - WG4で紹介のあったデジタル通貨のUXの観点からみると現金型に近い？

（参考）これまでの関連する議論の振り返り（第１０回会合より）



（出所）CBDCフォーラムWG4 第10回会合資料（株式会社NTTデータ様）より抜粋

（参考）これまでの関連する議論の振り返り（第１０回会合より）



（出所）CBDCフォーラムWG4 第10回会合資料（株式会社NTTデータ様）より抜粋

（参考）これまでの関連する議論の振り返り（第１１回会合より）

現金・預金によるUXとデジタル通貨への示唆

- 対面で日本銀行券を利用する「現金」と日銀当座預金を基礎として市中銀行の「預金」が一般利用者の「通貨」
- さらに決済手段として資金移動業資金や前払式決済手段、さらには電子決済手段などが取扱われている。

現金型

対面・台帳レス（現金その場限り）
匿名あるいは利用者を制限しない
券面の信用は保証されていて、どこでも使える。
→仕組は用意をされていて、信用の上に成立。

預金型

非対面利用も可。
利用に当たって登録（KYC）が必要。（一部除）
一般的に台帳はサービス提供者が個別管理。
→ネットワーク間の連携は課題（⇒オープンバンキングの議論）

デジタル通貨の導入での期待

誰でも、簡単に利用できる決済手段
→ICカード等をかざすだけで利用できる、等
個人間で、なるべく環境に依存せず利用できる
P2Pでもコミュニケーションのお作法はみんな同じ

共通のプロトコル（interoperability）
→効率化した処理の実装。
→どのプロトコルにするかの論争
各種サービスと効率的に結合ができる（composability）
→コミュニケーションのレールに組込める

（出所）CBDCフォーラムWG2・WG4共同開催会合資料（三井住友信託銀行株式会社様）より抜粋

（参考）これまでの関連する議論の振り返り（第１１回会合より）

AIエージェントとおカネ

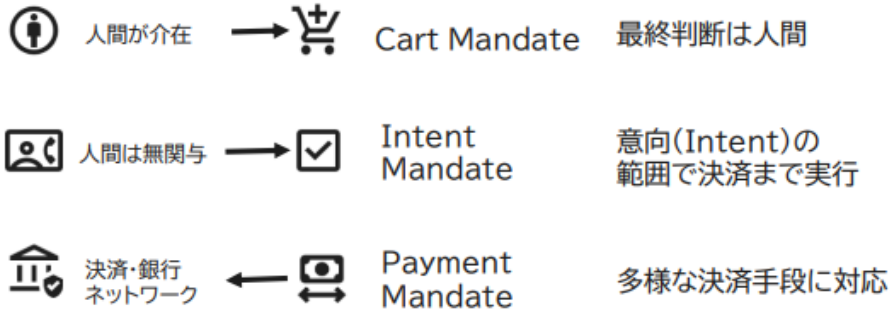
- AI活用の拡大ペースはとても早く、情報分析・資料作成だけでなく一定の裁量の下で利用されるエージェントも出現。
- AIエージェントが商取引を行う際には資金決済を手当てする必要があり、APIなどで金融機関にアクセスなどを利用。
- Googleからは”Agent Payment Protocol”が公表されており、裁量（＝ユーザーの意向、intent）は暗号学的に検証が可能なVCとして与えられ、その裁量の範囲でAIエージェントが取引を進める。
- 但し、「人間と同じ」設計である必要あるか？AIにとって現金相当な仕組みはありえるのか？

情報収集⇒分析⇒決済まで人の介在なく実行

決済手段は人間と共通であり続けるべき？

筆者作成

Google：Agent Payment Protocol



出所：The Agent Factory - Episode 8: Agent payments, can you do my shopping? の図表の拙訳

（出所）CBDCフォーラムWG2・WG4共同開催会合資料（三井住友信託銀行株式会社様）より抜粋

ディスカッションポイント

CBDCの将来的なデザインの可能性
―新たなテクノロジーの活用に向けて―

- **将来的なアーキテクチャの可能性**
  - ✓ 台帳の分散化、台帳フリー
  - ✓ プライバシー、コントローラビリティ
  - ✓ 標準化、プログラマビリティ
  - ✓ 既存システムとの連携

- **AIエージェントの活用可能性**
  - ✓ 将来的なアーキテクチャとの組み合わせ
  - ✓ 適している領域、留意点