

UTXOモデルの将来

生永 雄輔

2024年3月13日

UTXOモデルの適用

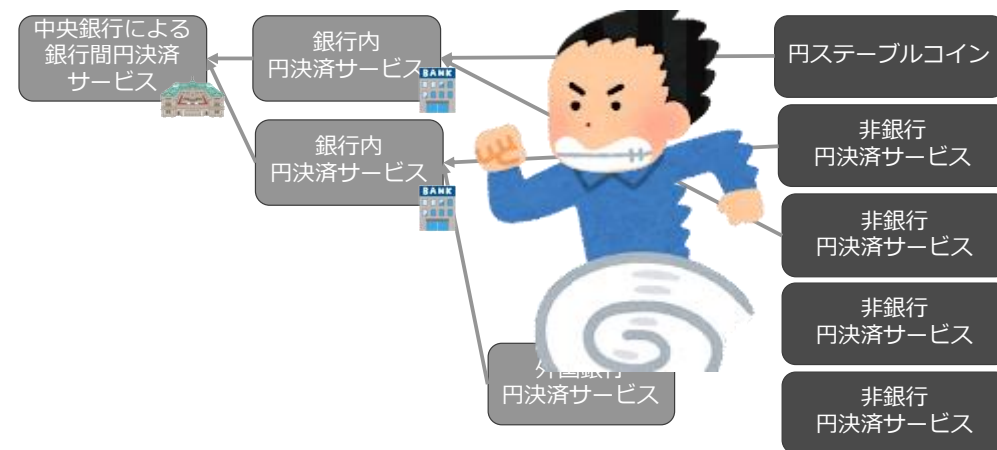
- 1 Layer1ーCBDCモデル
- 2 オフライン決済
- 3 フルCBDC

蛸壺化を避けるには？

Discussion Purpose Only

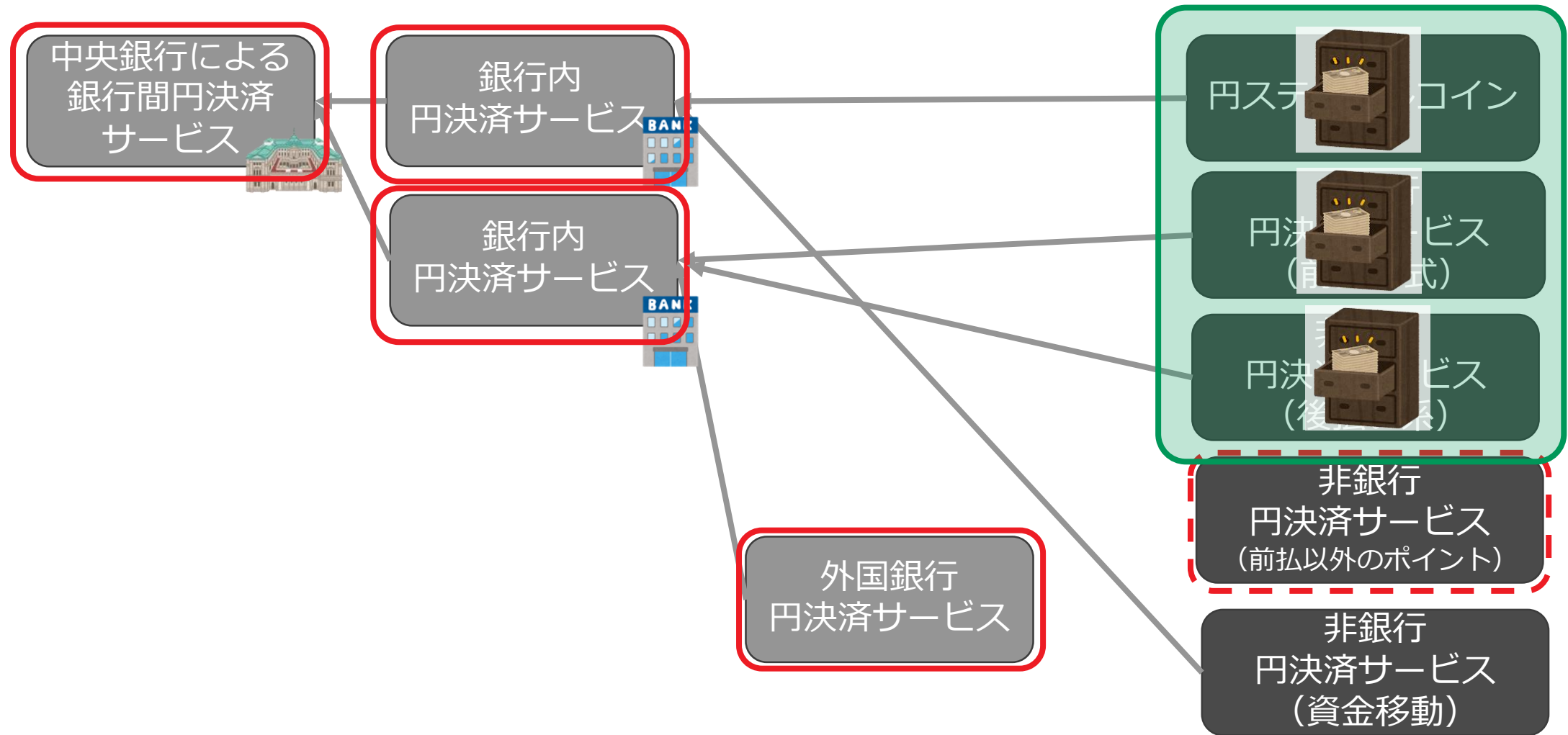
- ✕ 決済サービスが（流動性を提供する）銀行になる・・・
- ✓ 非現実的では・・・

○ 蛸壺間の資金移動を高速化



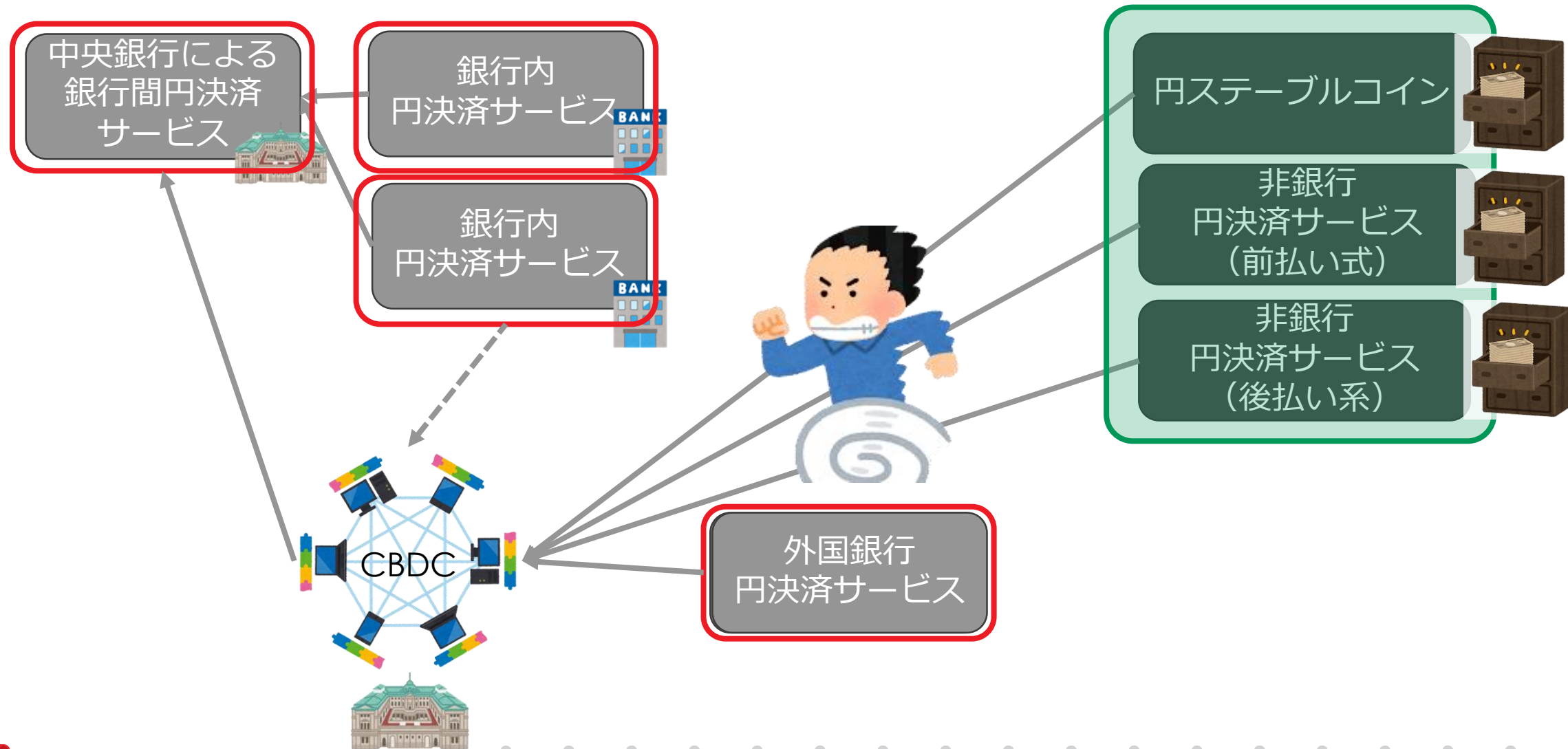
Layer1—CBDC

Discussion Purpose Only



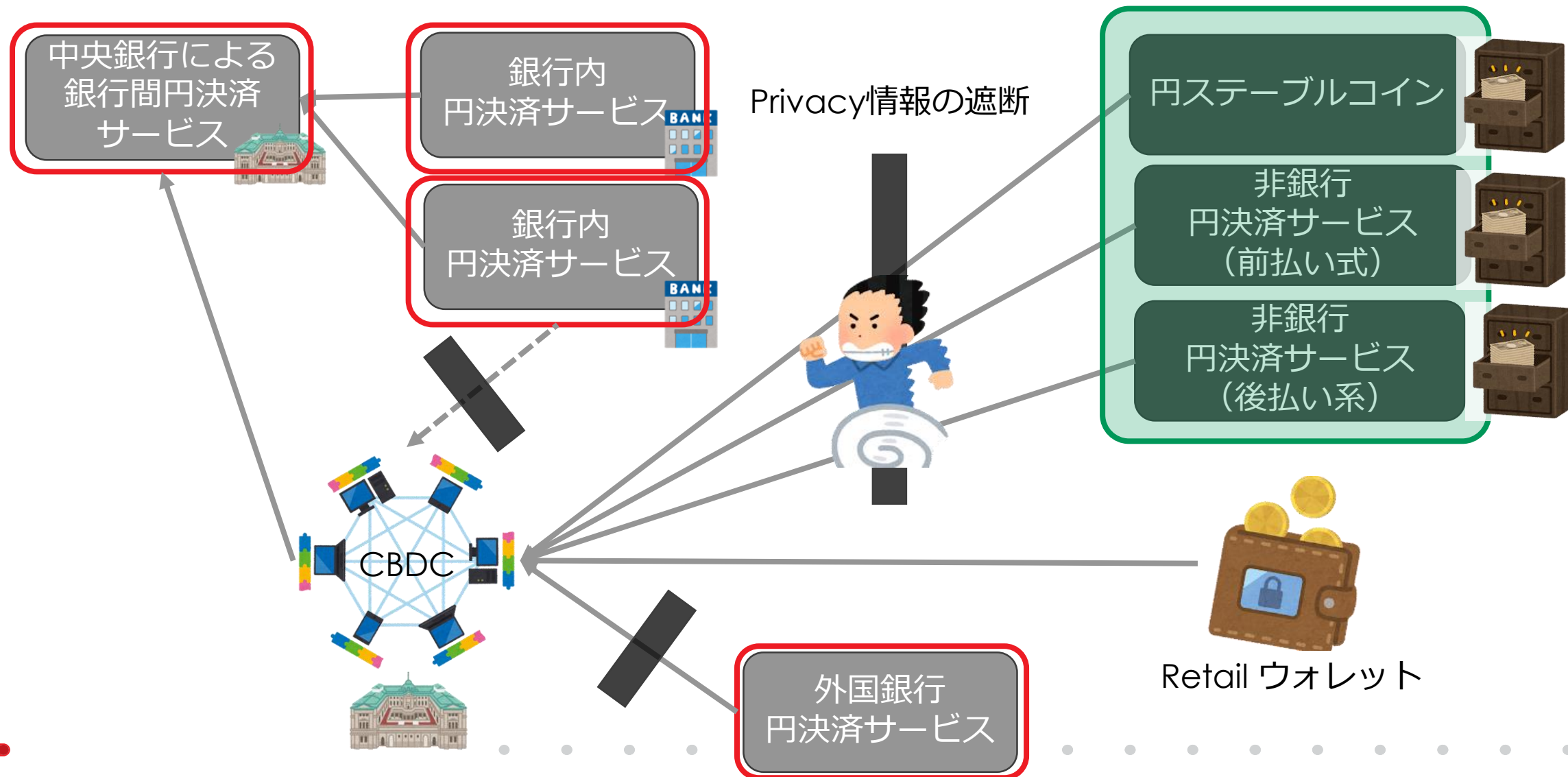
Layer1—CBDC

Discussion Purpose Only



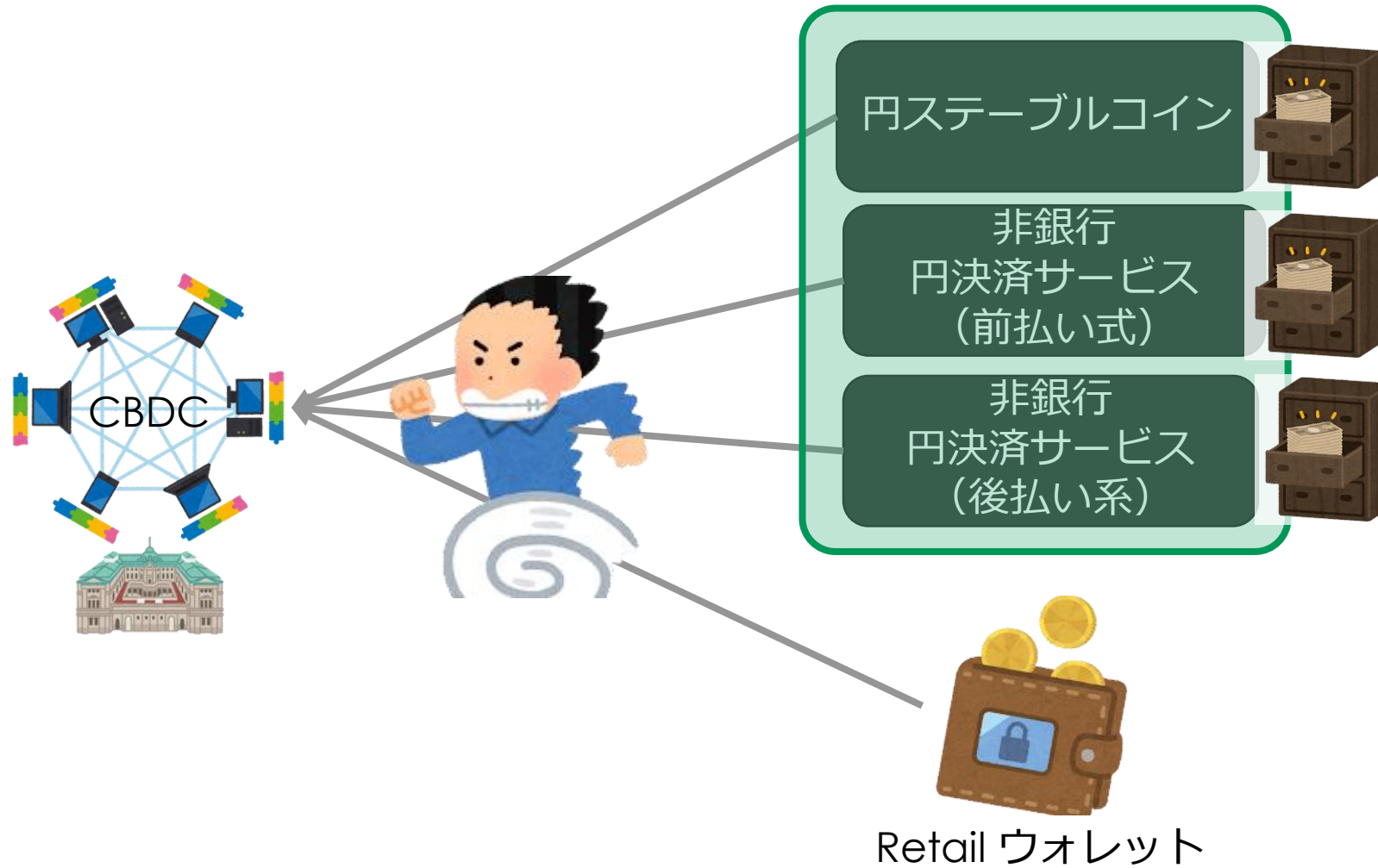
Layer1—CBDC

Discussion Purpose Only



Layer1-CBDCとパフォーマンス

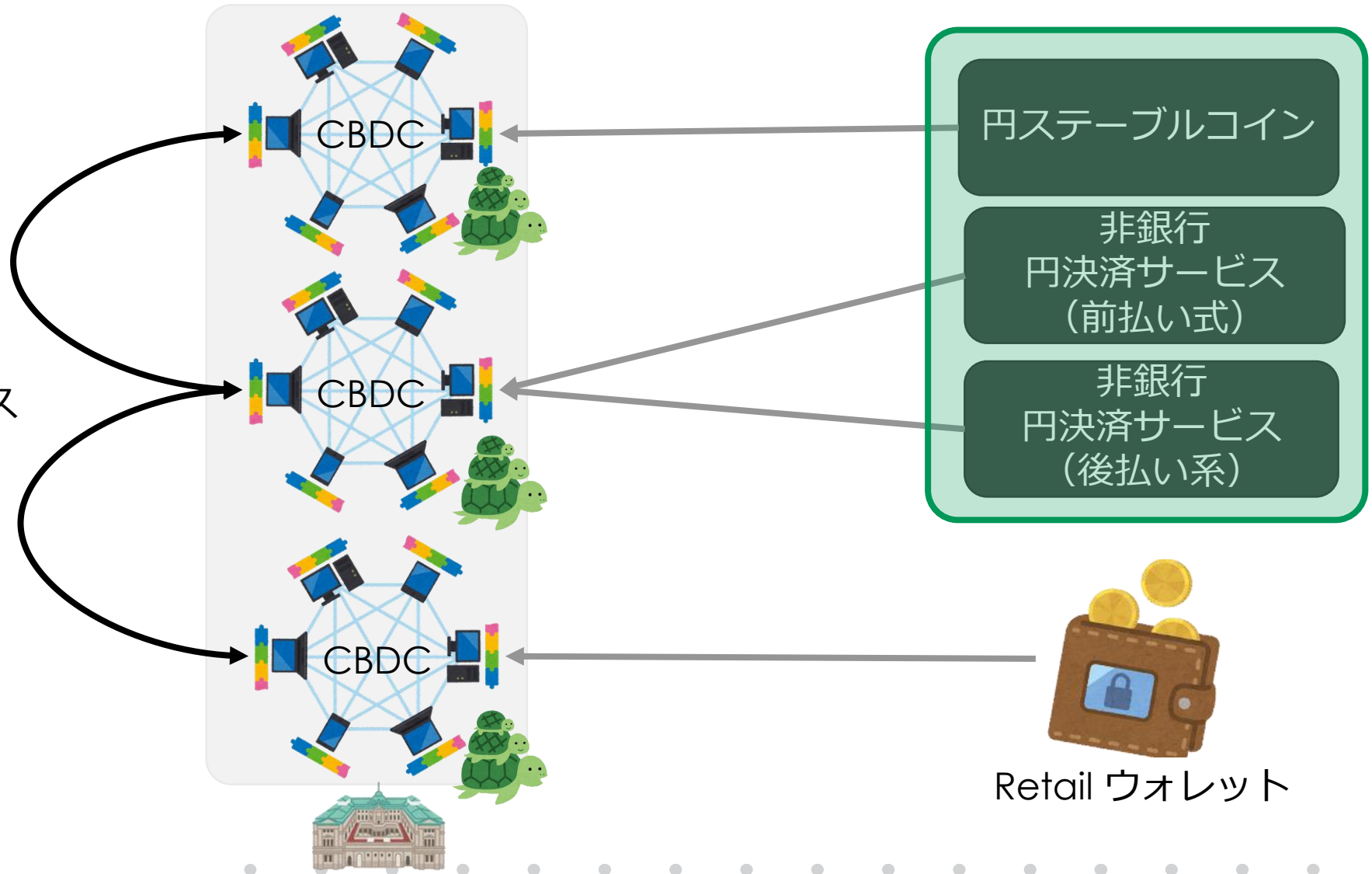
Discussion Purpose Only



Layer1-CBDCとパフォーマンス

Discussion Purpose Only

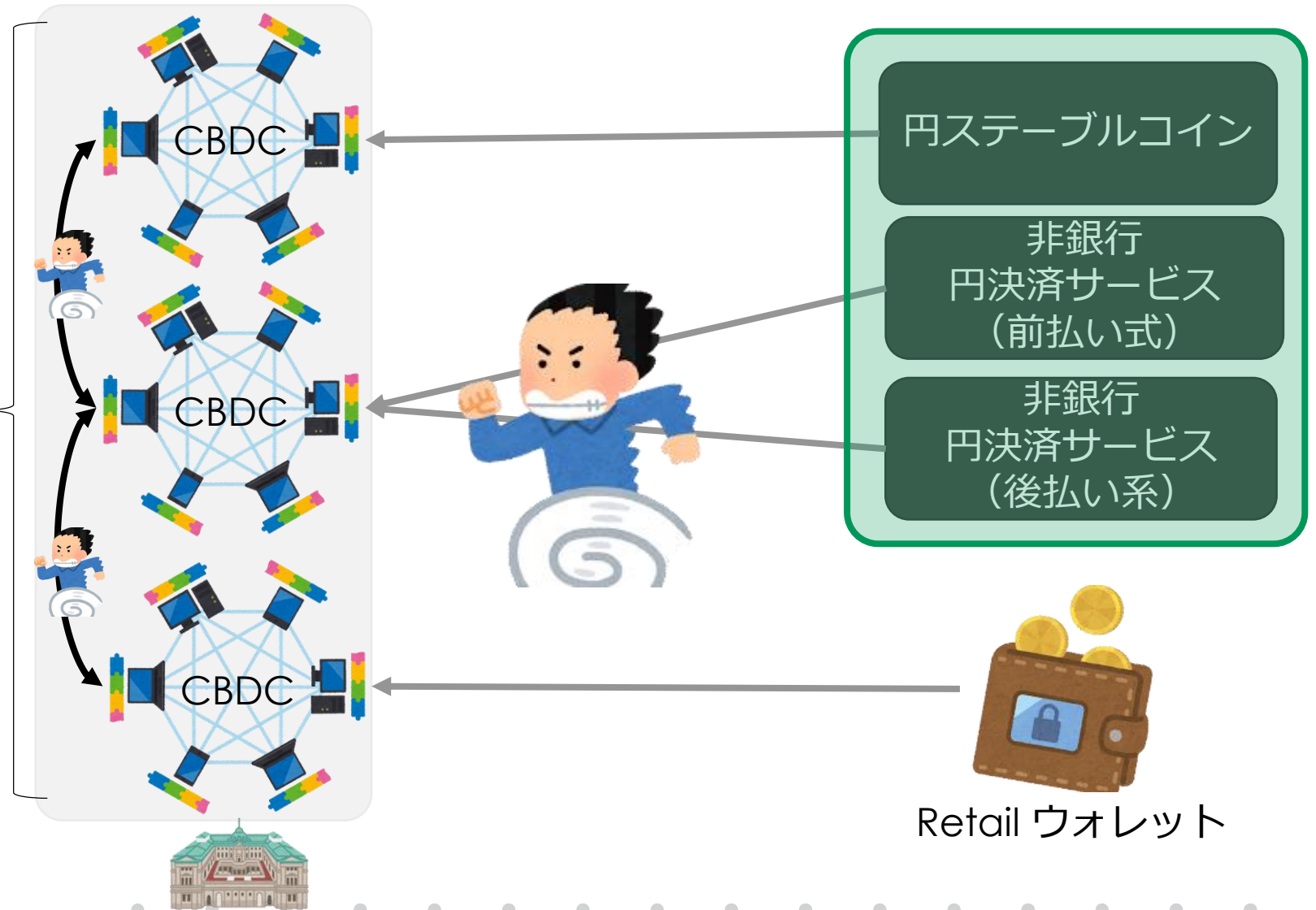
CBDCネットワークを複数個
用意することでパフォーマンス
向上は可能



Layer1-CBDCとパフォーマンス

Discussion Purpose Only

- ✓ CBDCは複数ネットワーク構成にすることも可能。
- ✓ 例えばトータル100万TPS必要
→
50個のネットワークなら
2万TPSを目指せばいい



Layer1-CBDCとパフォーマンス

Discussion Purpose Only

技術上の課題は

○単体のパフォーマンス

◎シャーディングのフィージビリティ

◎インターオペラビリティ

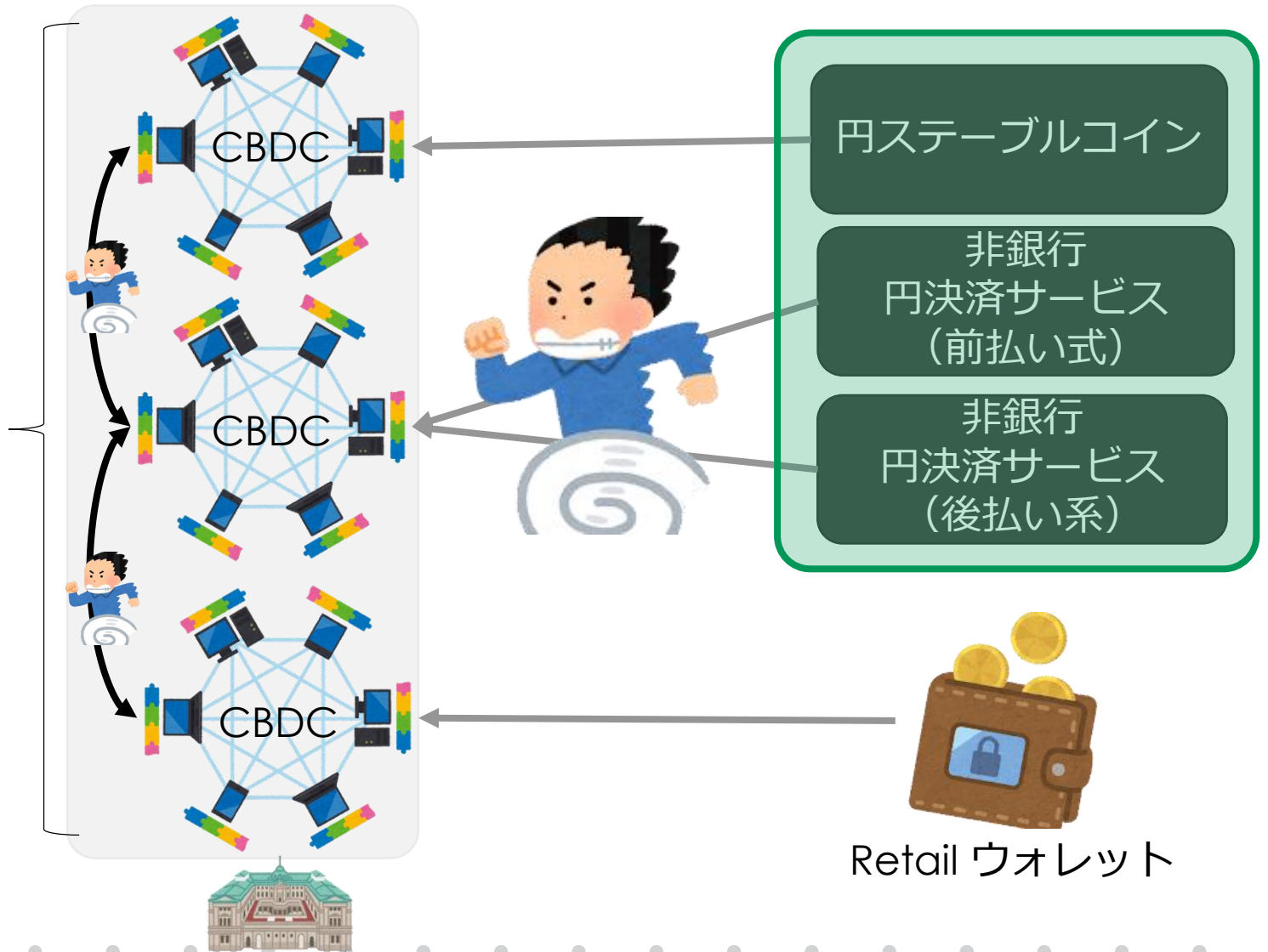
(ISO20022, Hyperledger Harmonia)

◎ネットワークを超えたIDの同定

(DID/VC等)

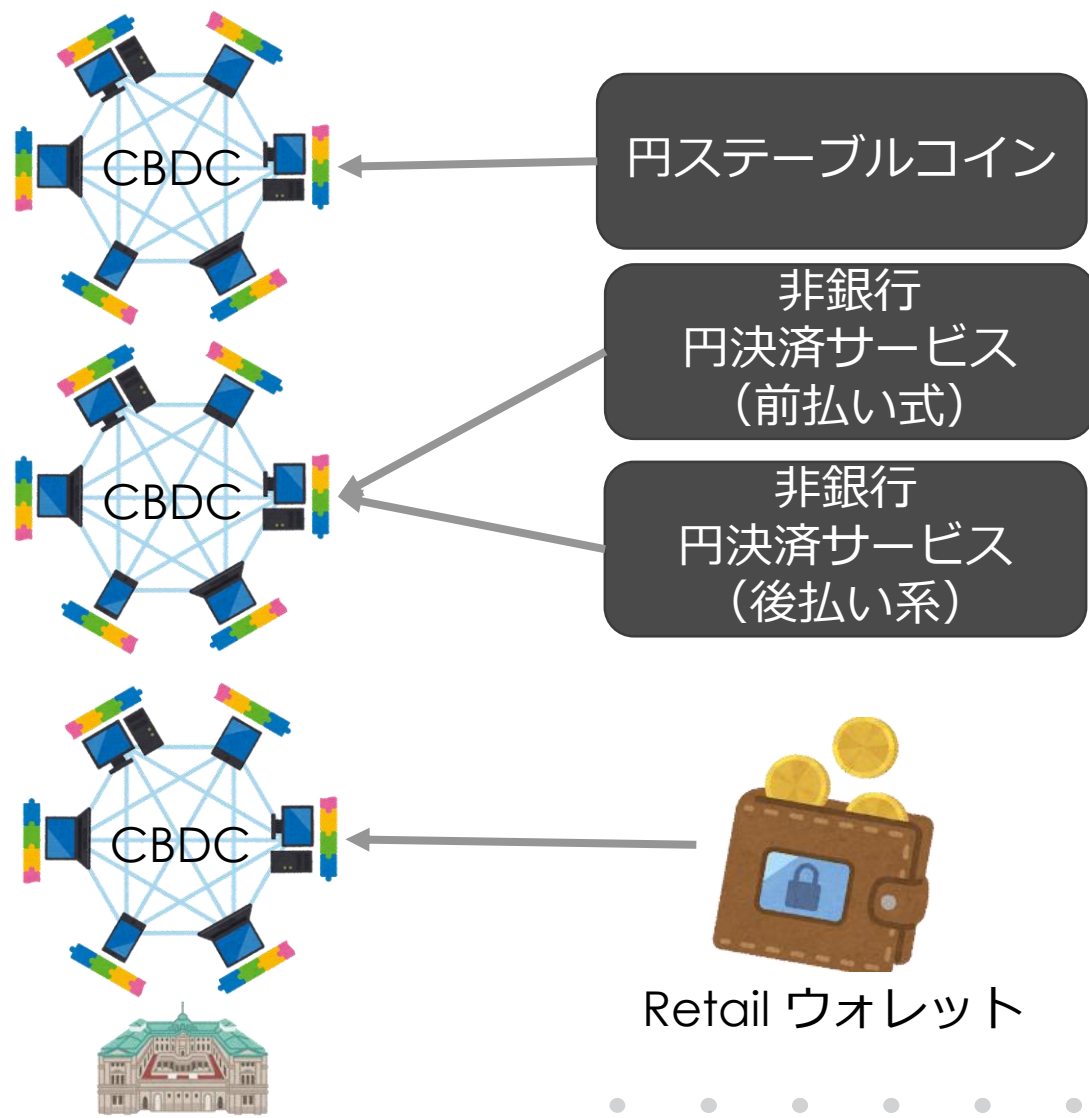
○Layer 2 技術

(トラストレスの必要性はない)



Layer1-CBDCにおけるUTXOの使い道

Discussion Purpose Only



使用しているデータモデル



バランスモデル



トークンモデル



UTXOモデル

UTXOモデルは柔軟性が高い

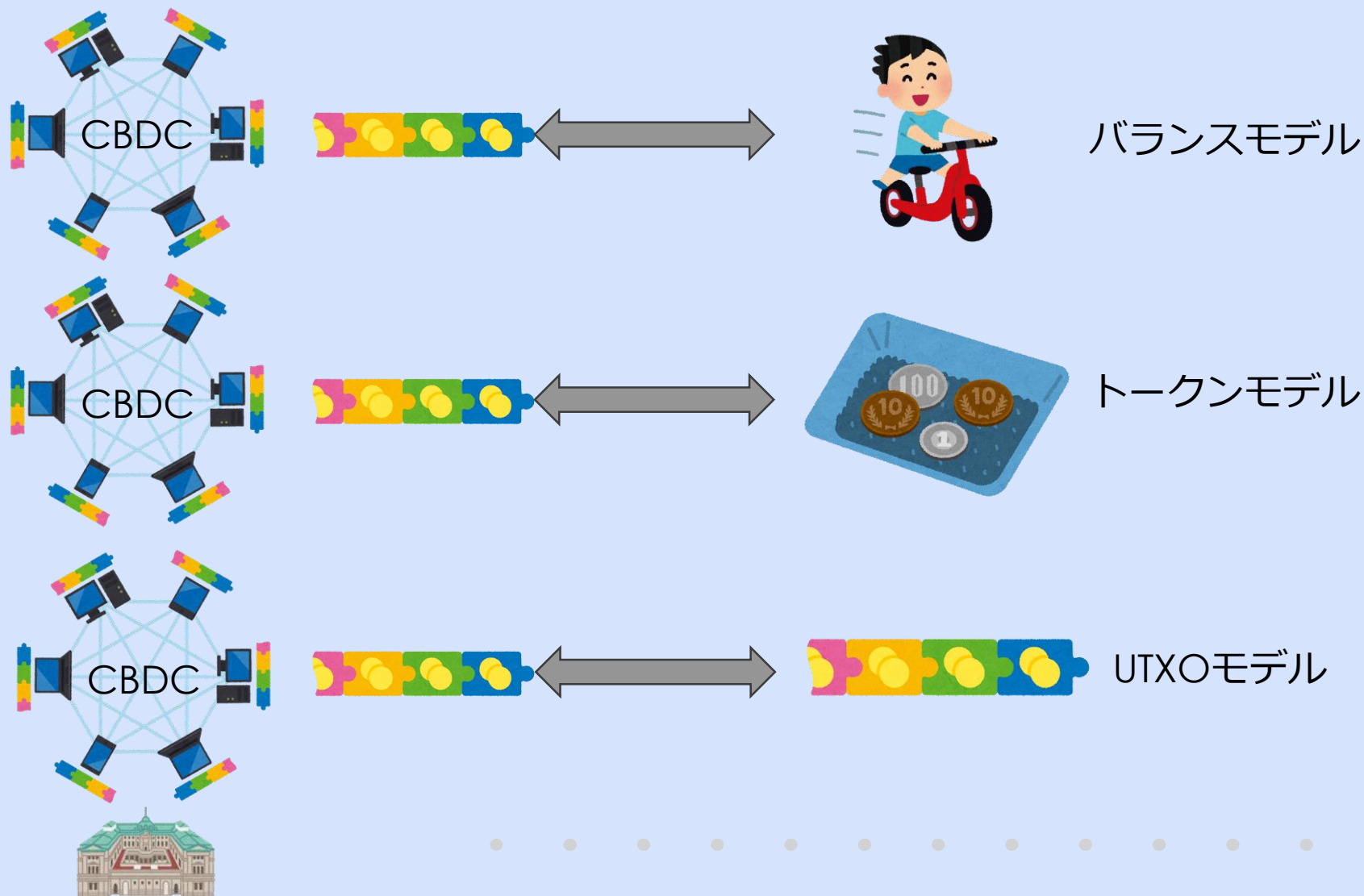
Discussion Purpose Only

モデル名	長所	短所
バランスモデル 	- 金額によってデータ量が増えない - 主体別残高を計算する必要がない - エンジニアにとって理解が容易	- 二人と同時に取引できない - 取引相手に残高が見える
トークンモデル 	- 複数の人と同時に取引できる - 取引相手に自分の残高が見えない - ユーザーにとって理解が容易	- 金額が増えるとデータ量が増える - 主体別残高計算が大変
UTXOモデル 	- 設計次第でバランスモデルにもトークンモデルにも変化可能 - データ量の圧縮可能 - 主体別残高の秘匿可能 - 複数人の同時取引可能	柔軟な為、理解が難しい

[アイデア]

UTXOモデルの柔軟性が簡便なインターオペラビリティ実現につながる可能性

Discussion Purpose Only



Layer1-CBDCについてのまとめ

Discussion Purpose Only

- 流動性の移動速度向上を目的として、CBDCを活用できるかもしれない
 - ✓ 関連事例：国債のトークン化（参考資料）
- 多数の基盤と接続する際に、UTXOのデータモデルの柔軟性が使える
- パフォーマンスの向上にはシャーディング等の技術を活用可能。
 - ✓ 関連事例：株のポストトレード（参考資料）

【参考】 RTGS ? / 2フェーズコミット ?

- RTGSではないけない？

<https://www.boj.or.jp/about/education/oshiete/kess/i14.htm>

- ✓ 非金融機関に対して口を開けるのか？
- ✓ 複数ネットワークを活用しづらい

- 2フェーズコミットではないけない？

<https://www.ogis-ri.co.jp/otc/hiroba/technical/DTP/step2/index.html>

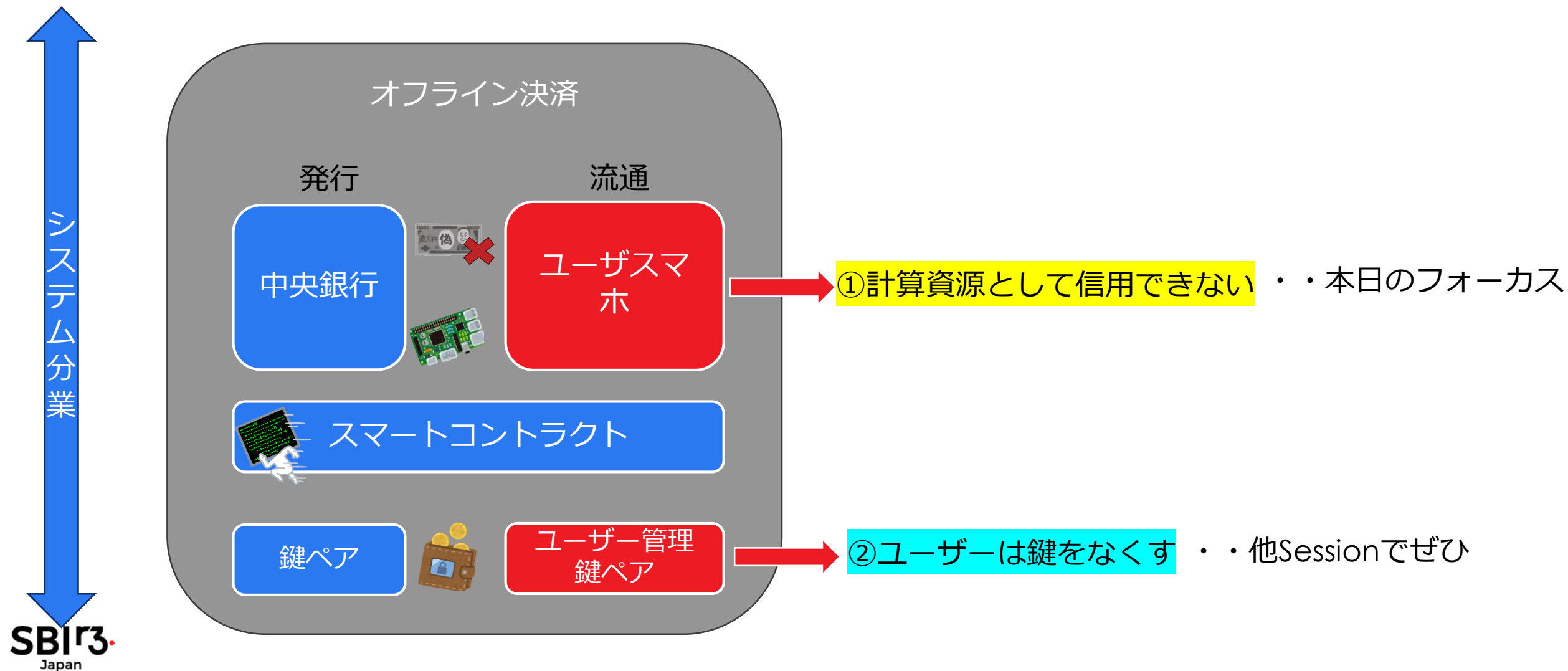
- ✓ 課題は2つ
 - システム連動先の障害波及（東横線が止まると西武池袋線が・・・）
 - 共通化した2フェーズコミット実装を用意できるか？
 - 不明区間の処理、デッドロック回避、etc...

UTXOモデルの適用

- 1 Layer1ーCBDCモデル
- 2 **オフライン決済**
- 3 フルCBDC

オフライン決済の課題

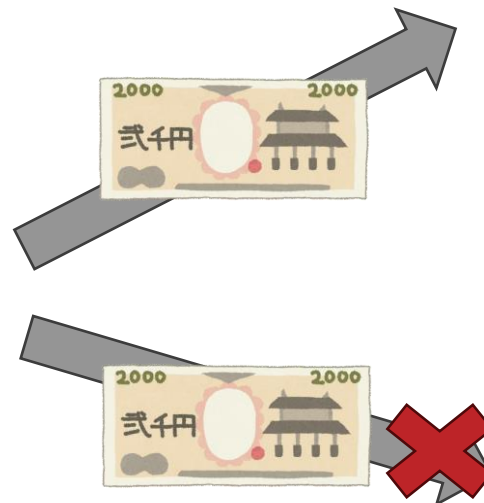
Discussion Purpose Only



① 計算資源として信用できない

Discussion Purpose Only

3000→1000



0→2000

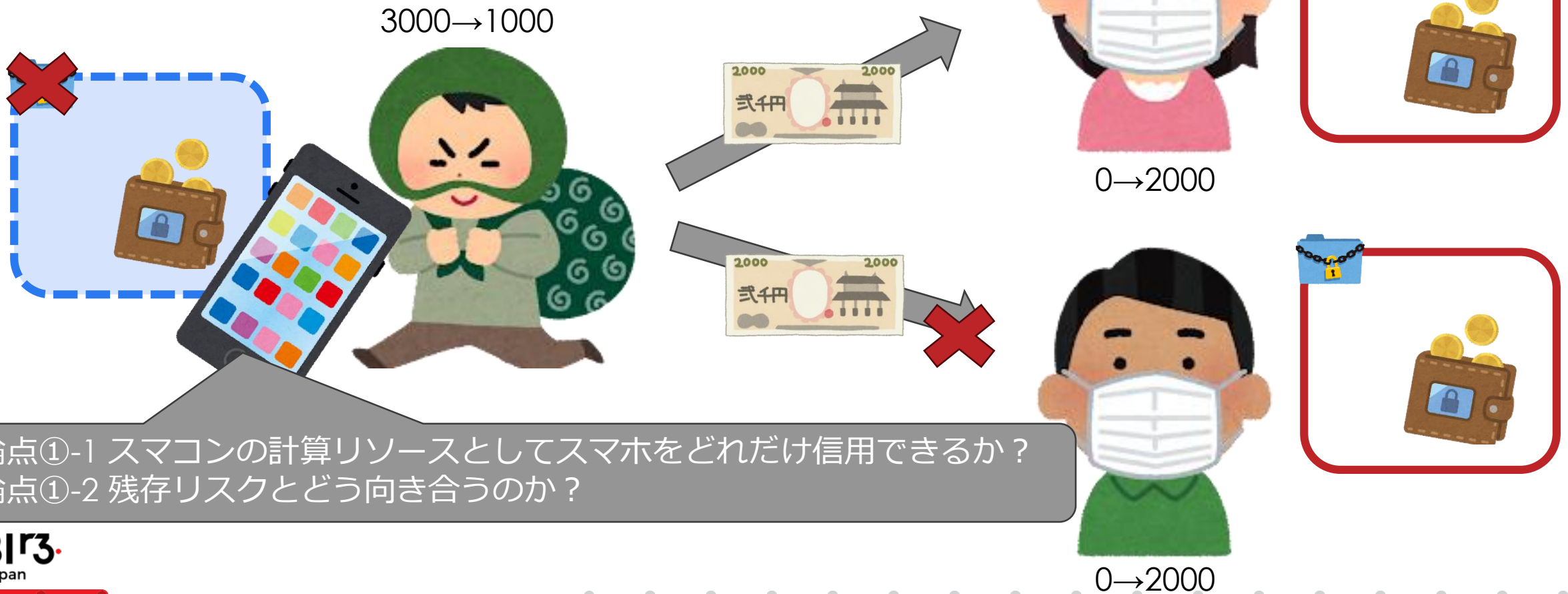


0→2000

データコピーが容易なので、偽札作るのも容易
→防止する仕組みが欲しい

① 計算資源として信用できない

Discussion Purpose Only



論点①-1 スマコンの計算リソースとしてスマホをどれだけ信用できるか？
論点①-2 残存リスクとどう向き合うのか？

① 計算資源として信用できない

Discussion Purpose Only

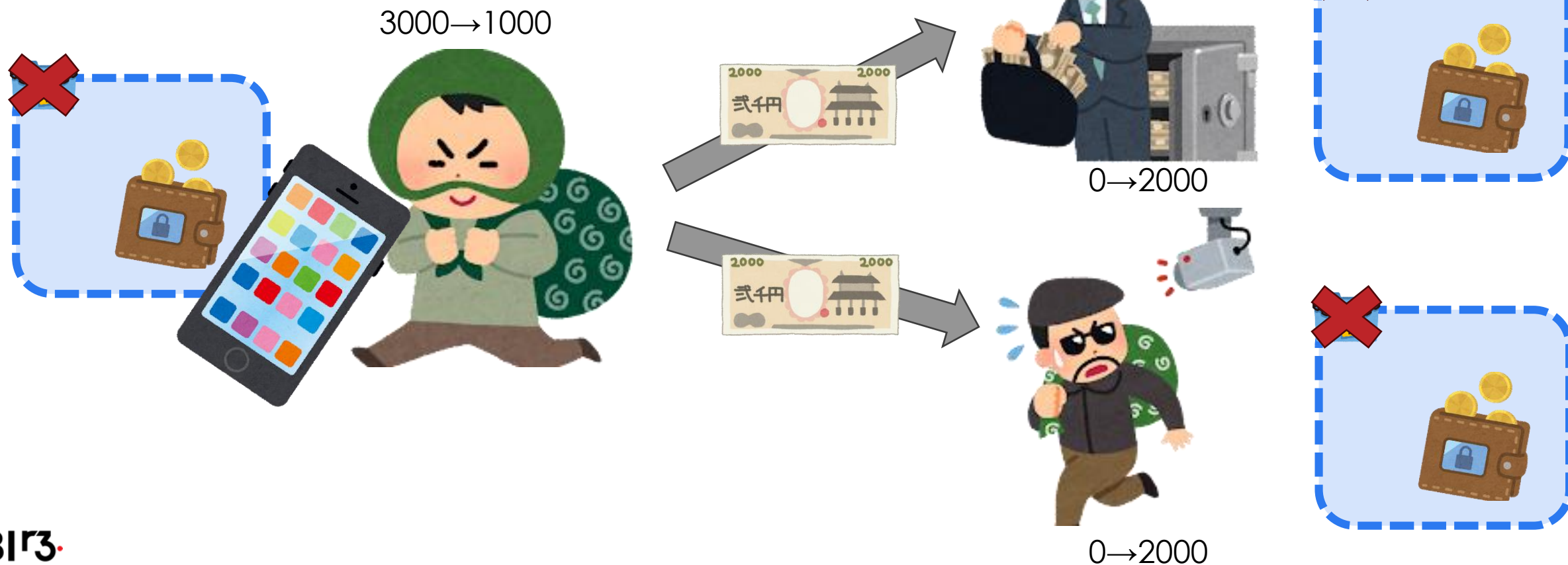


論点①-1 スマコンの計算リソースとしてスマホをどれだけ信用できるか？
論点①-2 残存リスクとどう向き合うのか？

①-2 残存リスクとの向きあい方

Discussion Purpose Only

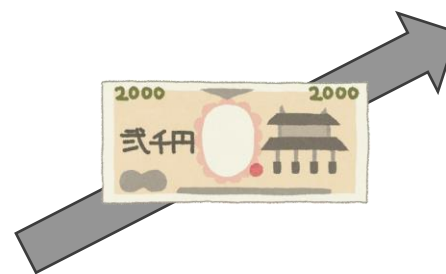
当事者が全員「悪意」を持っていたらどうしようもない・・・



①-2 残存リスクとの向きあい方

「善意の第三者」をいかに救えるか。

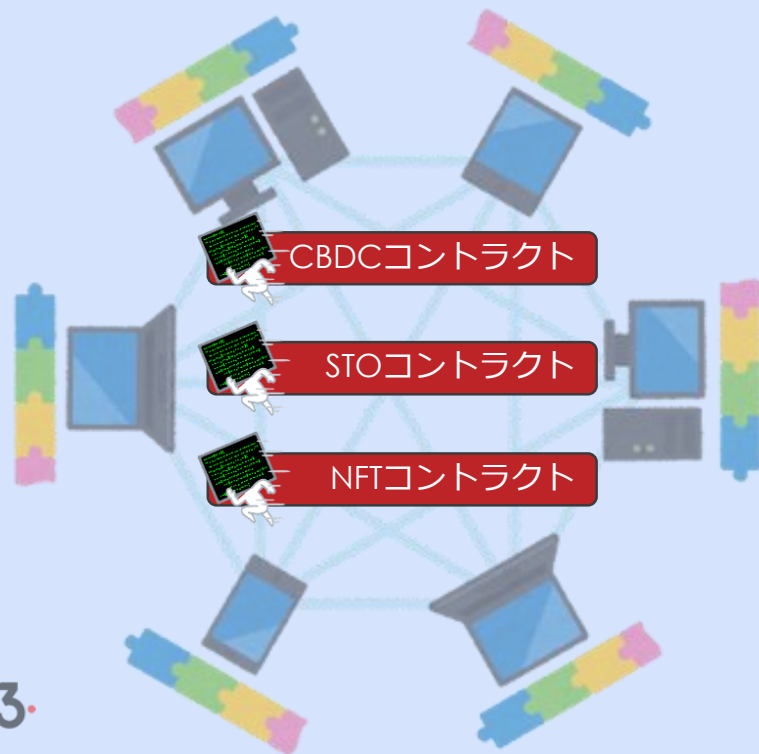
Discussion Purpose Only



UTXOへのトランザクション埋込

Discussion Purpose Only

- 一般的なスマートコントラクト
 - ✓ ネットワークに埋め込まれたプログラム



- UTXOへのトランザクション埋込
 - ✓ 特定取引に埋め込まれたプログラム

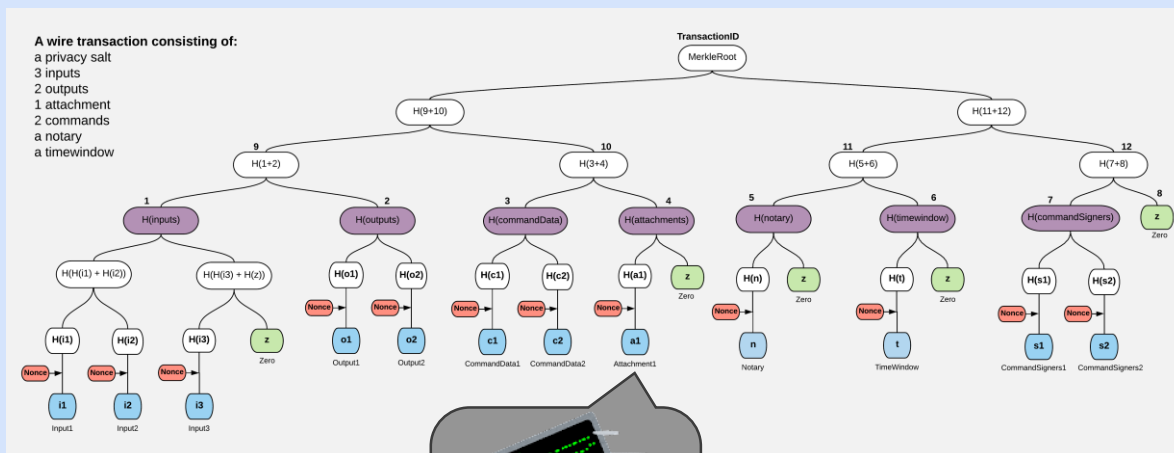


トランザクション埋込の実装例

Discussion Purpose Only



UTXOモデル：
一つの取引をTransactionとしてデータモデル化

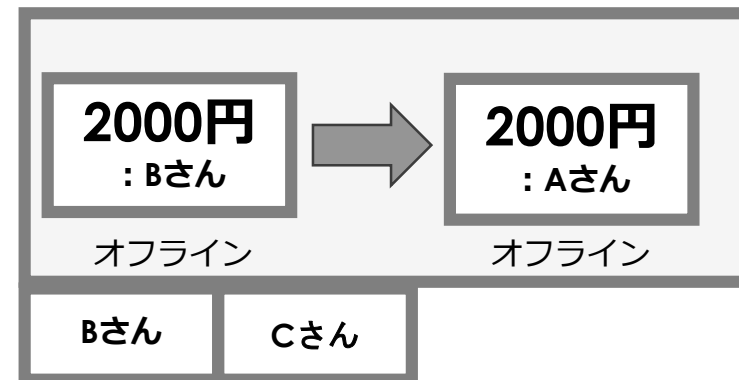
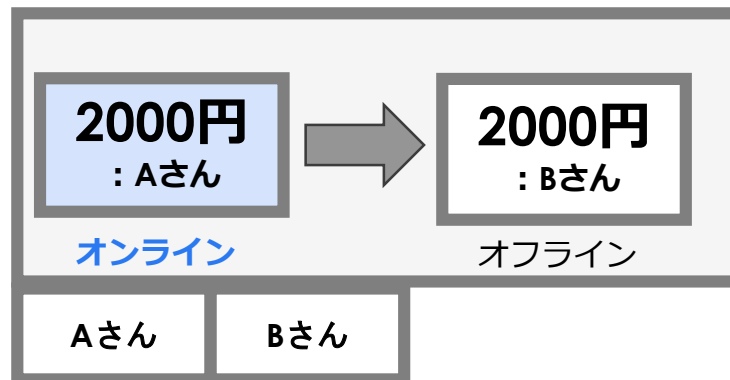
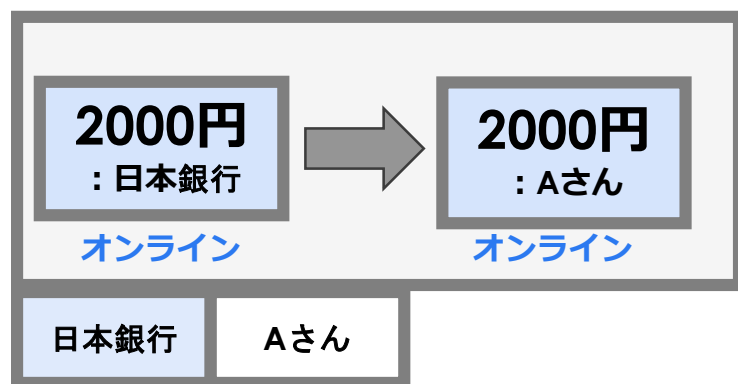
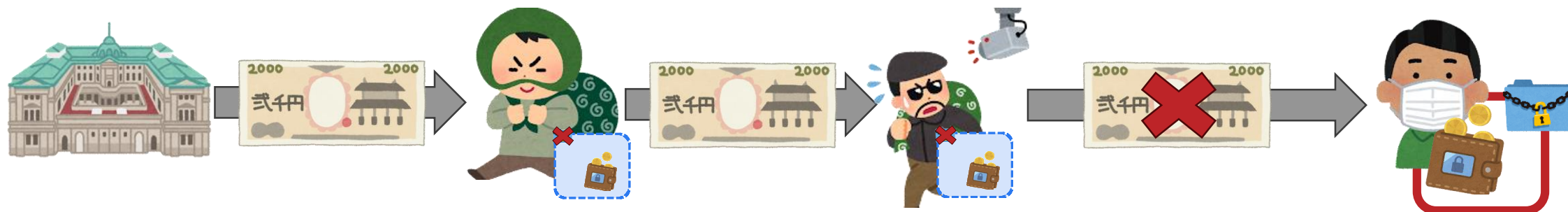


実装例：
Transaction事に一つのMerkleTreeを構成
& 子要素にプログラムを埋込

①-2 残存リスクとの向きあい方× UTXO

Discussion Purpose Only

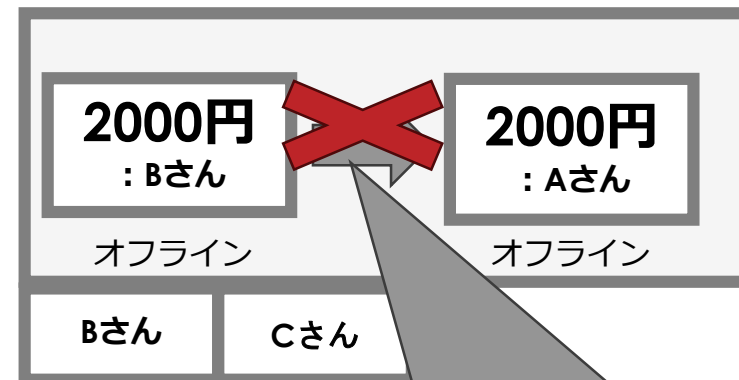
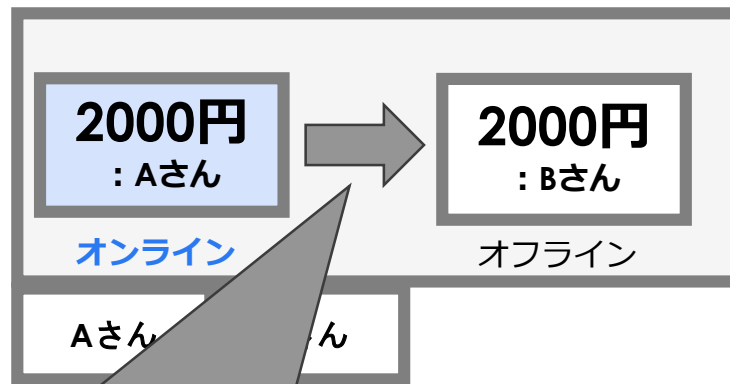
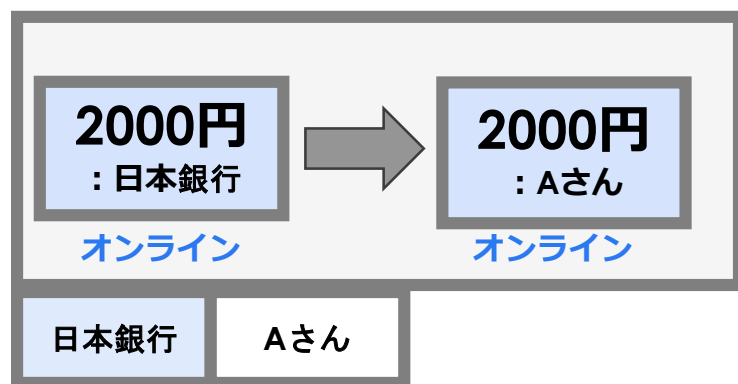
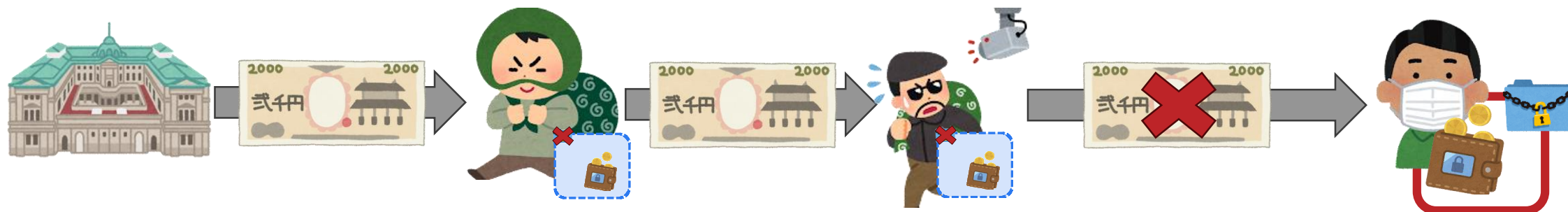
リスク対応：取引回数制限



①-2 残存リスクとの向きあい方× UTXO

Discussion Purpose Only

リスク対応：取引回数の制限



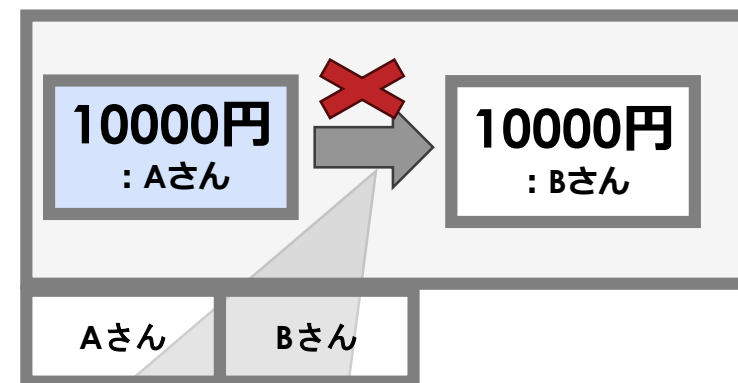
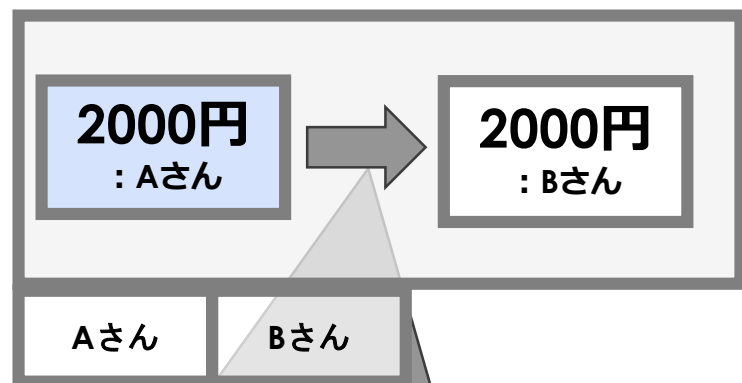
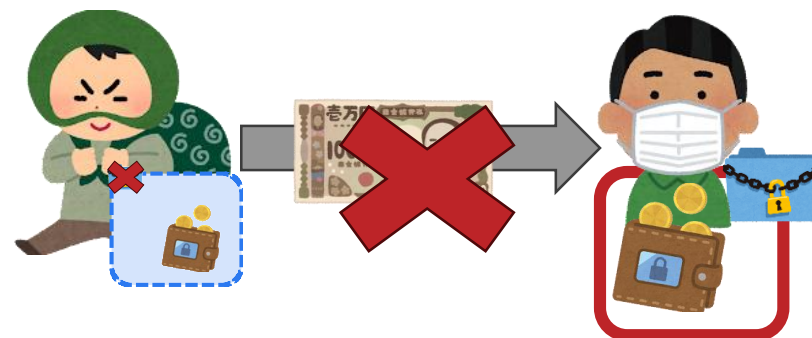
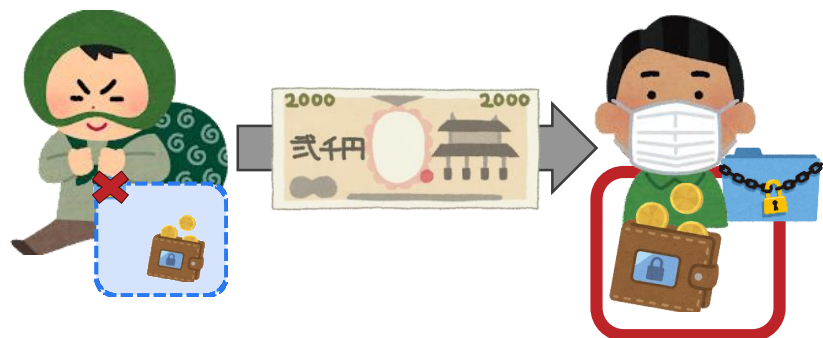
スマコンルール：Aさんの2000円には、日本銀行の署名があるので**オフライン**で使用可能

スマコンルール：Bさんの2000円には、日本銀行の署名がないので**オフライン**で使用不可

①-2 残存リスクとの向きあい方× UTXO

Discussion Purpose Only

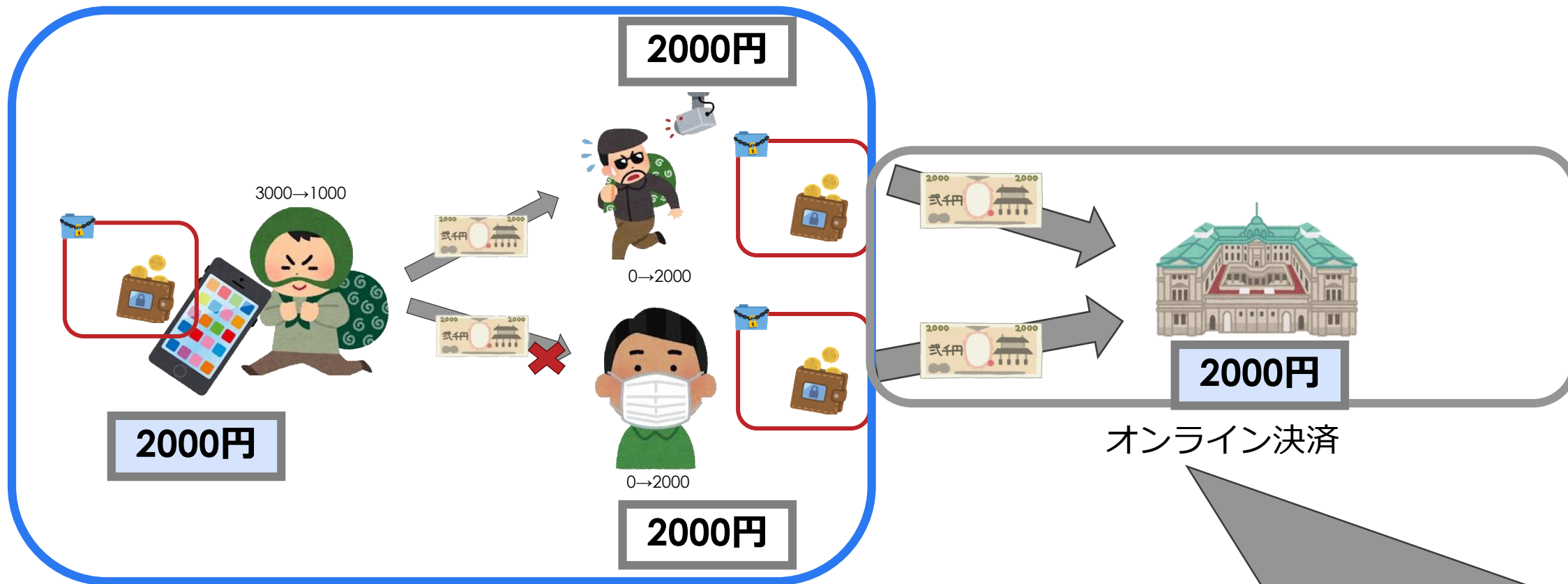
リスク対応：取引金額の制限（例えば5000円）



オフライン決済→オンライン事後検証

Discussion Purpose Only

オンライン復帰後の検証は可能



オフライン決済

オンライン決済

- ・オフライン→オンライン時に遡及検証⇒非許容データをどう扱うか？
- ・UTXOを用いれば、取引ベースで対応検討可能

UTXOモデルの適用

1. 2層式CBDCモデル
2. オフライン決済
3. フルCBDC

フルCBDCの実現に向けた全体像

Discussion Purpose Only



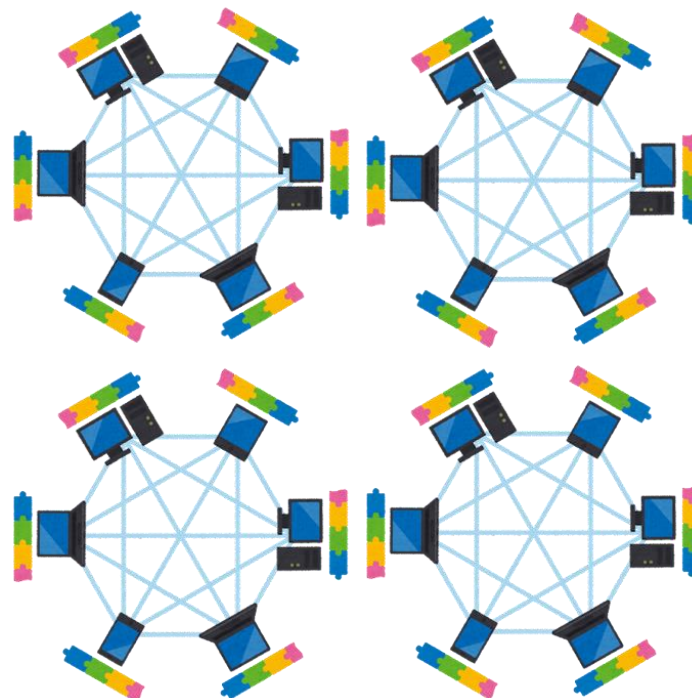
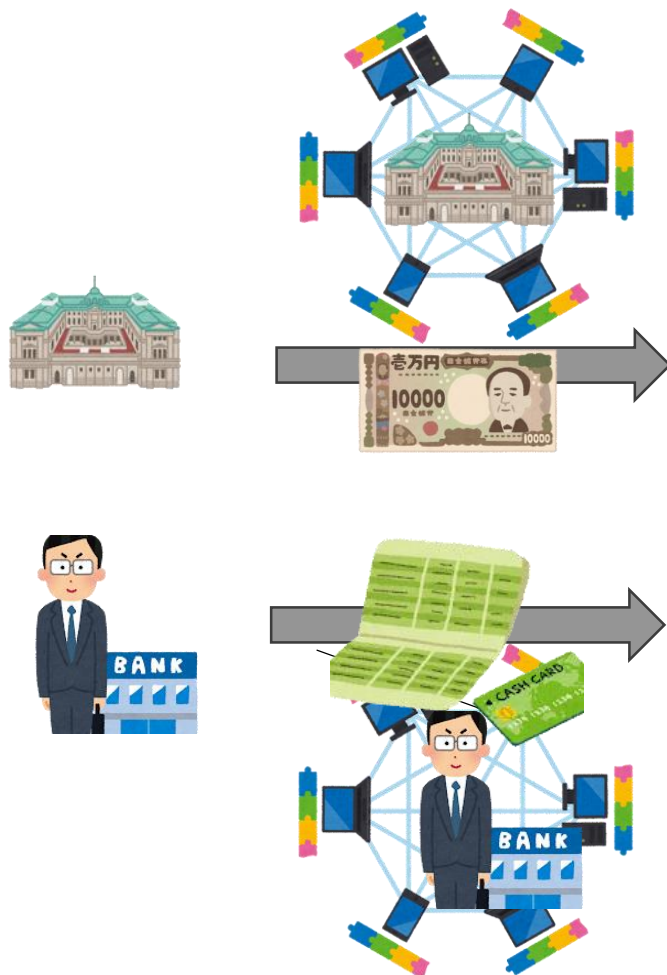
フルCBDCの実現に向けた全体像

Discussion Purpose Only



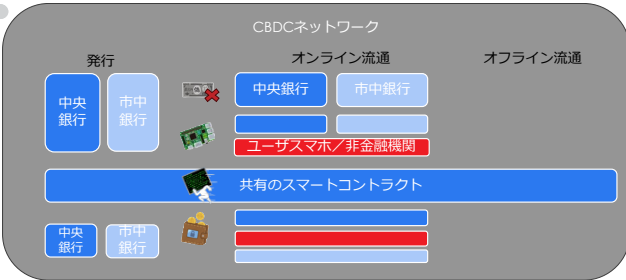
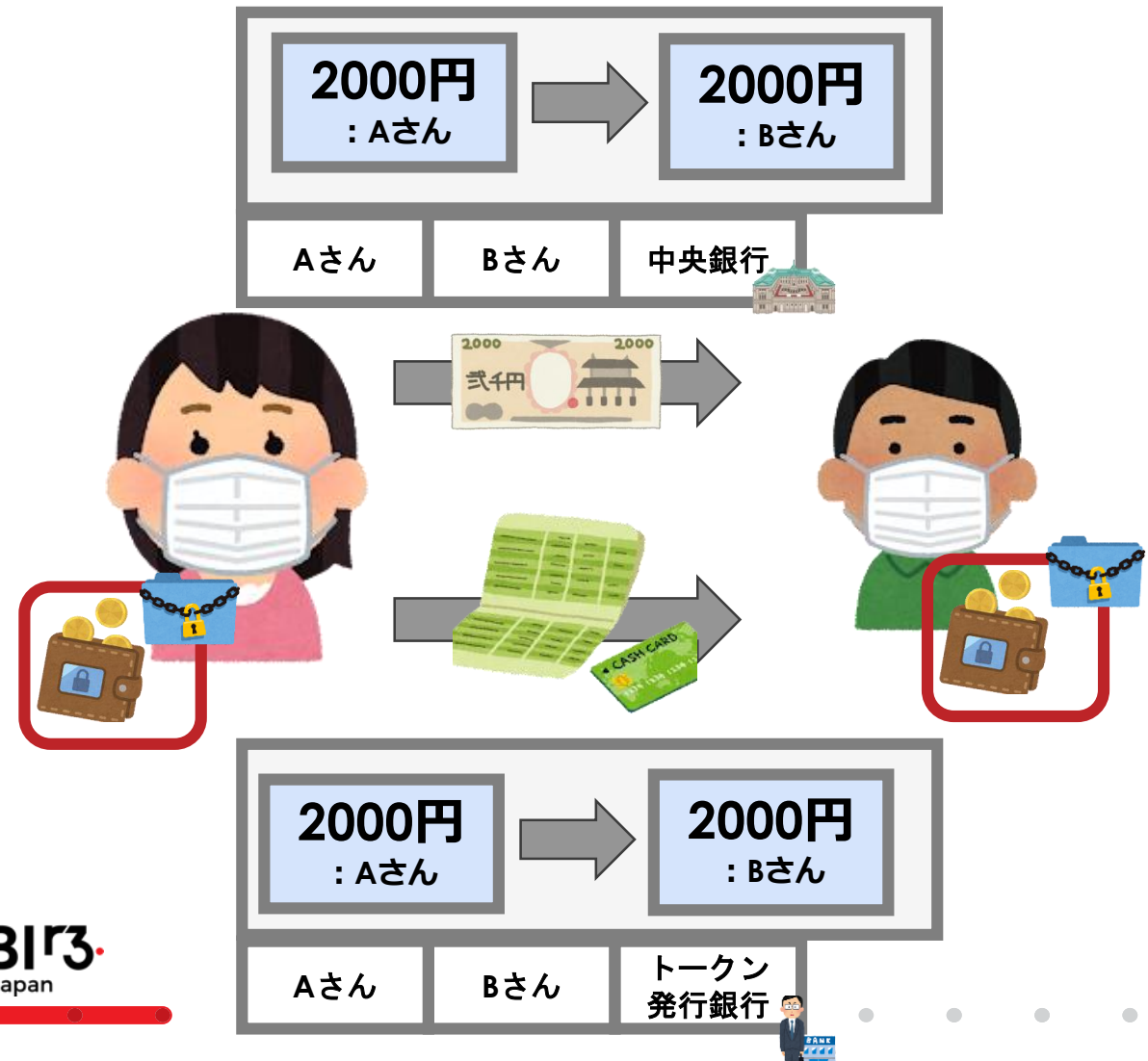
銀行：発行制御

発行体を中央銀行&市中銀行に限定する（マネーサプライ提供主体を制限）



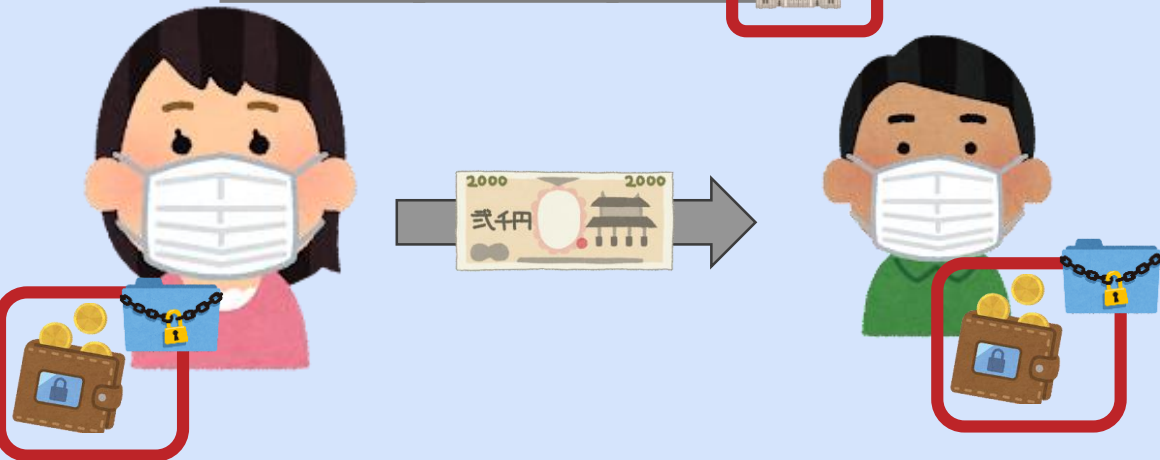
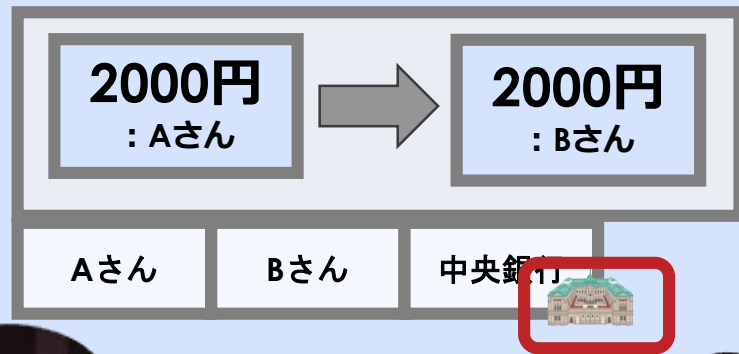
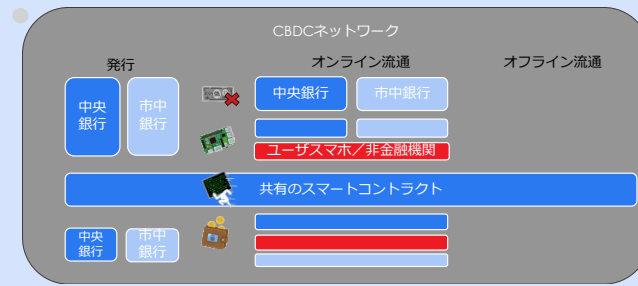
オンライン流通

オンライン流通時には、トークン発行銀行が取引に参加



UTXO×サステナビリティ

最低限のリソースによる当事者コンセンサス&発行体コンセンサスの実現



UTXOの決済において、**ネットワーク全体合意は不要**

(不特定多数のIssueを認める場合はこの限りではない)

債務者 (Issuer) & 取引当事者の合意だけを要求とする場合

⇒PoW等のコンセンサスアルゴリズムで必要となる

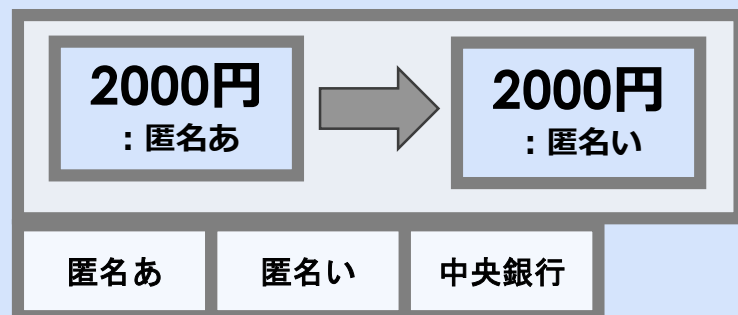
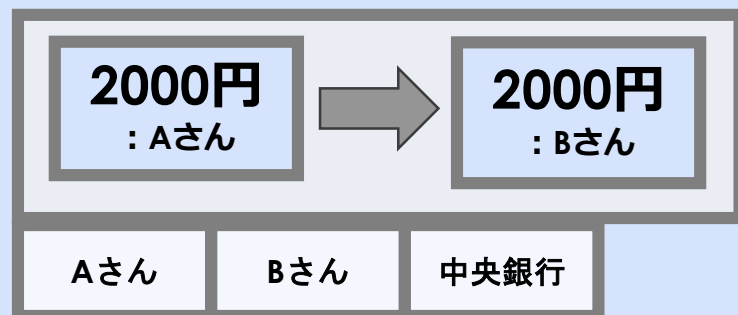
- ・複数計算資源での重複実行
- ・計算資源間での多重データ通信が不要。

- ⇒
- ・サービスのサステナビリティ向上
 - ・サービスのパフォーマンス向上

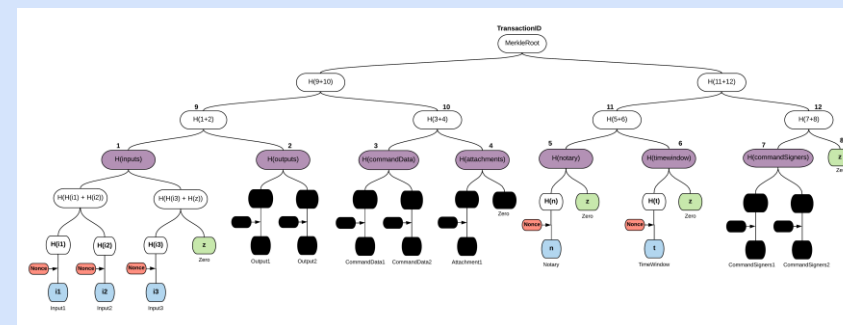
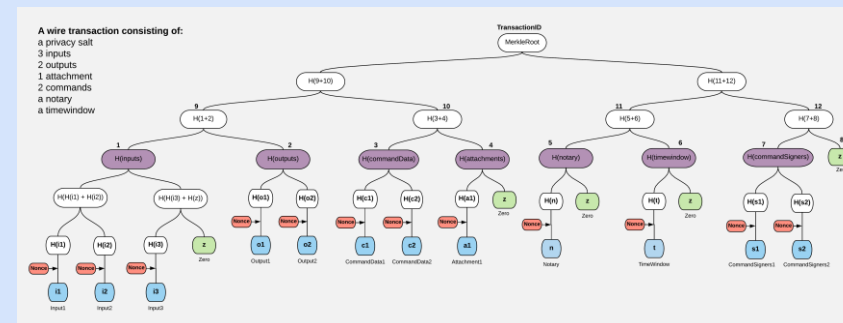
⇒商用化リテールCBDCやトークン化の課題解決にUTXOは資する可能性が高い

UTXO×匿名化

Transaction Tear Off



実装



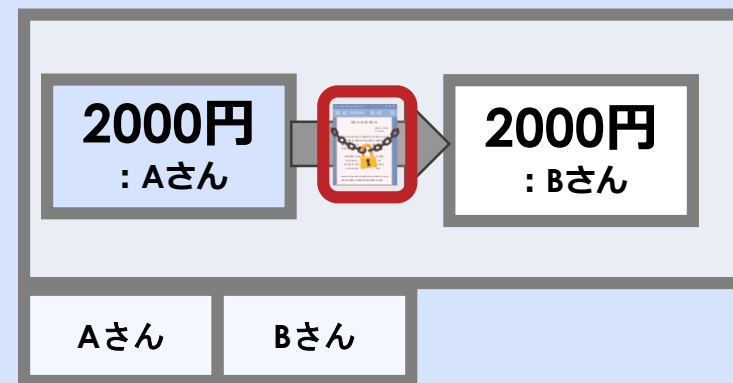
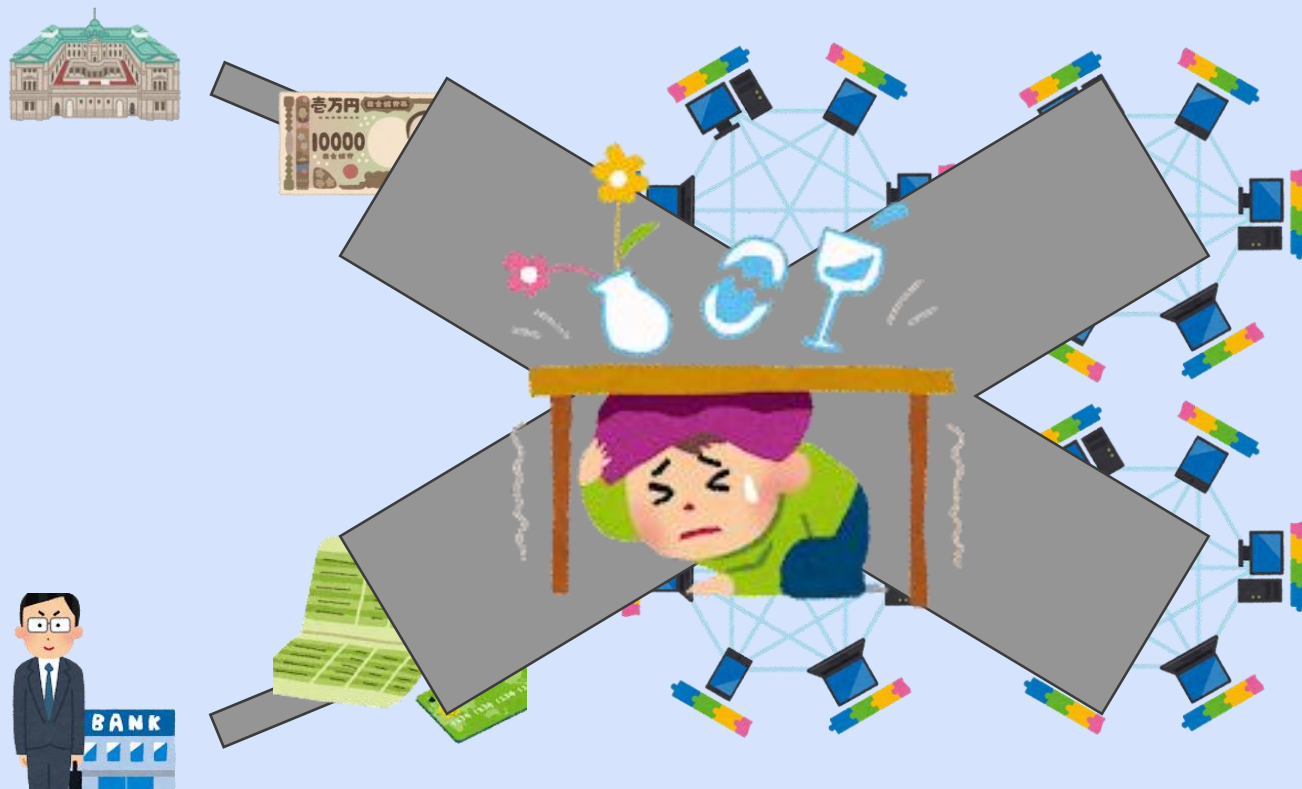
債務者が合意するために最低限必要な情報

- Inputとなるデータの正当性
- 金額（2000円）が取引前後で変化しないこと

- ① マークルツリー上で不要な情報を隠蔽
(ハッシュ値のみを共有)
- ② 埋め込まれたスマートコントラクトは、
共有された 情報のみを使って合意検証を実施

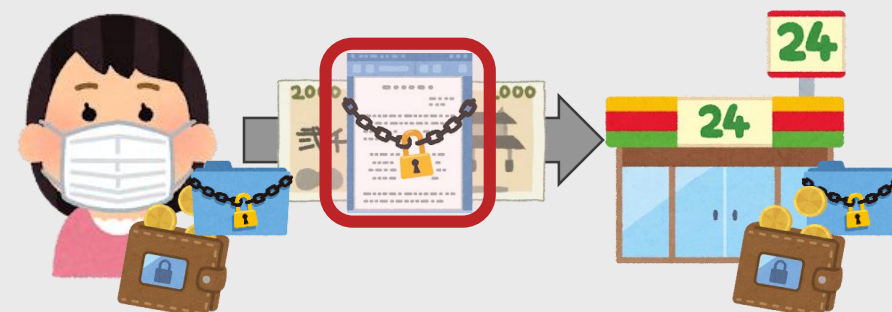
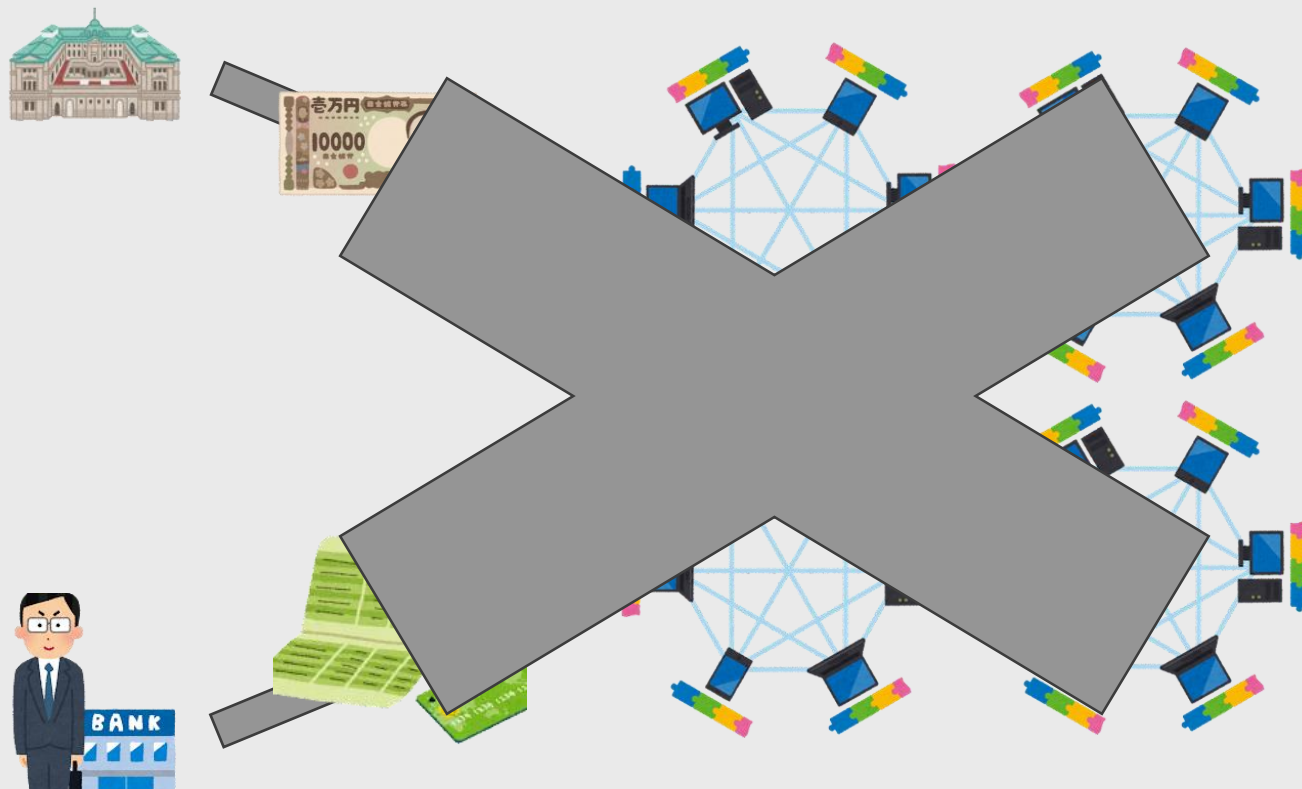
オフライン決済

銀行が参加しない決済には、スマートコントラクトに強い制約をかける



オフライン決済 = 発行体に参加しない決済という整理 Discussion Only

オフライン決済を耐障害対応だけではなく、非金融ユースケースへの接続確保という観点で活用



フルCBDCまとめ：20年後に向けて

Discussion Purpose Only

- 日本でここまで必要なのかは？
- 実装に向けたアイデア
 - ✓ UTXOへのスマートコントラクト埋込
 - ✓ Issuerは中央銀行と市中銀行だけに制限（信用創造には強い制約が必要）
 - ✓ 「オフライン決済＝発行体を確認しない決済」と定義
- 付随するアイデア
 - ✓ 決済ユースケースにおけるサステナビリティの確保
 - ✓ 匿名性ニーズへの対応
 - ✓ そもそも決済基盤の弱いグローバルサウスへのシステム販売

Discussion Points

Discussion Purpose Only

--今日話した課題-----

- 階層化によるスケーラビリティ向上の度合いとその課題
- オフライン決済を前提として、ウォレットとスマートコントラクトの接続方法

--さらなる課題-----

- スマートコントラクト実行環境に対するセキュリティ
- ユーザー鍵紛失時の資金再発行の実現可能性
- DvP、PvPに対するアイデンティティ管理

まとめ

Discussion Purpose Only

- サービスは十分に分散化している
 - ✓ 流動性を提供しないサービス上での決済という新たな領域が生まれている。
 - ✓ 新たな領域の課題 = 流動性とその速度
 - ✓ UTXOが持つデータの柔軟性は流動性提供の為の共通基盤として有用ではないか？
- システムはこれから分散する
 - ✓ ウォレット、データ自己主権等がきっかけ
 - ✓ システム分散により解決したい課題に対して、UTXOモデルは以下の面で有用
 - トランザクションへのスマートコントラクト埋込
 - プライバシー確保とガバナンスの両立
- 20年後を見据えると、決済サービス&システム全体をUTXOモデルが大きく変える可能性もある。



SBI r3.

Japan