

CBDCフォーラム WG4 第10回

価値移転プロトコル（電子現金）について

Off-Chain Solution for Tokenization

株式会社NTTデータ 次世代決済技術推進室

前回（ステーブルコイン）の振り返り（1/2）

ネットワークによって“**遍在する**” 計算リソースを背景にブロックチェーン技術は普及。分散化の流れは不可逆。
短期間に多様な技術・ユースケースを輩出するとともに分散アプリケーション基盤を生み出した

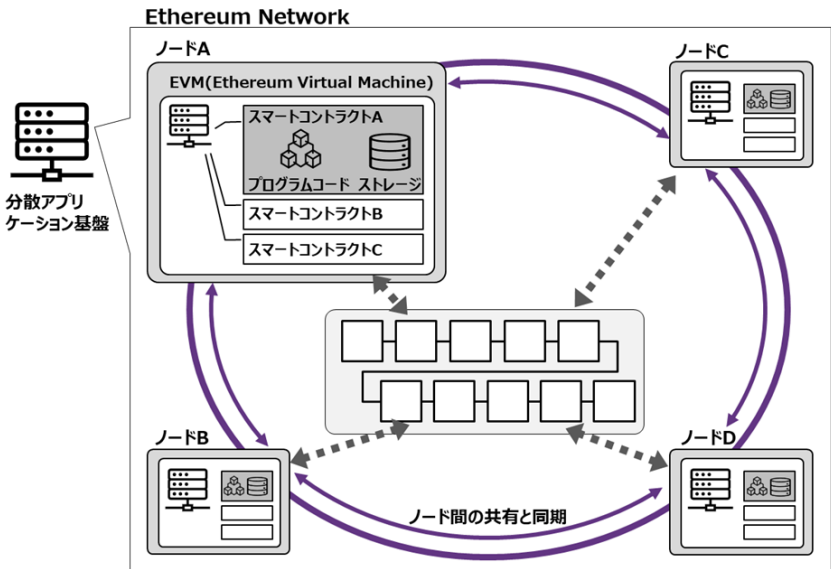
一昔前のシステムと同等以上の性能、リソースを備えたデバイスが高速・低遅延なネットワークに
常時接続され、天文学的ともいえる数が世界にあまねく普及した世界



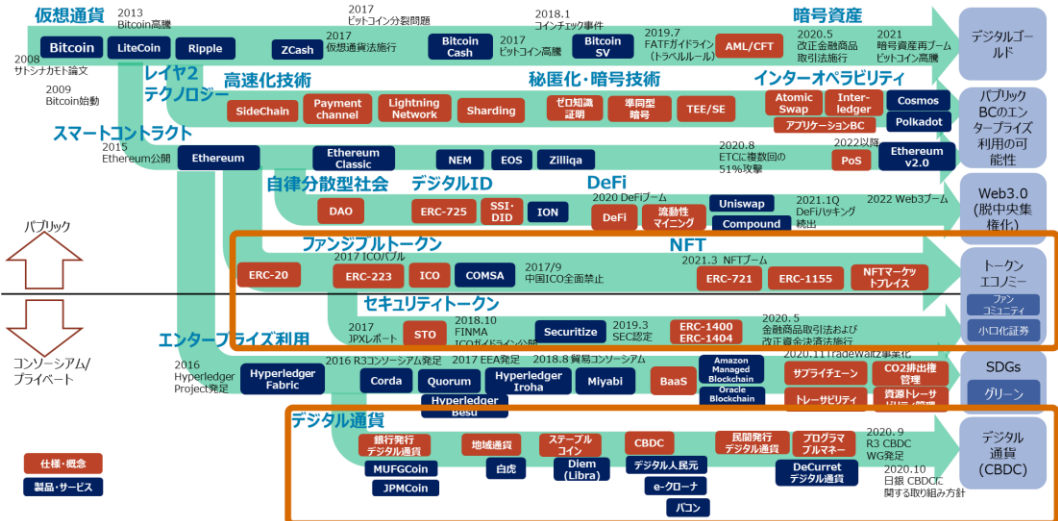
1974年 (Intel 8080)		2024年 (Apple A18)
2MHz	→	4GHz
64KB	→	8GB
6μm (6000個)	→	3nm (数十億個~)
300bps	→	20Gbps(5G)

2024
iPhone16 Pro

ネットワーク全体があたかも一台のコンピュータであるかのように振る舞う
(分散アプリケーション基盤)

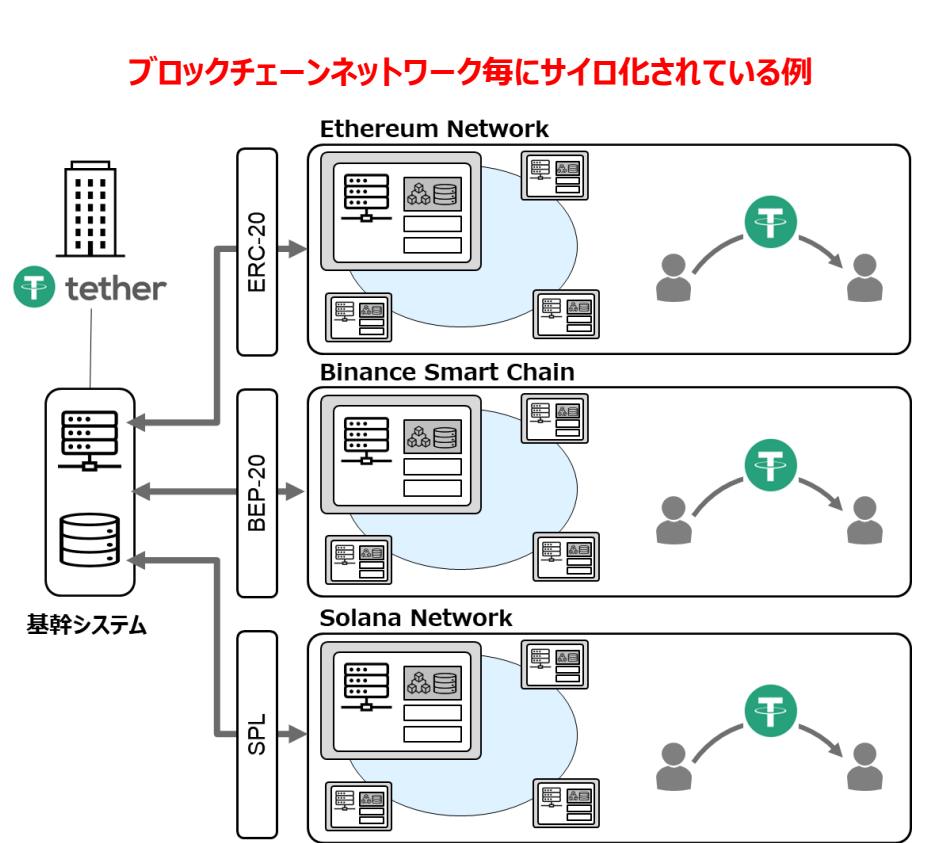


濃密な15年。新たな技術、新たなビジネス、新たな課題の熱狂的な生々流転



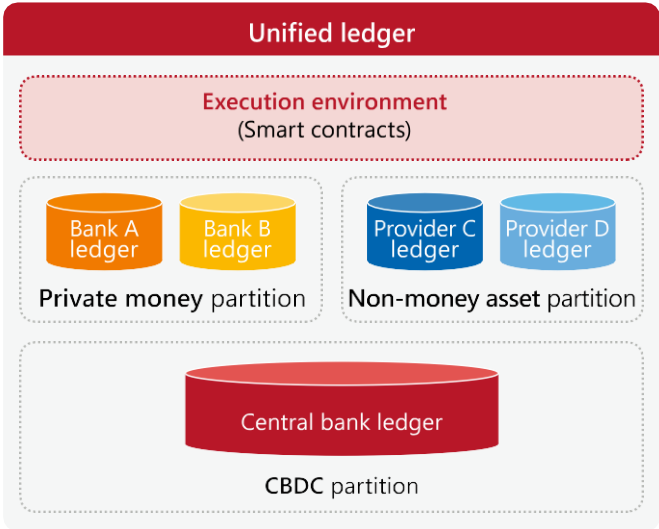
前回（ステーブルコイン）の振り返り（2/2）

ブロックチェーンであっても分散“台帳”であるがゆえに排他性やサイロ化は付きまとう。
一方でBIS等金融当局サイドからはサイロ化の解消とマネーの単一性保持の観点からUnified Ledgerを提唱



デジタルマネーは通信ネットワークのエッジにあって、銀行やノンバンクが運営する**サイロ化された独自DB**に存在し、これらのDBと接続するには**外部のメッセージングシステムが必要**である。
メッセージ、照合、セトルメントの分離によって遅延が発生する可能性があり、完了したアクションが参加者には未完了に見えることが多い。その結果、長期間エラーに気づかず、エラー解決にコストがかかり、運用リスクが増す可能性がある。
これらのことから**ペイメントプロセスはコストがかかり、面倒で、遅く、不透明であり、ユーザー要求の変化に対応できない可能性**がある。

同一プラットフォーム上に民間のトークン化マネーとCBDCを保有することにより、サイロ化したDB間で順次メッセージを送信する必要がなくなる→**2つのアセットを同時に交換**する（相手が送金したときのみ送金する）**アトミックな決済**が可能になる。
上記プロセスにおける、ある仲介機関から別の仲介機関へのペイメントの**ホールセール決済もホールセールCBDCで即時**に行う。
適切なアクセスコントロールを有するパーティション化したデータ環境を使用することで、**取引当事者には完全な透明性を確保して、取引当事者以外には取引を秘密**にできる。
同一プラットフォーム上でメッセージとペイメントレールを結合することで、unified ledgerは**ペイメントプロセスにおける遅延を排除して、決済リスクを軽減**する。



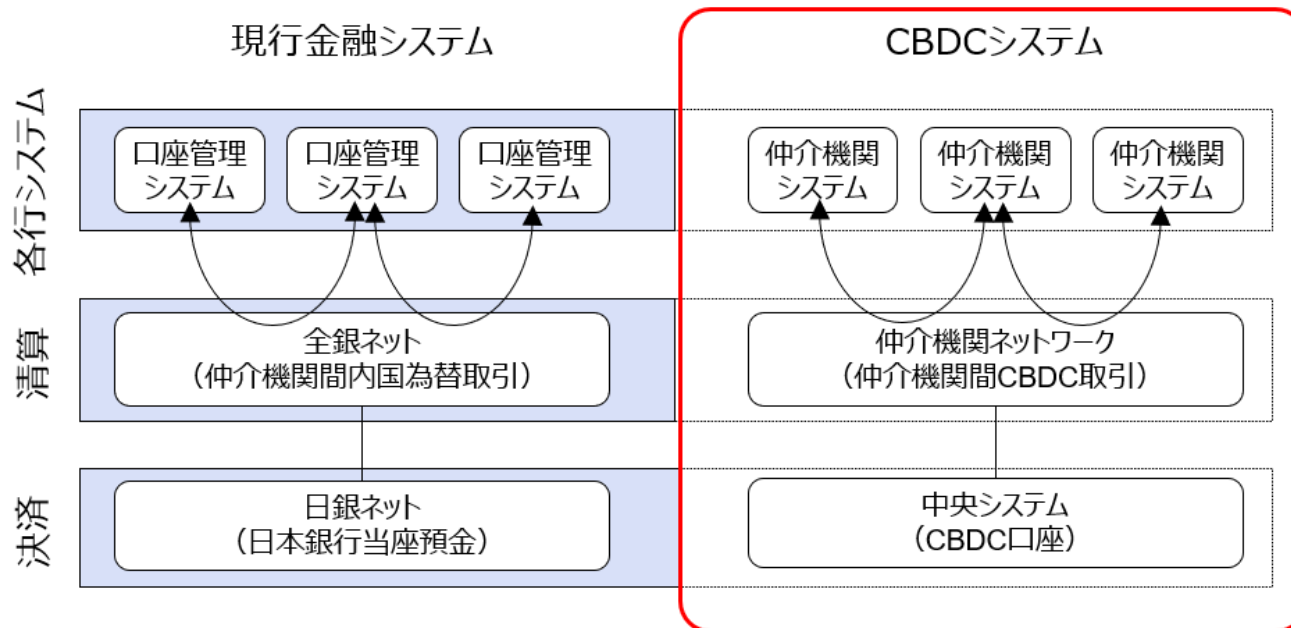
全てを一つの台帳に...



サイロ化されたシステム間の“水平的”共存への疑問

新たな決済システムを同じ技術レイヤで作ることを前提とした議論だけでよいのだろうか。

“CBDCという契機”を活かしてどのような未来を招来するのかを議論したい



「保有上限」

※財務省CBDC有識者会議「取りまとめ資料」より抜粋

【銀行預金との共存・役割分担】

- 銀行預金から急激／継続的な資金シフトが生じた場合、金融システム・経済に悪影響を及ぼす可能性。セーフガード措置の検討が必要。
- － 保有額制限は、銀行預金からの資金シフトを直接制限できる一方、手数料による対応は、特に金融ストレス時に機能しない可能性もあり、その効果が明確ではない。保有額制限を主軸として検討していくべき。

「民業圧迫」

【その他の決済手段との共存・役割分担】

- CBDCが他の決済手段を「支える」共通インフラの役割を果たすことで、各決済手段間の競争促進・ネットワーク効果の更なる発揮につながる。
- 一方、民間事業者のビジネスモデルに影響を及ぼす可能性。関係当局・関係事業者の間で十分な議論が必要。

新たな決済システムが同じレイヤで提供されるからでは？

・・・台帳が持つ「排他性」という属性が問題の根源

ブロックチェーン（分散台帳）を使ったからといって解消されない

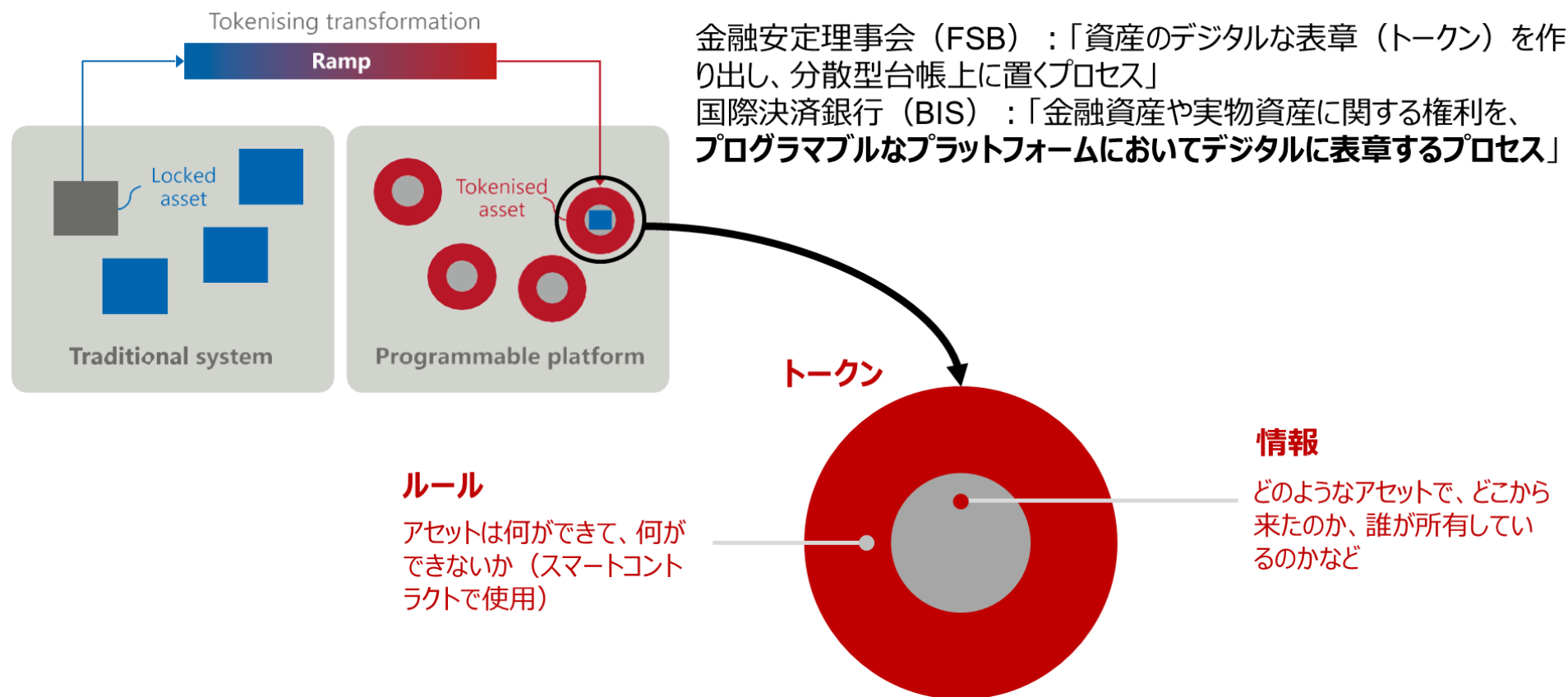
“デジタル化”とは？

“トークン化”と“プログラマビリティ”

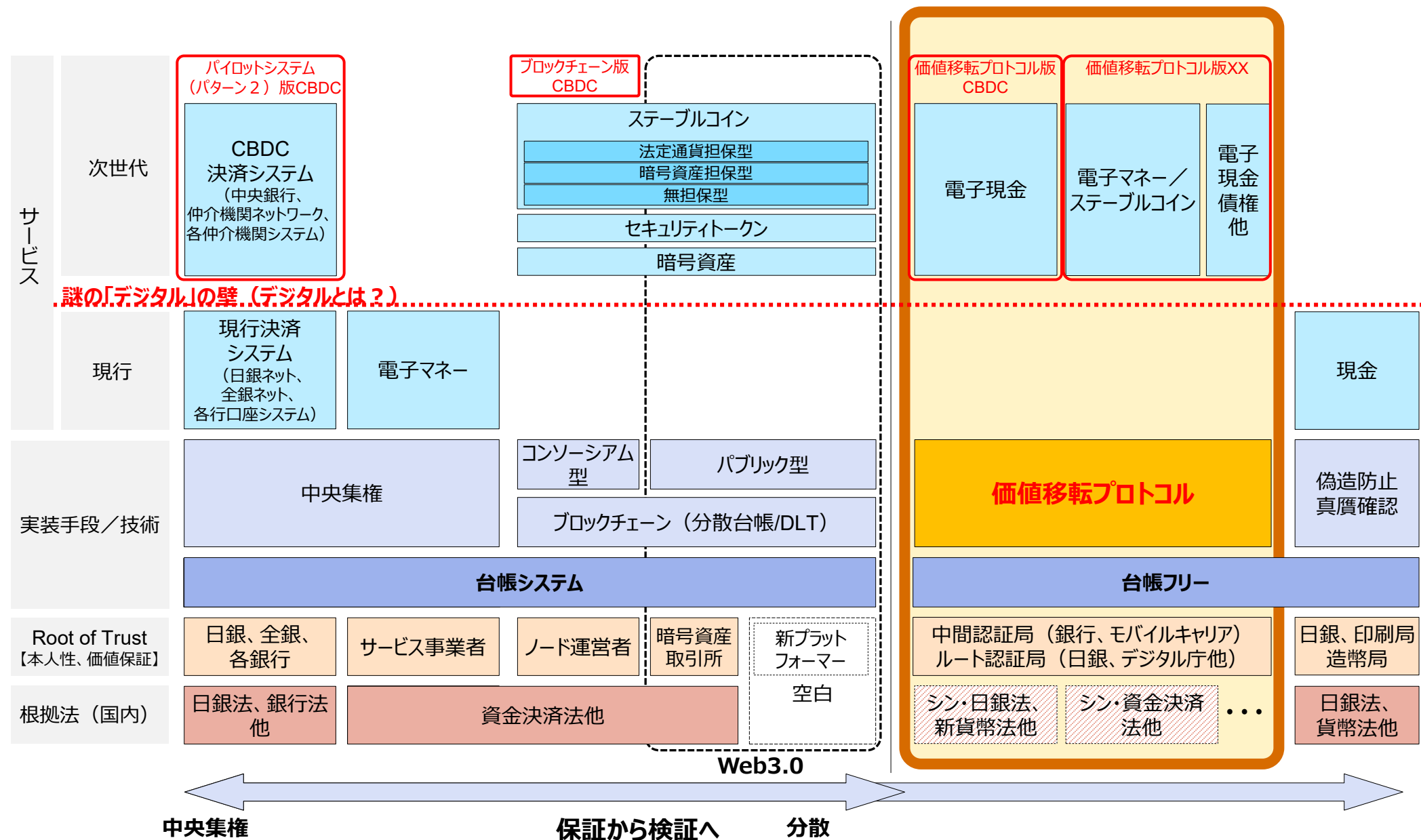
トークン化とは

高いプログラマビリティの実現を目指して

「従来の伝統的決済システム上の価値」を「**プラットフォーム自体が実行環境となるシステム上のトークン**」に置き換えるプロセス



価値移転プロトコル（電子現金）の実現する世界と従来技術の世界観



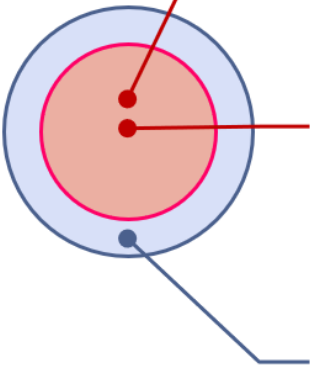
価値移転プロトコルとトークン構造

価値移転プロトコルはデバイス間で直接価値や情報を改ざんさせずに安全に転々流通させる技術

プラットフォームの制約を受けることなくお金に色を付けることが可能



トークン構造



信頼の連鎖

トークン情報

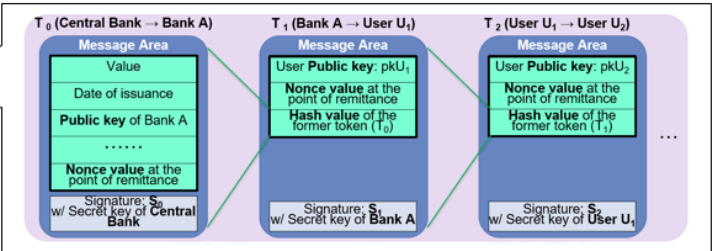
永続的な属性情報
Ex. 額面、種別、有効期限、
利用制限・ルール

添付情報

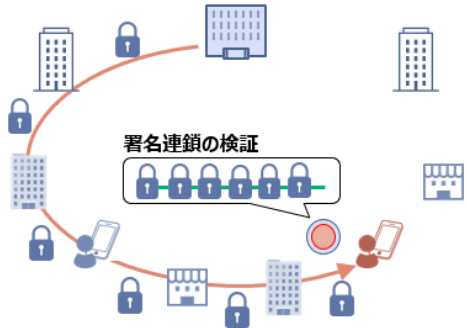
一時的な属性情報（取引固有）
Ex. VC、EDI情報、レシート、プログラム

価値移転プロトコル

トークンの有効性を検証するための署名連鎖

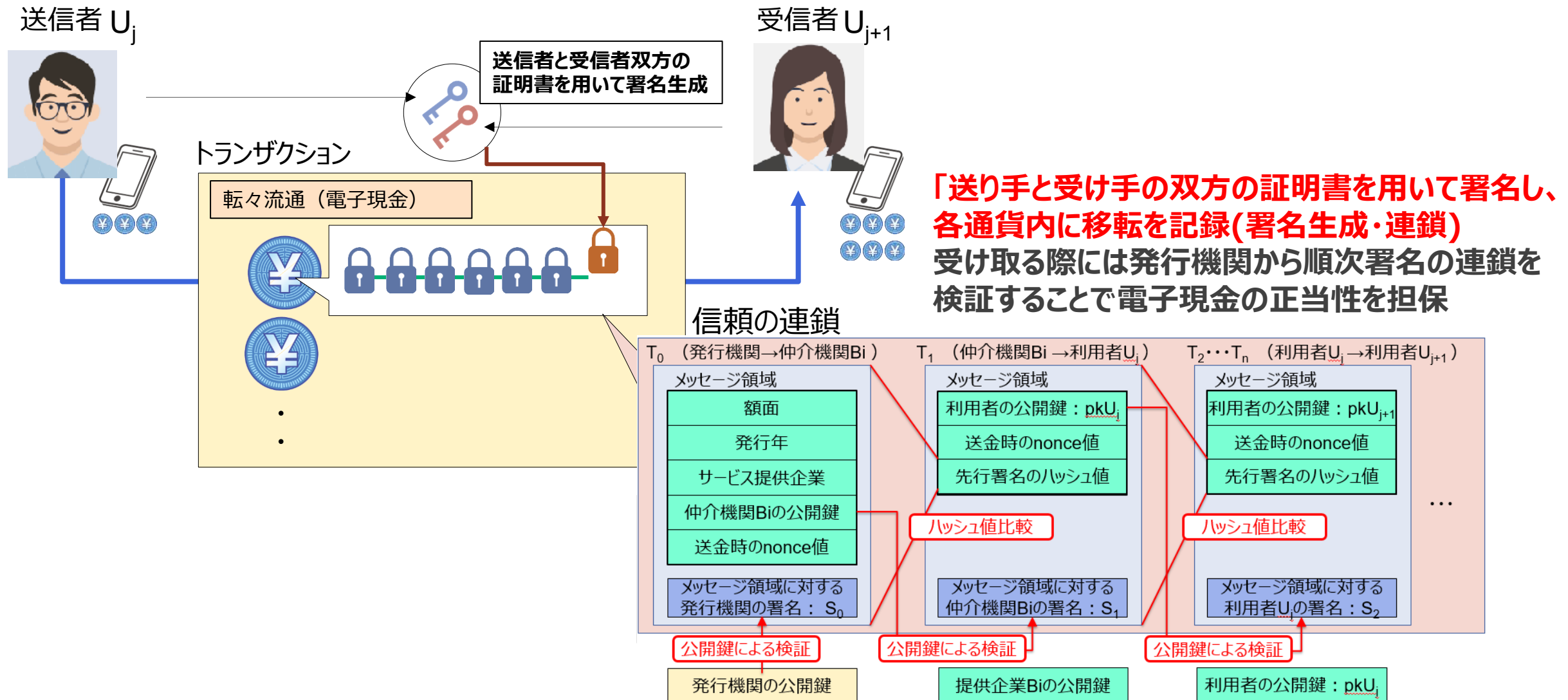


署名連鎖の検証



(参考) 価値移転の仕組み

流通する電子現金自体に検証に必要な「署名データの連鎖」を格納することで、当事者間で正当性を確保可能とする

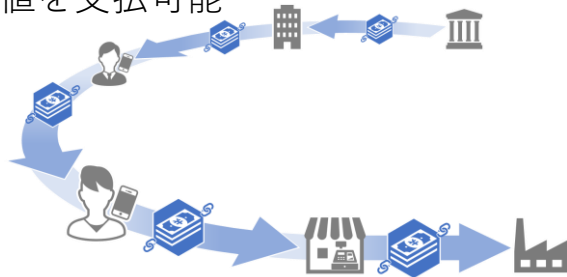


価値移転プロトコルの利点

従来技術と比較して、価値移転プロトコルに準拠したシステムでは様々なメリットを享受することが可能

転々流通性の実現

二者間で決済が完結でき、受取者は即時に価値を支払可能



性能上限の解消・設備コストの低減

台帳への処理集中が解消。性能上限がほぼ存在せず、設備コストも低減される



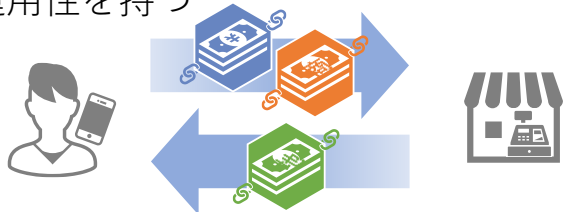
ふるまいの制御

用途や利用可能地域などの制限、高額転売の抑止、有効期限の設定など



トークンの相互運用性

PFではなくプロトコルであるため、同じプロトコルに準拠しているトークンは相互運用性を持つ



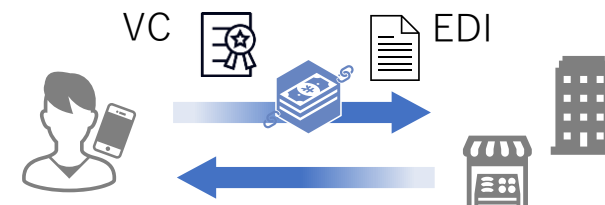
障害に対する強靱性確保

通信手段透過なので障害発生時もローカル通信によってデバイス間で決済可能



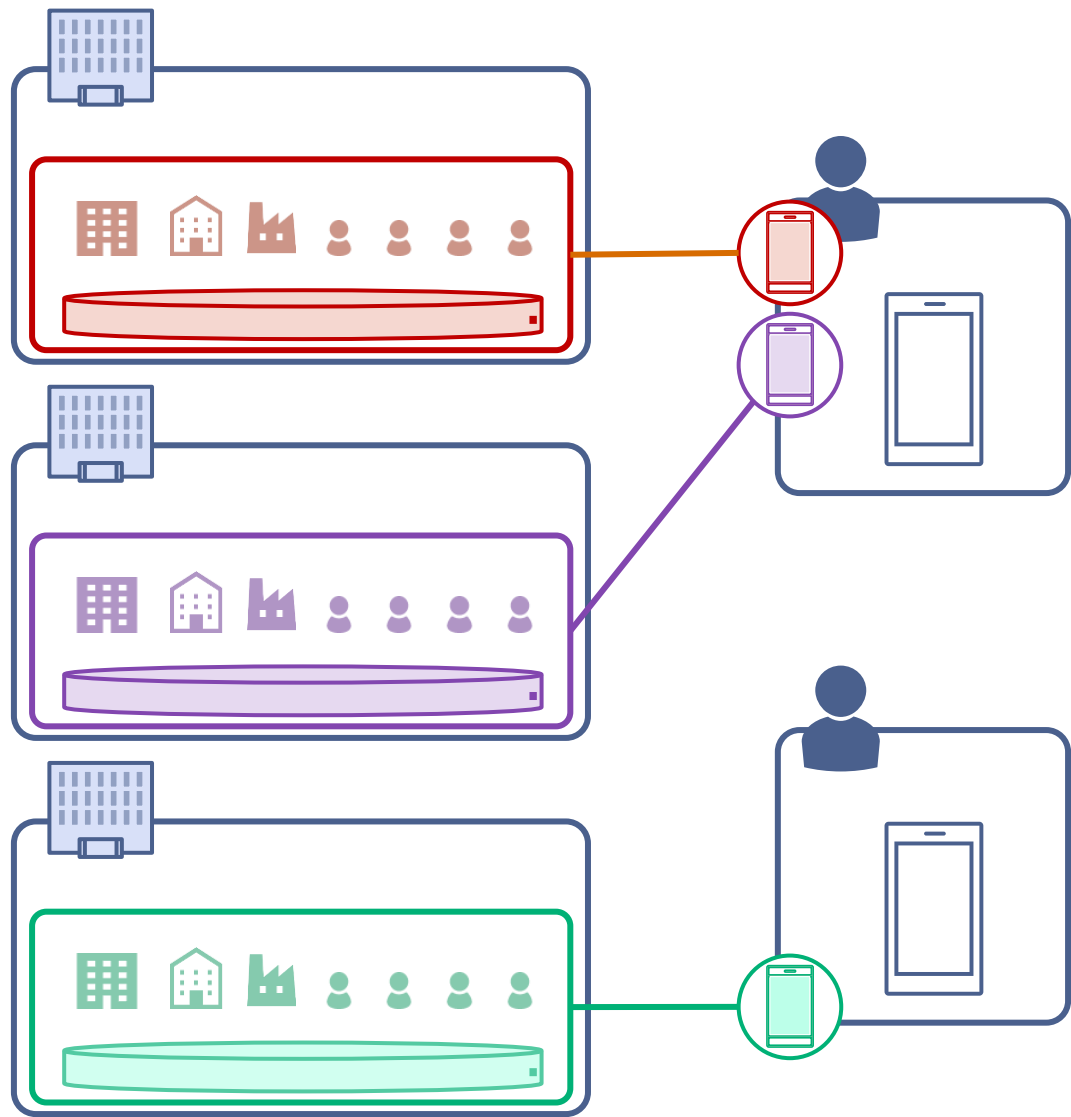
価値と情報のAtomicな転送

VCやEDI、内訳等の同時送付や、クーポンや領収書、診療明細等の返信等

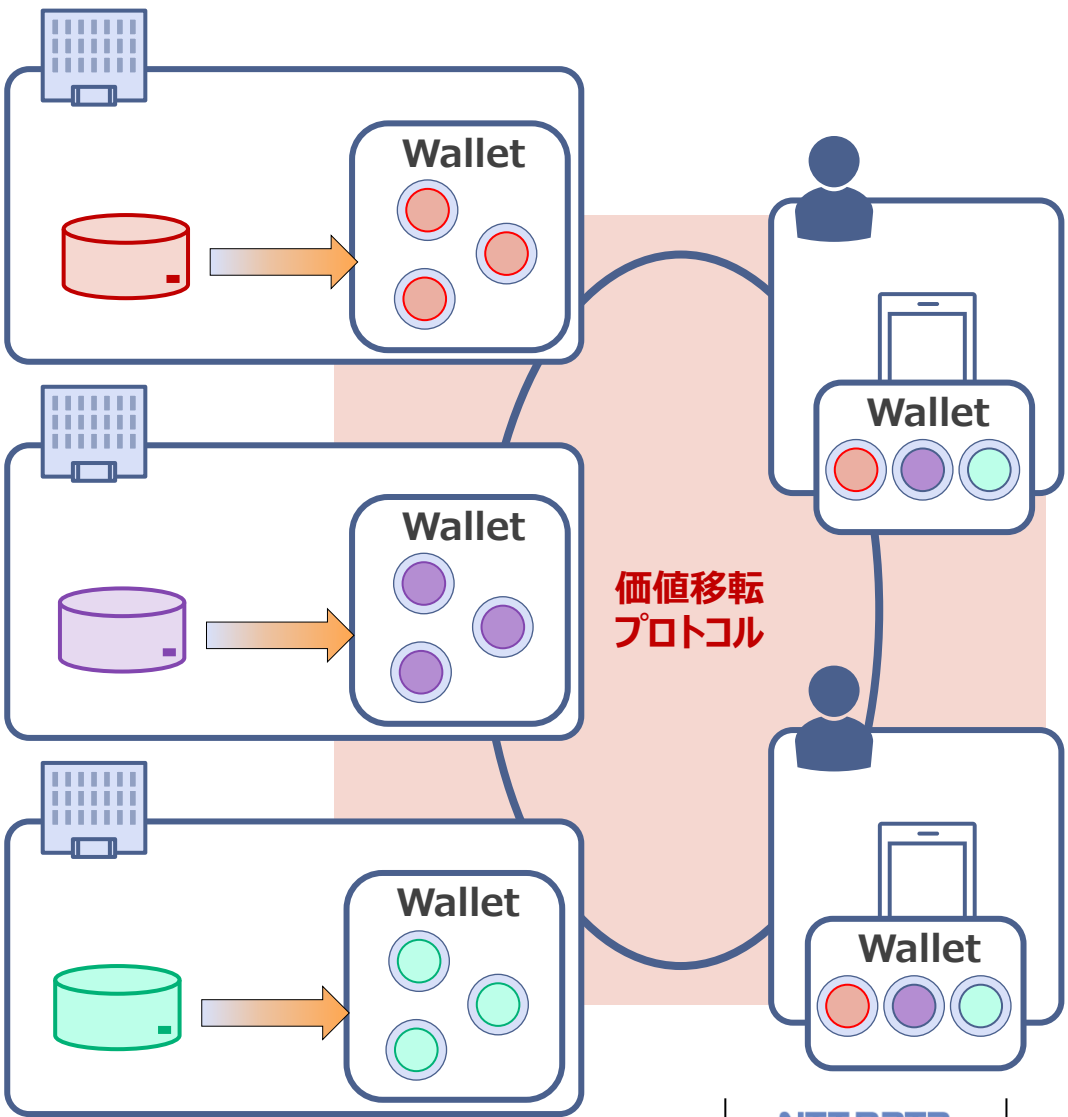


脱サイロ化の実現 ～プラットフォームからプロトコルへ～

台帳システム

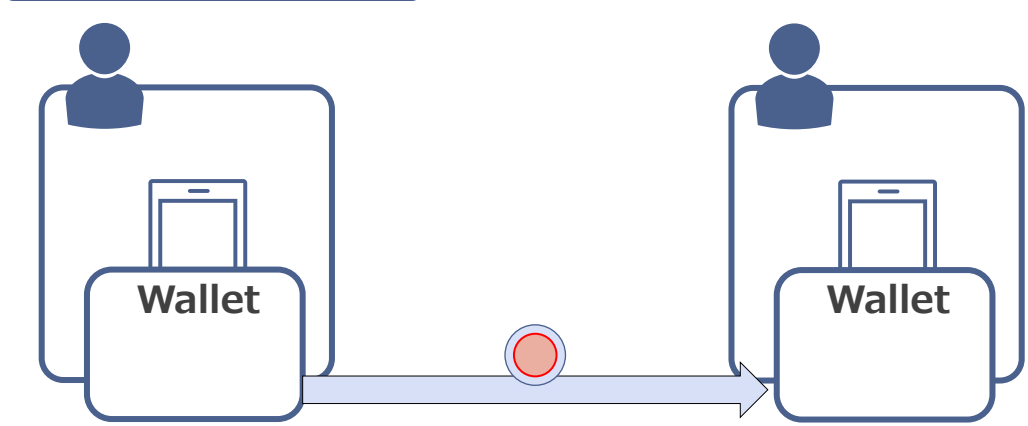


価値移転プロトコル

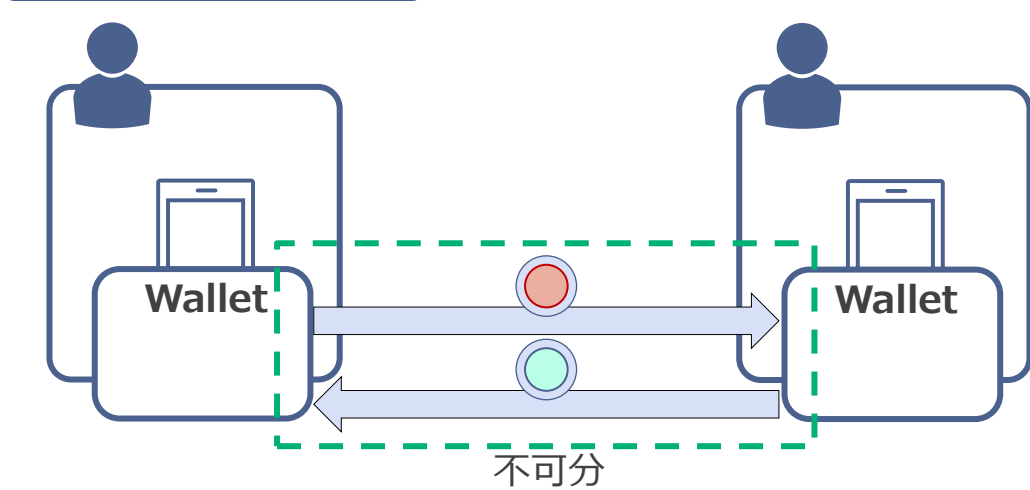


各種転送方式

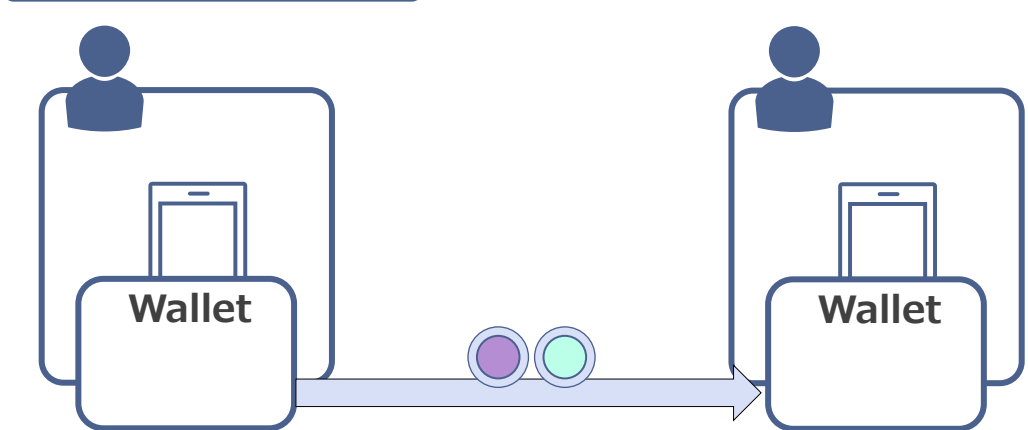
単一転送



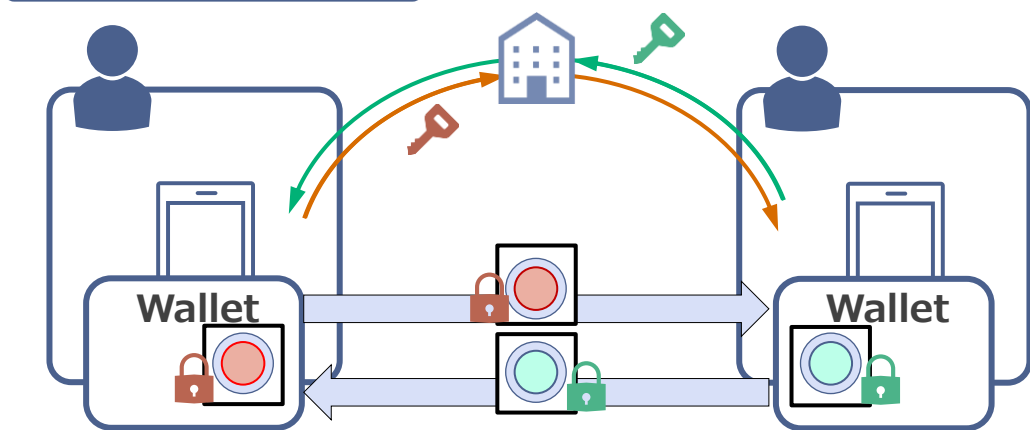
DVP/PVP



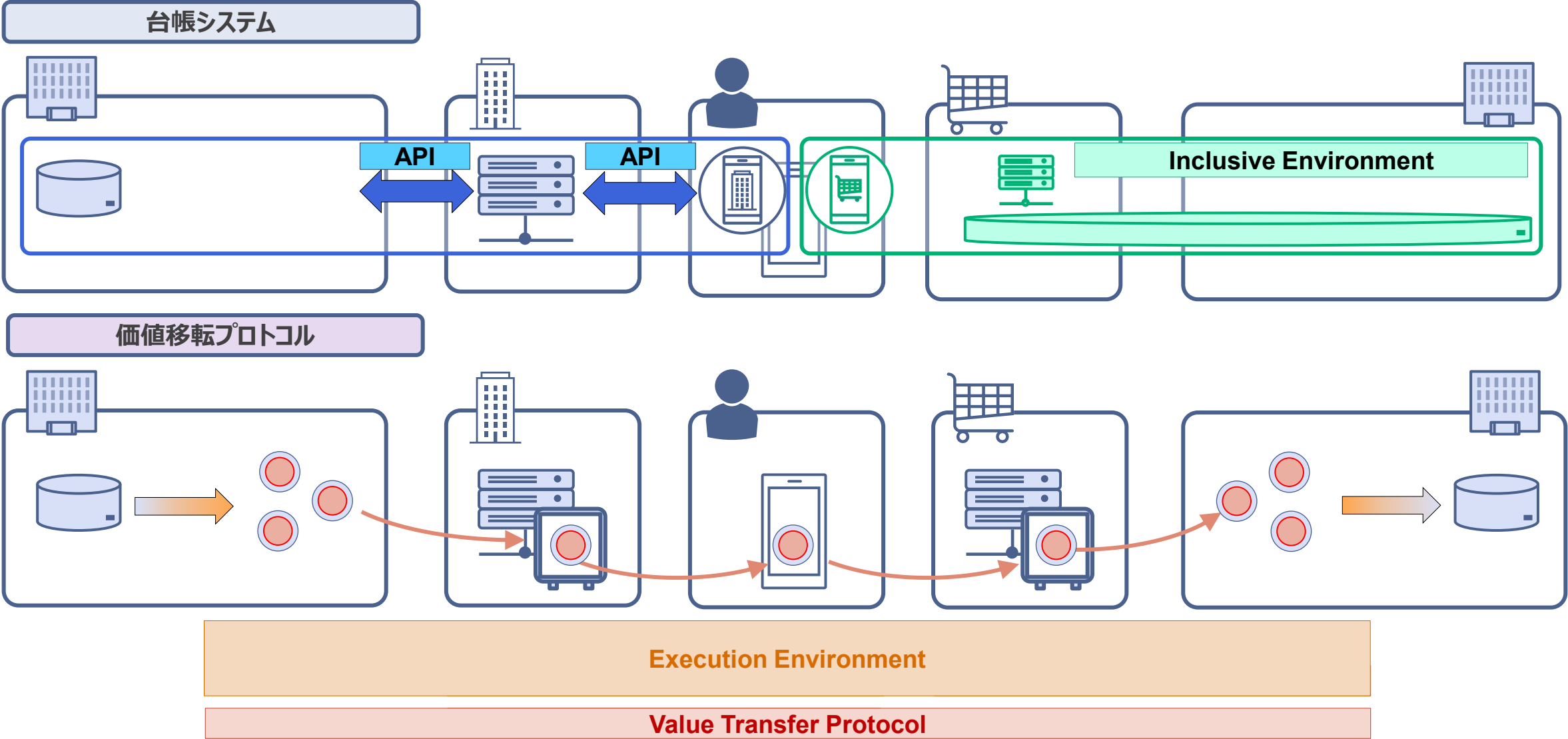
混合転送



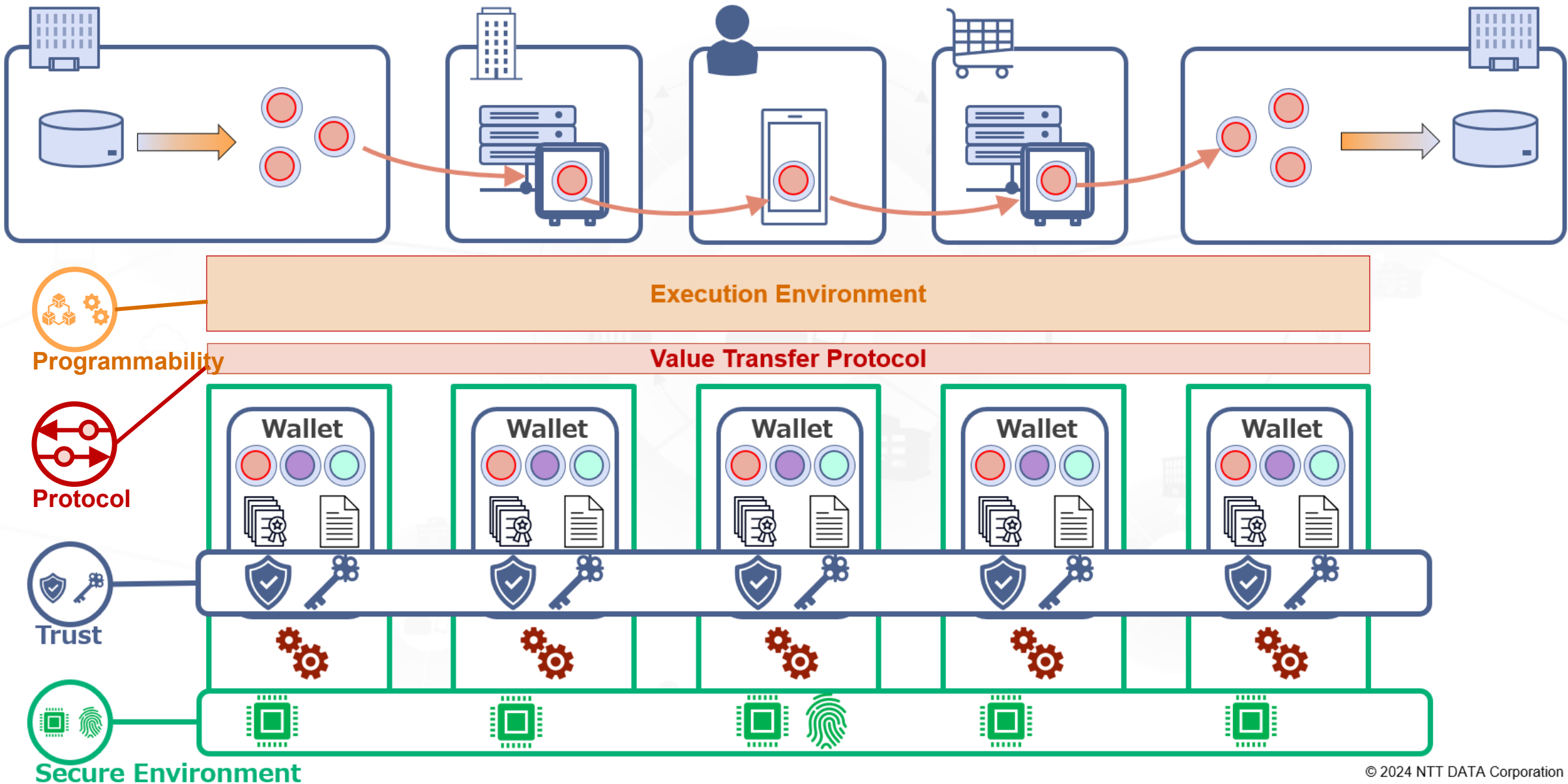
エスクロー



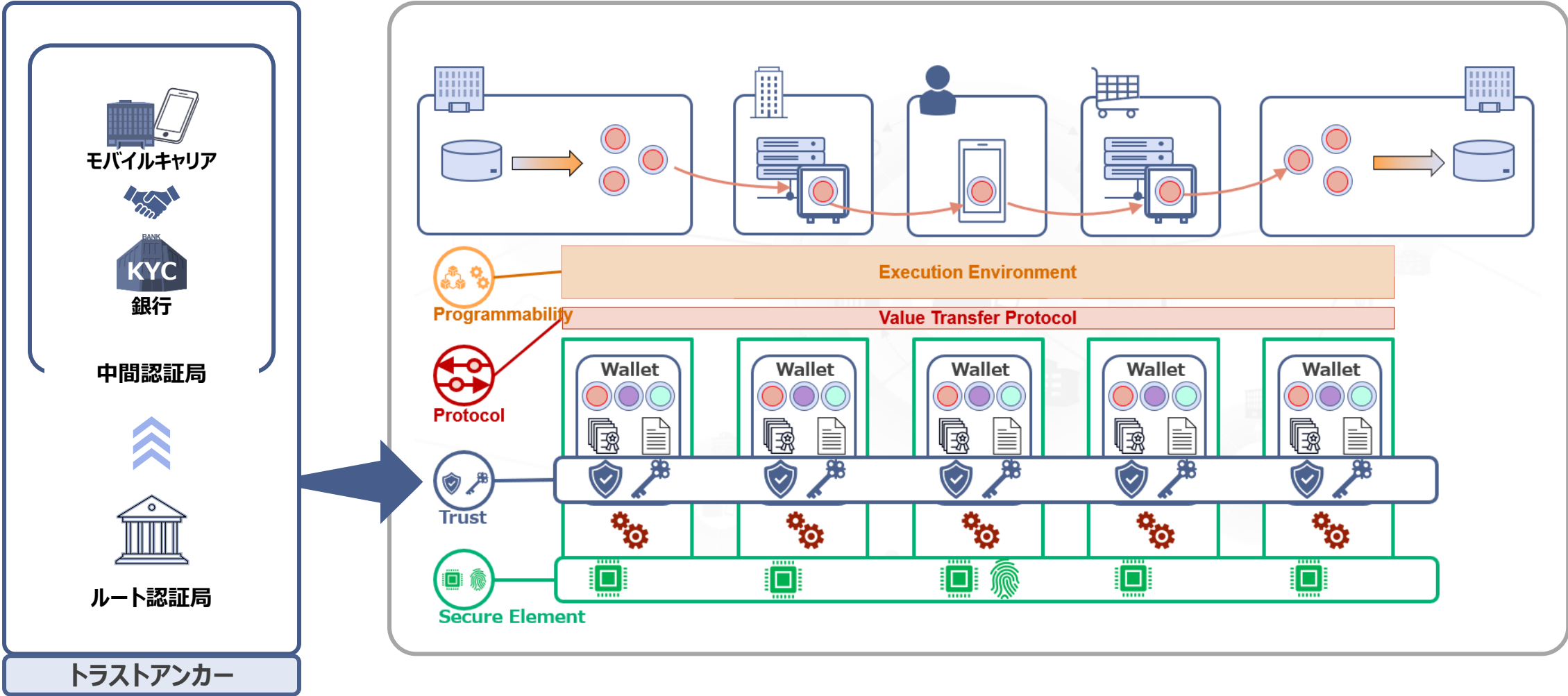
プログラマビリティ



Walletとそれを支えるTrust、Secure Element



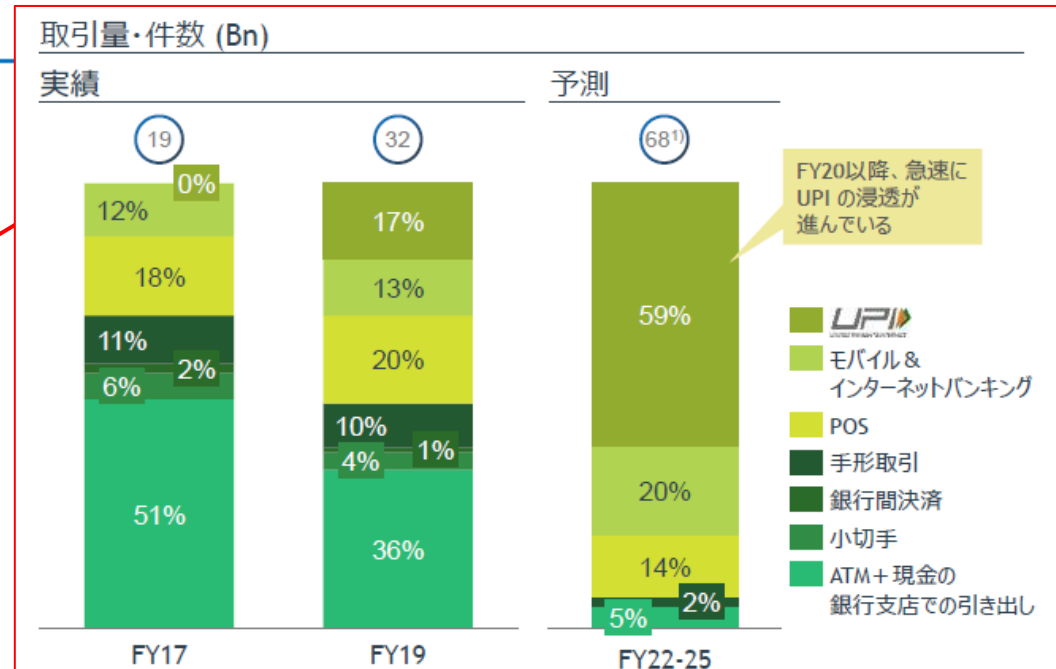
Digital Identity Walletとトラストアンカー



(参考) デジタル・インディア

デジタルアイデンティティ（Aadhaar）を基盤にUPI（インドのファストペイメントサービス）をはじめとする各種ユースケースを実装。
アイデンティティインフラと金融サービスが一体となって整備されている事例。

	目的	対応機能のAPI
Consent Layer (本人の同意のもとでのデータ共有)	プライバシーを確保しながらのデータ共有が可能に	○Consent Artifact ○Account Aggregator
Cashless Layer (キャッシュレス)	金融取引コストを引き下げ	○AEPS ○APB ○UPI
Paperless Layer (ペーパーレス)	紙の書類を減らすことで効率性を向上	○Aadhaar eKYC ○DigiLocker ○eSign
Presence-less Layer (非対面)	いつでもどこでも、その場になくても、本人確認が可能に	○Aadhaar認証 ○Aadhaar eKYC
Aadhaar		

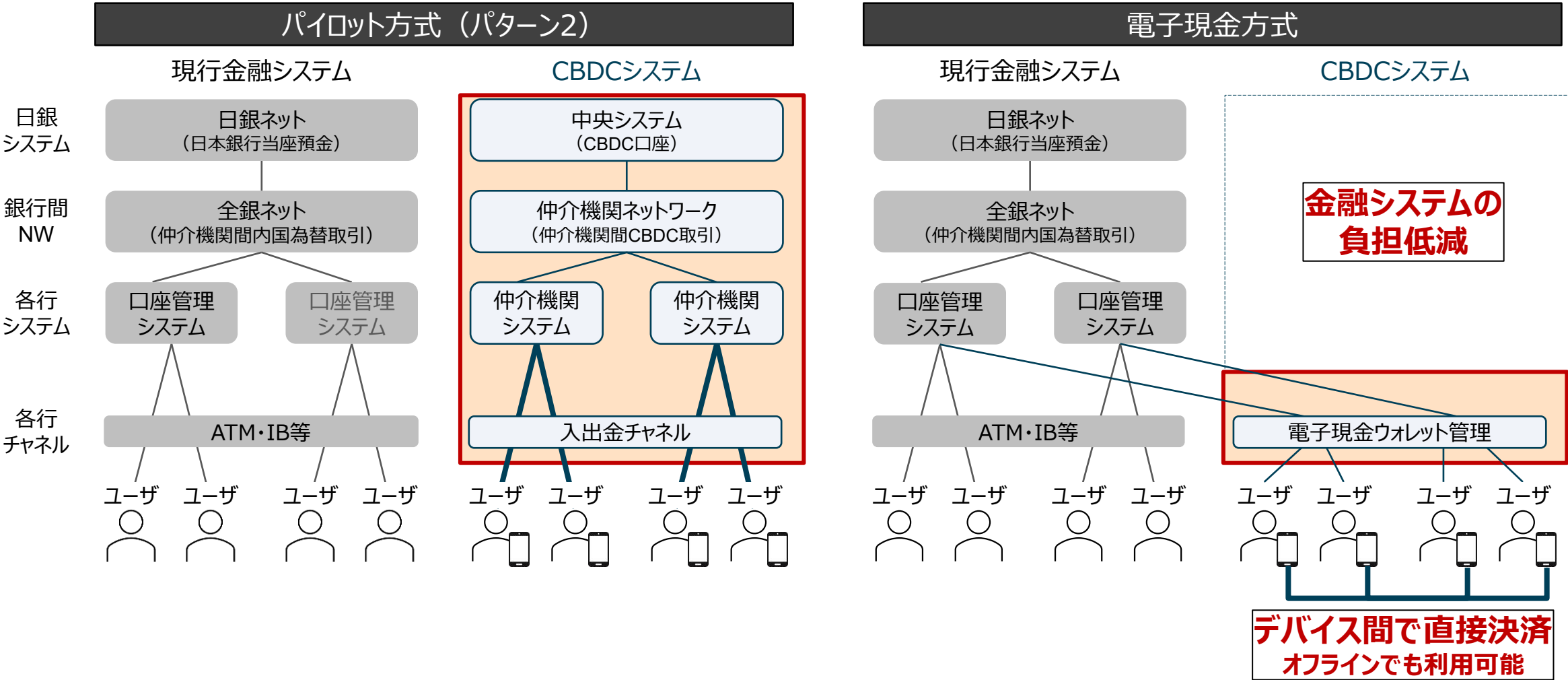


UPIの浸透度合い

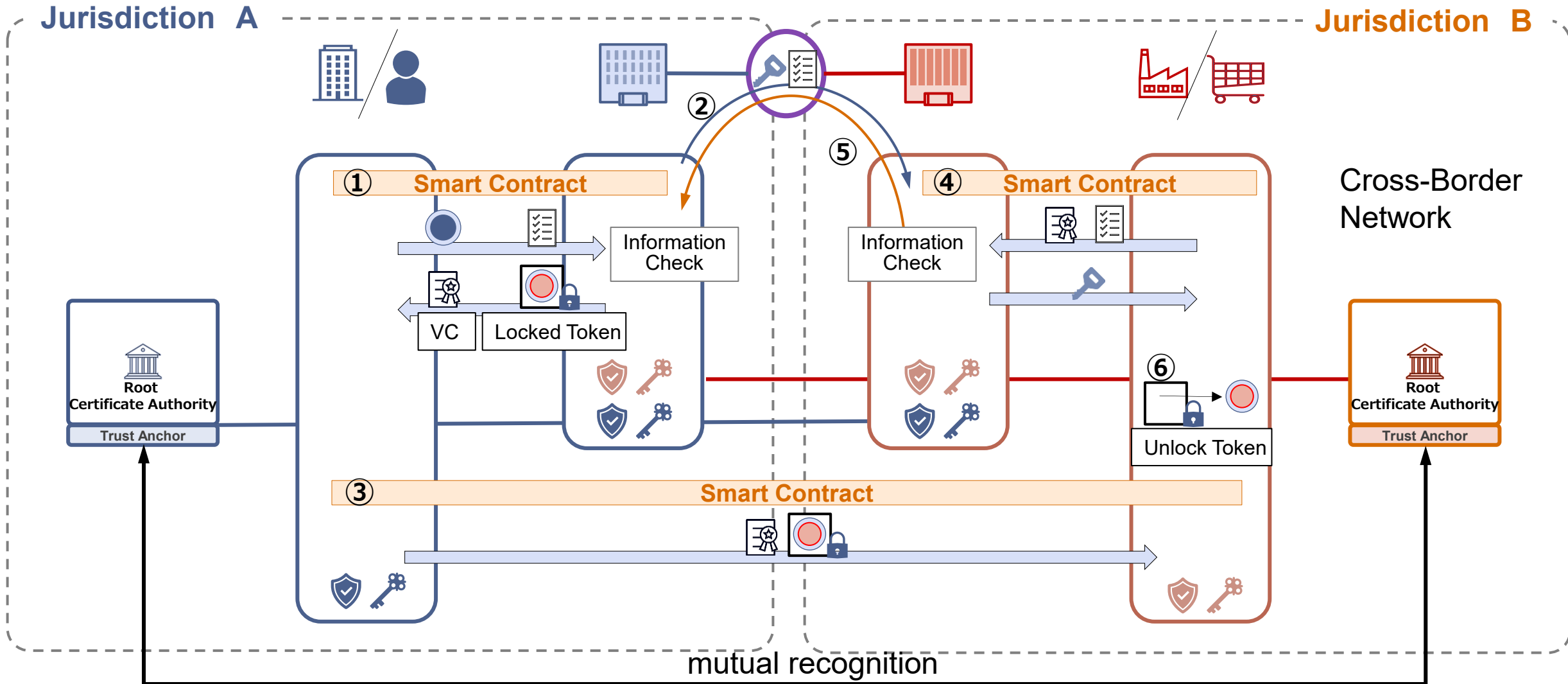
「財務省 財務総合政策研究所 インドワークショップ（令和4年度）」より
<https://www.mof.go.jp/pri/research/conference/indiaws/indiaws2022.html>

CBDCを電子現金で実現する場合

電子現金では現行システムにデバイス間の直接決済を追加することで実現するため、金融システムの全体の負担や投資が低減されます。

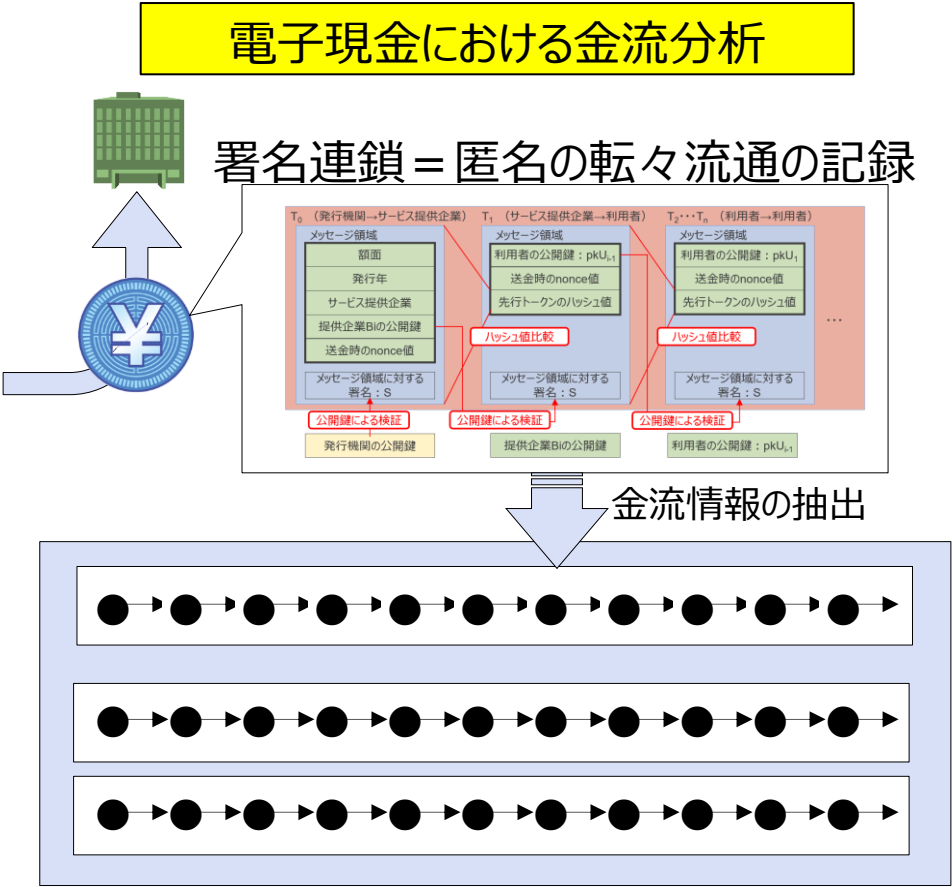


クロスボーダー決済と価値移転プロトコル

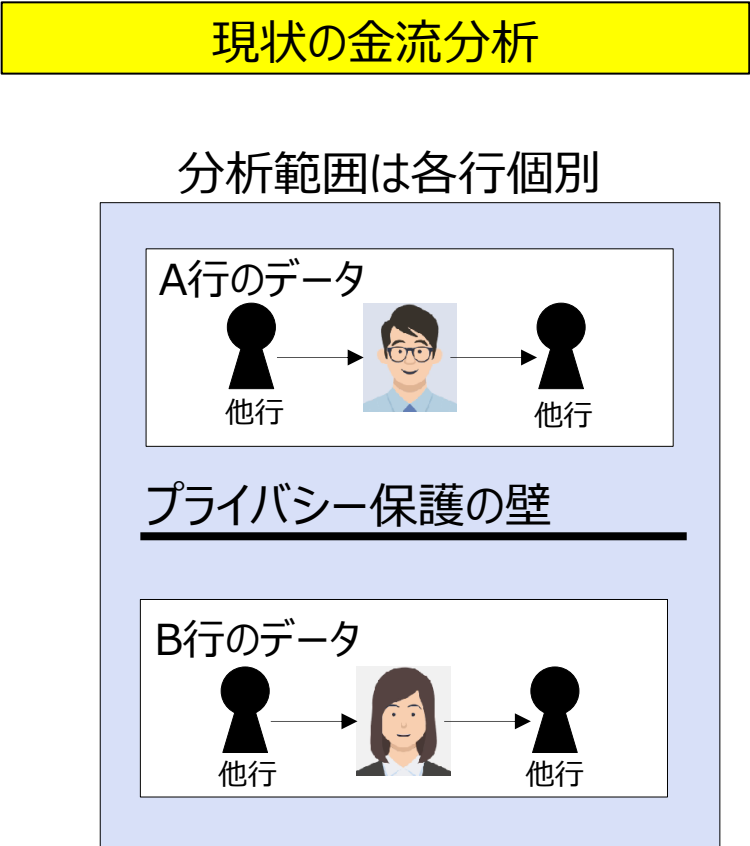


AML/CFT、情報活用における現状との対比

電子現金ではトークンの還収時の検証において、各金融機関は匿名の金流情報を得ることができる。
これを活用してAML/CFTにおけるネットワーク分析や地域の経済分析のインプットとすることが可能。



各行で金融機関に閉じない匿名の金流情報を分析可能



集約しても分析範囲は各行個別

Part.2 セキュア環境他

参考文献のご紹介

本章の内容は下記金融研究所様との共同研究レポートもお読みいただけると幸いです。

台帳を用いない決済方式に関する
技術面からの一考察

たむらゆうこ あべまさゆき おくだてつや つがわひろまさ みやざわとしゆき やまむらかずき
田村裕子・阿部正幸・奥田哲矢・津川天祐・宮澤俊之・山村和輝

あかはねよしはる たぐちともき ひらくりゆうと ますだひろと やまだけんと
赤羽喜治・田口智貴・平栗勇人・増田博人・山田健斗

Discussion Paper No. 2024-J-19

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

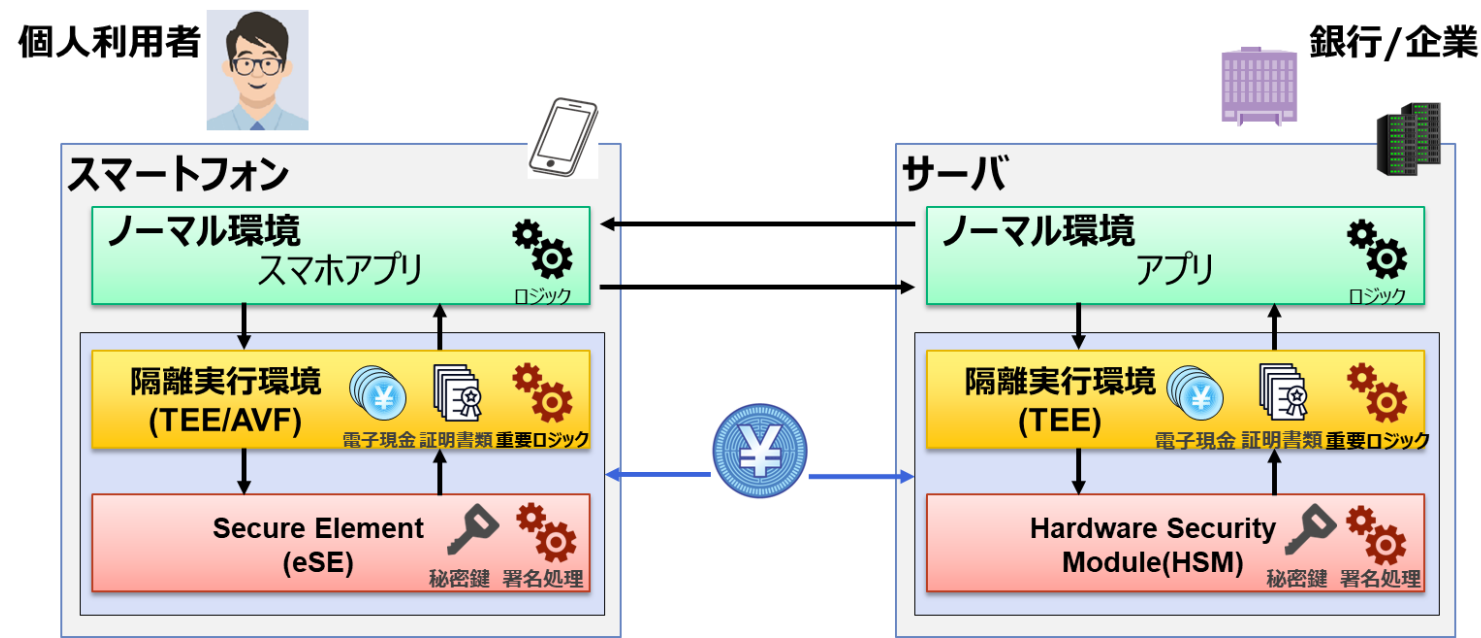
〒103-8660 東京都中央区日本橋本石町 2-1-1

<https://www.imes.boj.or.jp/research/papers/japanese/24-J-19.pdf>
2024年11月公開

1. はじめに	1
2. 電子現金方式の基本構成	3
(1) 台帳方式と電子現金方式との違い	3
(2) 電子現金方式に求められる性質	6
(3) 基本方式	8
(4) セキュリティに関する考察	16
(5) プライバシ保護と透明性に関する考察	18
3. 電子現金方式の実機検証	20
(1) 過去の実証実験	20
(2) 実機検証の概要	21
(3) 実機検証結果	26
4. 電子現金方式の効率化に向けた検討	27
(1) 電子現金の送受信にかかる効率化	28
(2) 電子現金の還収にかかる効率化	30
(3) 変動額面方式に関する考察	30
(4) プライバシを強化した電子現金方式	33
5. おわりに	39
参考文献	41
補論 1. 認証機関の機能を分割した場合の証明書発行手順	44
補論 2. 電子現金方式の効率化	45
(1) 電子現金の送受信にかかる効率化	45
(2) 電子現金の還収にかかる効率化	48
補論 3. プライバシを強化した電子現金プロトコル	49
(1) Σプロトコル	50
(2) 3つの実現方法	51

価値移転の署名・検証ロジックや秘密鍵等を守る仕組み

署名・検証ロジックの改ざんや秘密鍵の漏洩によって電子現金の偽造や複製などの不正が起きないように、これらを隔離実行環境やセキュアデバイスで保護し、安全な価値移転を実現する。



耐タンパ性	デバイス	ロジックの保護	秘密鍵の保護
	スマホサイド 	Runtime Application Self Protection(RASP) スマホアプリに対する不正な入力や攻撃の検知及び阻止 構成証明(アテステーション) 実行するアプリケーションの改ざんを検知する技術 Trusted Execution Environment(TEE)/AVF 隔離された環境でアプリケーションを実行するための技術	embedded Secure Element(eSE) 外部からの解析攻撃への耐性を備えたチップの機能
	サーバサイド 	Trusted Execution Environment(TEE) 通常のOSから隔離された環境でアプリケーションを実行するための技術 構成証明(アテステーション) 実行するアプリケーションの改ざんを検知するための技術	Hardware Security Module(HSM) 外部からの解析攻撃への耐性を備えた秘密鍵管理専用のアプライアンス機器／クラウドサービスの機能

AVF（Android Virtualization Framework）：
チップ間の非互換性を解決するためにGoogleが提唱している
新しい隔離実行環境技術

(参考) GlobalPlatform (GP) について

セキュアコンポーネントの運用管理に関して、世界最有力の国際標準化団体（フォーラム標準）

■ 1999年設立、IoT向けセキュアデジタルサービス・デバイスに関わる団体へと発展

- ・サプライチェーン問題、ゼロトラストなど、Root of Trustとしてのセキュアコンポーネントへの期待の高まり
- ・欧州を中心とした新たなID市場としてのVC、IDウォレット市場の立ち上がり

■ 多様な企業で構成、多くの関連団体とアライアンス形成

- ・メンバー数約90団体、連携パートナー40団体以上
- ・NTTは11人の理事の一人（選挙制、現在アジア唯一・理事最長）

■ 国内からはPKIベースの管理方式や非接触通信方式などで貢献



Elected Board of Directors (11)

- ARM
- G&D (Treasurer)
- FIME (Chair)
- NTT
- Oracle
- Qualcomm
- STMicroelectronics (Vice-Chair)
- Thales
- T-Mobile
- Trustonic
- VISA

Japan Task Force



TOSHIBA

Work Program

Automotive

eID Wallet

Security/SBOM

SC/TPS*

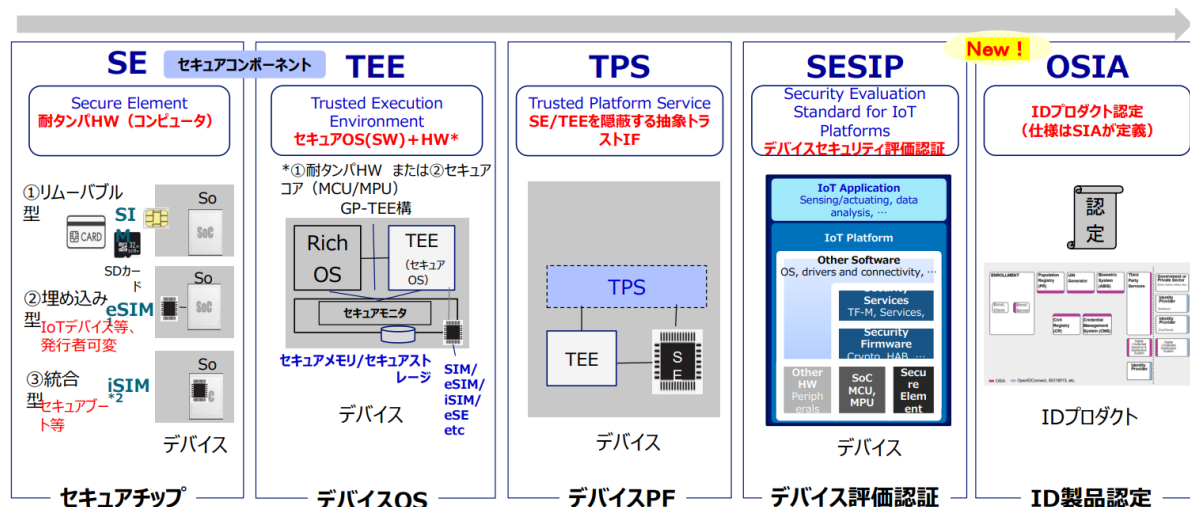
New TRUSTONIC Kenji TAKAHASHI
New THALES Kiseung SUNG
ORACLE Sejoon AHN Koji UNO

FeliCa Networks Masayuki TAKEZAWA
NTT Fumiaki KUDOH

TOSHIBA Takanobu ISHIBASHI Ariyuki KISHIMOTO
NTT Katsumi OSUGA Akira NAGAI

DNP Kensuke TAKAHASHI
NTT Fumiaki KUDOH
FeliCa Networks Masayuki TAKEZAWA

Regular Members
(7社から12名)



SE（セキュアエレメント）、TEE（高信頼実行環境、隔離実行環境）

NTTグループ連携による競争力創出

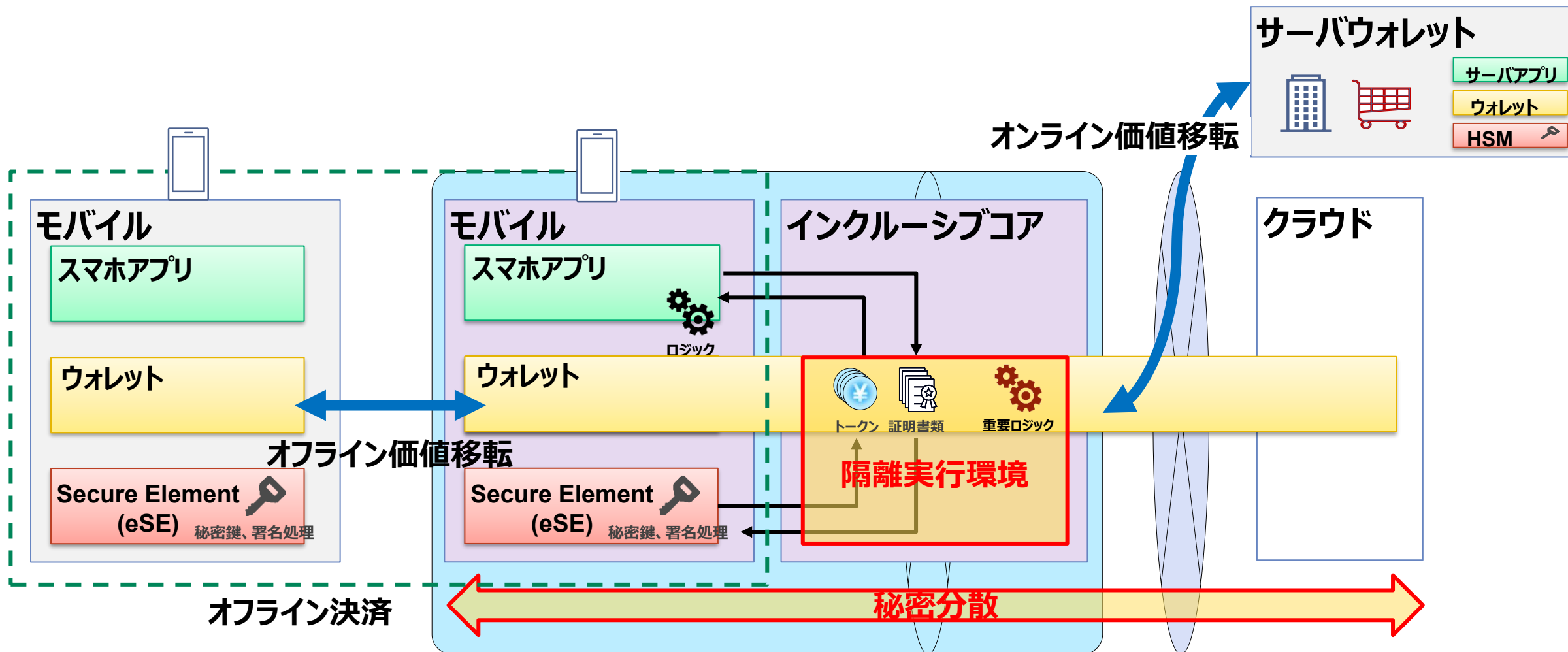
グループ横断（下図参照）の強みを連携し、リテール（モバイル）／エンタープライズ（サーバ） 双方におけるセキュアレイヤを構築し、**デジタル社会における“オセロ盤の端”を確保する**と共に、**標準化活動**を進めていく。



インクルーシブコア（In-Network-Computing）との連携について

価値移転プロトコルを通信インフラ（エッジ）と連携させることで可用性、安全性を確保

- ・オンライン／オフライン双方において透過に価値移転を実現できる技術（防災・強靱化）
- ・キャリアならではの強みを発揮できる“**オセロ盤の角**”を構築（対Google、Apple等）



(参考) BISのProject Polarisレポート

BIS（国際決済銀行）におけるCBDC検討プロジェクトの一つProject Polaris（オフラインペイメント型）から2023年5月レポート公開（当社も協力企業リストに掲載）

※「オフラインペイメント＝台帳を使わないP2P決済」という定義であり「ネットワークを使わない対面決済」ではない。

“Reasons for offline payments with CBDC”

価値移転プロトコルはこの定義によれば全て「オフラインペイメント」

1. Resilience（障害復旧性）
2. Cash resemblance（現金と同じ特性）
3. Inclusion（金融包摂）
4. Lack of developed communications infrastructure
5. Privacy（プライバシー保護）
6. Lower transaction costs（低コスト）
7. Performance and scalability support（性能のスケーラビリティ）
8. Universal access（ユニバーサルアクセス）
9. Civil contingency（災害時対応）
10. Trust（信用性、本人性）
11. Making digital peer-to-peer (P2P) and person-to-business (P2B) payments（直接決済）

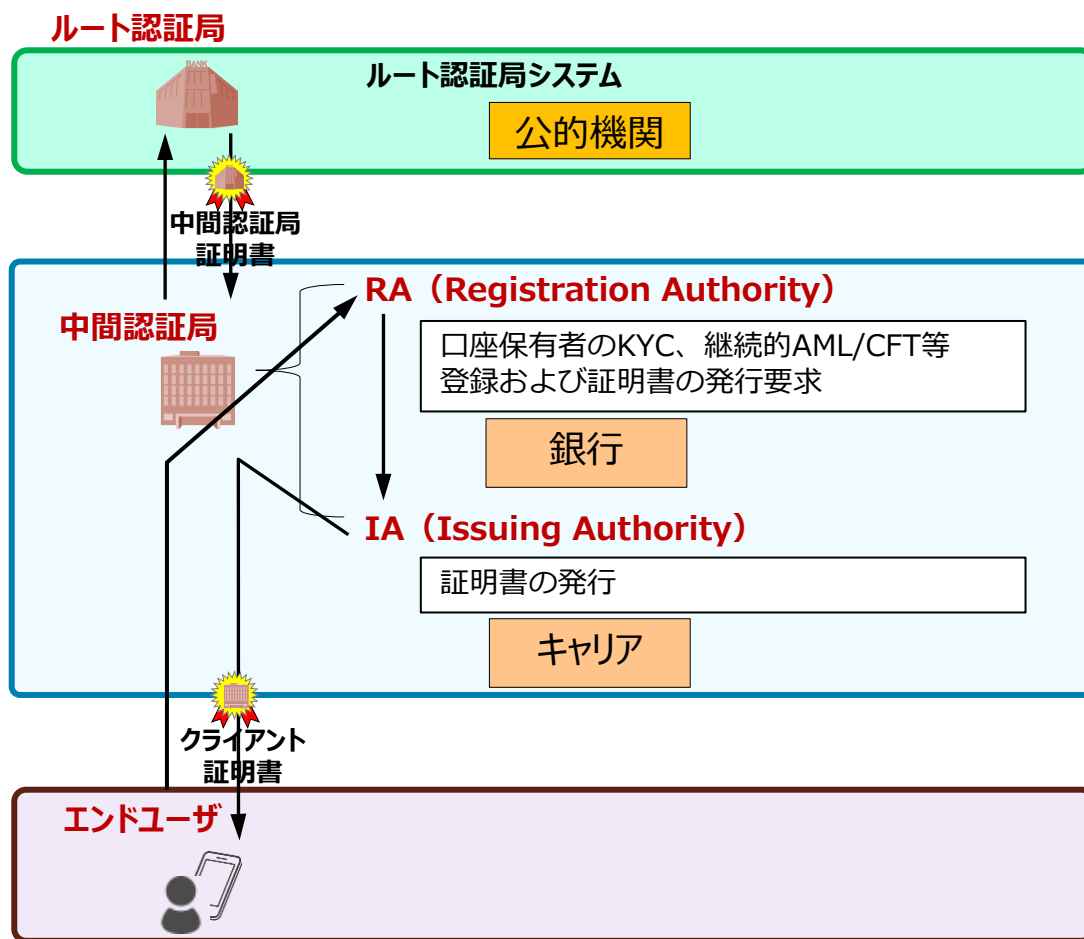


Handbook for offline payments with CBDC

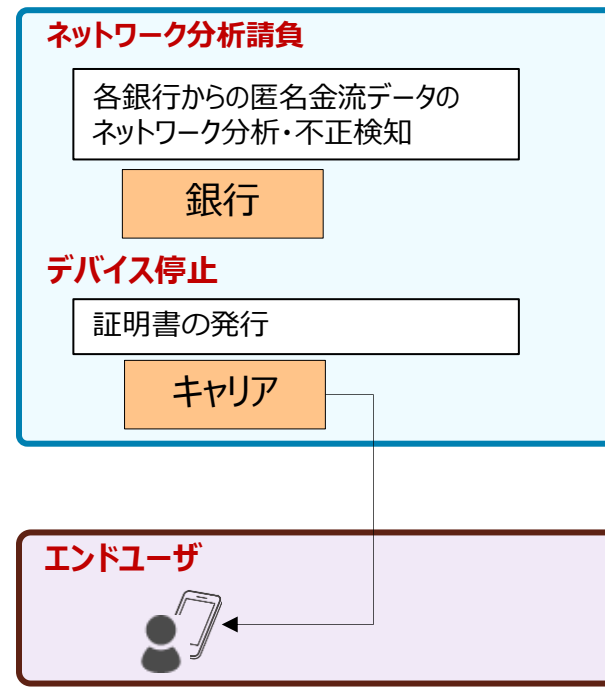
(May 2023)

(参考) CBDCにおけるTrust Anchorのスキーム案 (認証局の構造)

支える仕組①：証明書の流れ

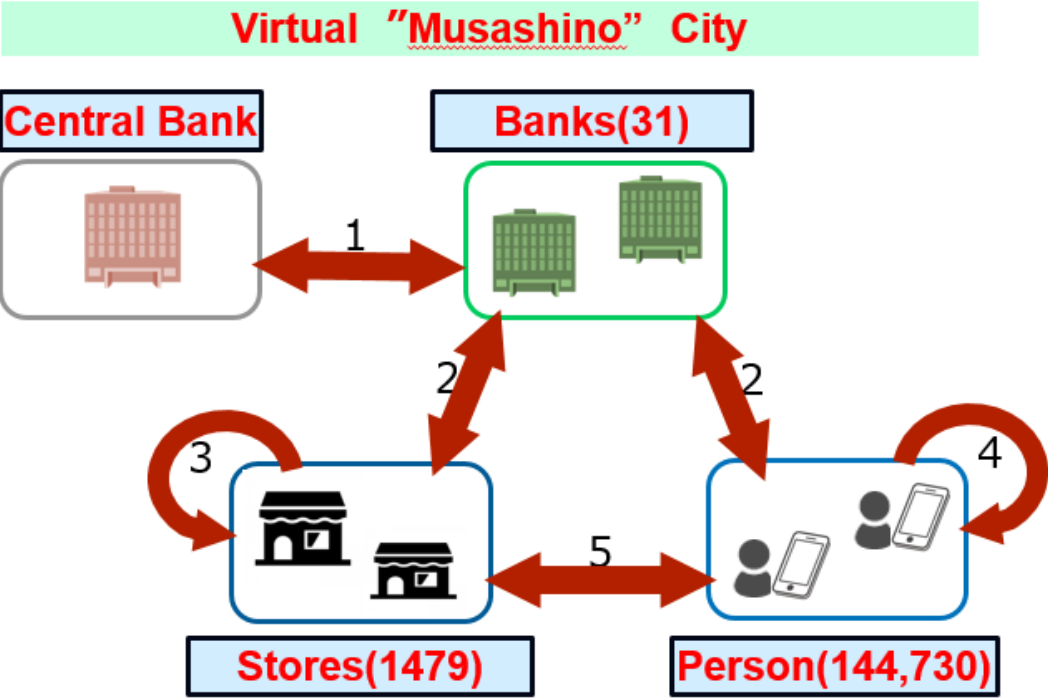


支える仕組②：不正検知／抑止



Modeling and simulation of token flow in market

台帳ベースではないトークンシステムの構築にあたり、ウォレット間移動するトークンの動向、ウォレット内のトークン構成等モデリングとシミュレーションによるフィードバックが必要。
現状“バーチャル武蔵野市”（人口15万人クラス）の都市における1年分のシミュレーション環境を用意してトークン選定アルゴリズムなどの改良を進めている



NO	protocol	sender	receiver	transaction
2	Exchange	Customer	CityBank	902,811
2	Exchange	Shop	CityBank	1,023
2	CashRegister_Reset	Shop	CityBank	539712
3	Remittances	Shop	Shop	539,819
4	Remittances	Customer	Customer	1,458,807
5	ShopPay	Customer	Shop	13,235,519

365 day

ShopPay_Change	Customer	Shop	7,458,109
ShopPay_No_Change	Customer	Shop	5,777,410