ChatGPT PLUS

GPT-4 currently has a cap of 25 messages every 3 hours.

CBDCとはなんですか？

ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May 12 Version

CBDCに関する取り組み
～Corda Tech Meetup 春の陣～

2023年5月

アジェンダ

- CBDCの現在地
- CBDC on Corda
- 3つの実装パターン

SBI R3 Japan

自己紹介

生永 雄輔（いくなが ゆうすけ）

◆SBI Holdings ブロックチェーン推進室 室付部長
◆SBI R3 Japan プロダクトサービス部長→ビジネス推進部長→エンジニアリング部長

＜略歴＞
兵庫県出身→大学から上京→**ＩＴ⇔金融**
学生時代　　：ゲーム理論・離散数学 (東大院修士@2004)
ITベンチャー：2000-2004（現像した**写真をネットで共有**）
2009-2013（自動車/船舶/発電所むけ**大型図面管理**）
金融機関　　：2004-2009（メガバンクで市場調査及び企画）
2013-2018（農林系金融機関で投資運営/企画/当局対応）
2018年SBIへJoin

CBDCの現在地

CBDCの３つの分類

	ホールセール(w-CDBC)	リテール(r-CDBC)	クロスボーダーCBDC
AE 先進国[1]	主に金融機関の間で活用されるCBDC	主に個人が使用することを想定したCBDC	国境を跨いだ取引にCBDCを活用する場合
EMDE 新興市場と発展途上国経済[1]			

1. Classification of AEs and EMDEs based on IMF World Economic Outlook classification, as of Apr 2020
Sources: BIS Working Paper 976, CBDC: Motives, economic implications and the research frontier, Nov 2021. BIS Working Paper 123, CBDCs in emerging market economies, Apr 2022 FIS, Triggers for CBDC Demand and Adoptio research

現状

BOE: デジタル ポンド *(r-CBDC)*
- オープン バンキングAPI
- 政策検討

米国連銀: デジタルドル
(w&r-CBDC)
- 政策に関する議論: USDの役割、CBDCをめぐる市民的自由
- 民間部門によるデジタルドルへの取り組み

ECB: デジタル ユーロ *(r-CBDC)*
- プライバシー
- 仲介の排除
- インターオペラビリティ

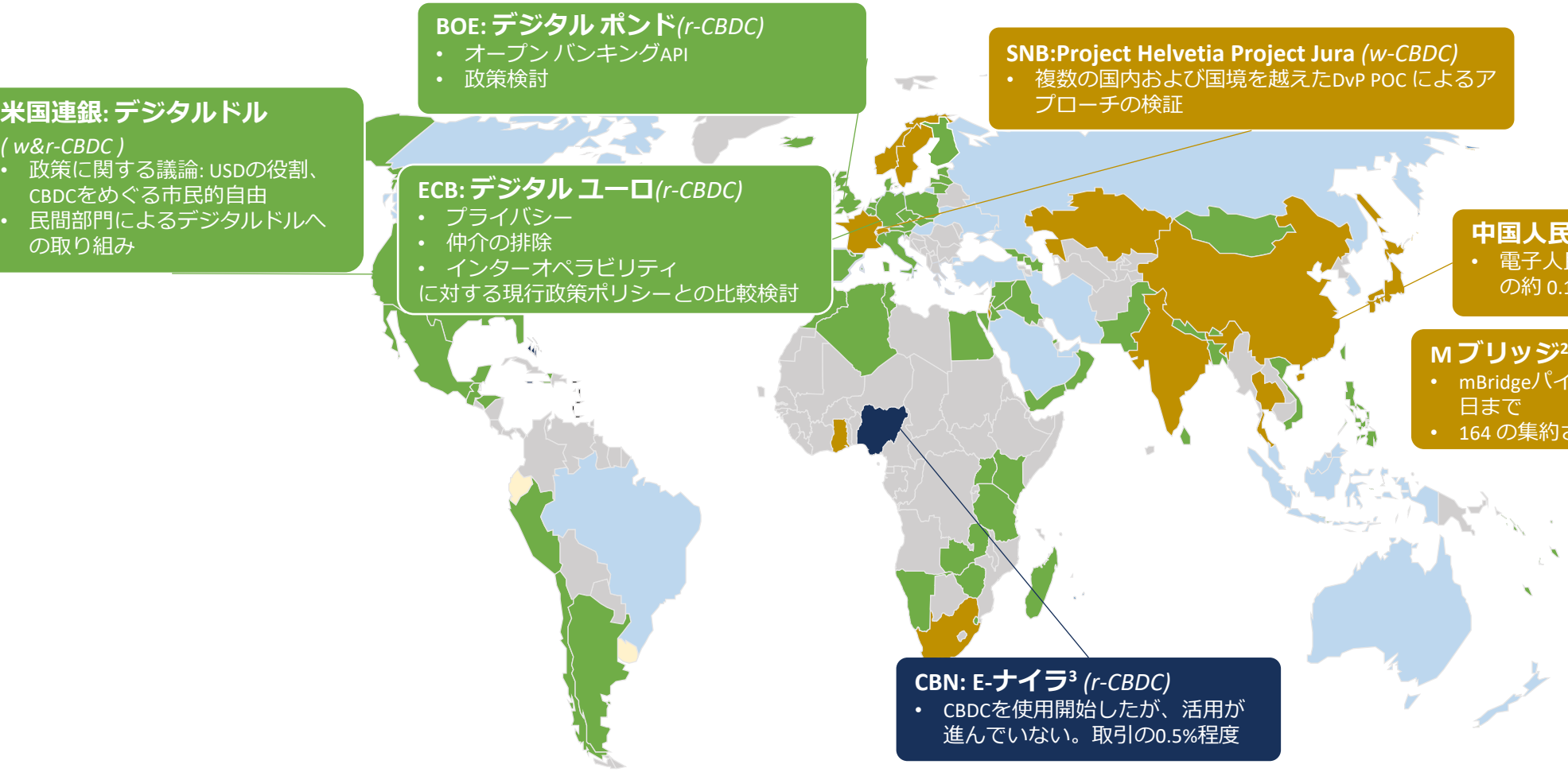
に対する現行政策ポリシーとの比較検討

SNB:Project Helvetia Project Jura *(w-CBDC)*
- 複数の国内および国境を越えたDvP POC によるアプローチの検証

中国人民銀行: e-CNY [1] *(r-CBDC)*
- 電子人民元の流通額は約 20 億ドル、CIC の約 0.13 %。累計売上高は140億米ドル

M ブリッジ [2] *(m-CBDC)*
- mBridgeパイロットは 2022 年 8 月 15 日から 9 月 23 日まで
- 164 の集約されたトランザクション~2,200 万米ドル

CBN: E-ナイラ [3] *(r-CBDC)*
- CBDCを使用開始したが、活用が進んでいない。取引の0.5%程度



商用 (4)　パイロット (14)　開発 (14)　研究 (59)　キャンセル (2)

1. 人民銀行　2022 年 12 月現在
2. BIS、2022 年 10 月
3. ブルームバーグ、2022 年 10 月

2023 年 3 月末の時点で、世界の GDP の 90% 以上を占める 91 か国が CBDC ソリューションを検討しています。

動向

1 成熟[1]

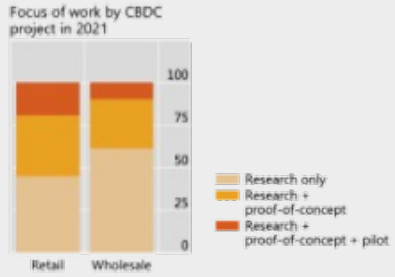


図 *1: CBDC* に関する *BIS* 調査、*2022* 年 *5* 月

- **リテールCBDC（もしくはホールセールとリテールの両方）**に焦点
- 使い捨てPoCからプロダクションへ

プロダクション

2 政策に対する新しいツール

図 *2:* インドネシアのデジタルルピー（*dIDR*）はインドネシア中銀の政策目標に。

図 *3: mBridge*の概要

- **経済および政策目標を**推進する基盤としての CBDC

政策目標が設計を決める

3 最適な設計への自信

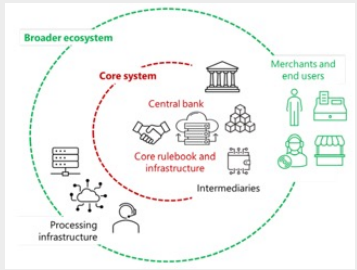


図 *4: 2* 層 *CBDC* モデル[2]の図

- **２層モデルの発見**
  ＞ホールセールとリテールの分離
  ＞ガバナンスとイノベーションのバランス

２層モデル

4 クロスボーダー取引

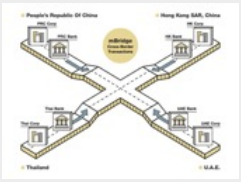


図 *5:* プロジェクト *mBridge*

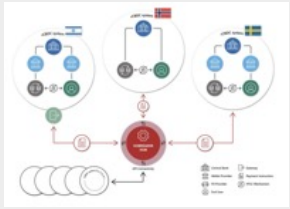


図 *6:*プロジェクト *IceBreaker* スウェーデン、ノルウェー、イスラエル

- **国家主導/国際機関主導のイニシアチブ**
- 例： mBridge 、BIS Open Tech

国際協力の戦略的ツール

1: BIS Paper 125: Gaining momentum – Results of the 2021 BIS survey on central bank digital currencies, May 2022
2: BIS : Central bank digital currencies – system design and interoperability, Sep 2021

動機

通貨主権（金融調節機能の維持）レジリエンス（金融危機耐性）

	ホールセール(w-CDBC)	リテール(r-CDBC)	クロスボーダー
AE 先進国[1]	• 安定と**レジリエンス** • アクセスの拡大 **スイス** Helvetia/ E-Franc **オーストラリア** RBA research	• **通貨主権**と**レジリエンス** • 金融包摂 **USA** Digital Dollar **EU** Digital Euro **イギリス** Digital Pound	• **通貨主権** • 効率性 **香港** E-HKD **シンガポール** Ubin+
	イノベーションの原動力としてのプログラマビリティ、コンポーザビリティ、相互運用性		
EMDE 新興市場と発展途上国経済[1]	• 効率性と**レジリエンス** • DeFi/暗号通貨との相互運用性 **ブラジル** Digital Real **カザフスタン** Digital Tenge **インドネシア** Digital Rupiah	• 金融包摂、**オフライン決済** • キャッシュレス社会への一足飛びの移行 **バハマ** Sand Dollar **ナイジェリア** eNaira **ECCB** D-Cash	• **通貨主権** • 効率性 **ブラジル** Digital Real **インド** eRupee **中国** 電子人民元

SBI R3 Japan

1. Classification of AEs and EMDEs based on IMF World Economic Outlook classification, as of Apr 2020

Sources: BIS Working Paper 976, CBDC: Motives, economic implications and the research frontier, Nov 2021. BIS Working Paper 123, CBDCs in emerging market economies, Apr 2022 FIS, Triggers for CBDC Demand and Adoptio research

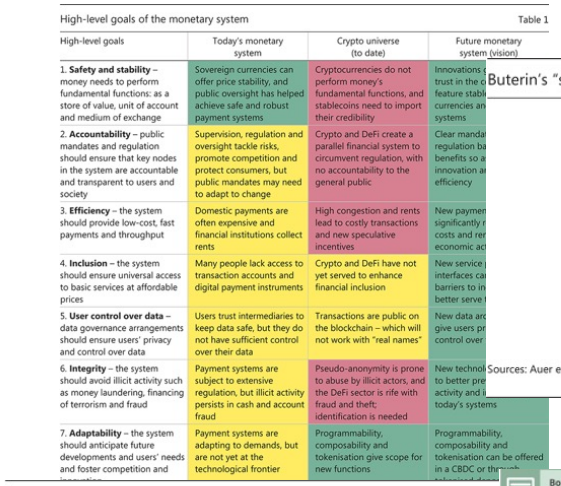
Topic: BIS Annual Report@2022/6

- 暗号通貨は通貨システム基盤として不適当。

- CBDCとFast Payment Systemは、
  - ✓ Programmability
  - ✓ Composability
  - ✓ Tokenization

  を実現可能。

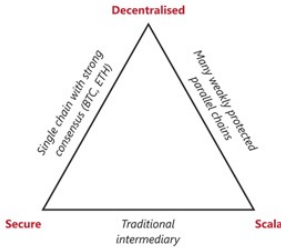
- 暗号通貨が持つ構造的課題の解決策の一つとしてCordaが紹介されている。
- ZKPは使えないと言い切られている。



High-level goals of the monetary system — Table 1

High-level goals	Today's monetary system	Crypto universe (to date)	Future monetary system (vision)
1. **Safety and stability** – money needs to perform fundamental functions: as a store of value, unit of account and medium of exchange	Sovereign currencies can offer price stability, and public oversight has helped achieve safe and robust payment systems	Cryptocurrencies do not perform money's fundamental functions, and stablecoins need to import their credibility	Innovations in trust in the … feature stable currencies an… systems
2. **Accountability** – public mandates and regulation should ensure that key nodes in the system are accountable and transparent to users and society	Supervision, regulation and oversight tackle risks, promote competition and protect consumers, but public mandates may need to adapt to change	Crypto and DeFi create a parallel financial system to circumvent regulation, with no accountability to the general public	Clear mandat… regulation ba… benefits so a… innovation a… efficiency
3. **Efficiency** – the system should provide low-cost, fast payments and throughput	Domestic payments are often expensive and financial institutions collect rents	High congestion and rents lead to costly transactions and new speculative incentives	New paymen… significantly r… costs and re… economic ac…
4. **Inclusion** – the system should ensure universal access to basic services at affordable prices	Many people lack access to transaction accounts and digital payment instruments	Crypto and DeFi have not yet served to enhance financial inclusion	New service… interfaces ca… barriers to in… better serve …
5. **User control over data** – data governance arrangements should ensure users' privacy and control over data	Users trust intermediaries to keep data safe, but they do not have sufficient control over their data	Transactions are public on the blockchain – which will not work with "real names"	New data arc… give users pr… control over …
6. **Integrity** – the system should avoid illicit activity such as money laundering, financing of terrorism and fraud	Payment systems are subject to extensive regulation, but illicit activity persists in cash and account fraud	Pseudo-anonymity is prone to abuse by illicit actors, and the DeFi sector is rife with fraud and theft; identification is needed	New technol… to better pre… activity and i… today's systems
7. **Adaptability** – the system should anticipate future developments and users' needs and foster competition and …	Payment systems are adapting to demands, but are not yet at the technological frontier	Programmability, composability and tokenisation give scope for new functions	Programmability, composability and tokenisation can be offered in a CBDC or th…

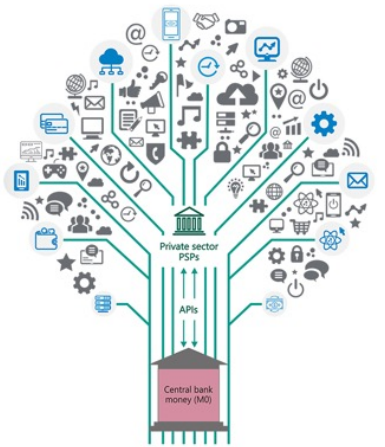
Buterin's "scalability trilemma" — Graph 3



Sources: Auer et al (2021); Buterin (2021).

© Bank for International Settlements

A metaphor: central bank as tree trunk supporting a diverse ecosystem



API = application programming interface; PSP = payment service provider.

Source: BIS.

© Bank for International Settlements

Box C
Making use of DLT with central bank money

In a permissionless blockchain used for crypto applications, all transactions are public. Privacy is maintained by hiding the user's real identity behind a private key. In this sense, there is *pseudo-anonymity*. By contrast, a monetary system based on users' real names raises the question of how to safeguard their privacy. Privacy has the attributes of a fundamental human right. Nobody else needs to know from which supermarket an individual buys their groceries. Therefore, a basic task of a decentralised monetary system based on real names is to find a way to ensure both that the ledger is secure without the need for a central authority, while at the same time preserving the privacy of the individual transactions.

One possible route is through permissioned DLT systems. In these systems, only select users that meet eligibility requirements can obtain access. Interactions between system participants are thus invisible to people outside the system. One example is the permissioned DLT system Corda, which is used by private financial institutions (eg for trade finance platforms) and in a number of central bank wholesale CBDC projects, including Projects Helvetia, Jura and Dunbar at the BIS Innovation Hub.

In Corda, updates to the ledger are performed through a validation function and a uniqueness function. Validation, which involves checking that the details of the transaction are correct and that the sender has the available funds, is done by the system participants. In fact, only the participants that are involved in a transaction are responsible for validating it. Checking that the sender has a valid claim to funds does not, however, ensure that they will not attempt to spend those same funds twice. Transaction uniqueness (ie the prevention of double-spending) is ensured by a centralised authority called a "notary". Notaries have access to the entire ledger and hence can ensure that funds being used in a particular transaction are not being used elsewhere. In the case of wholesale CBDCs, a natural candidate for the notary is the central bank, as this institution already plays a similar role in maintaining the integrity of the overall transaction record in centralised systems.

In such permissioned systems, a tension can arise between payment integrity and transactional privacy. Transactional privacy in a peer-to-peer exchange means that only the two participants involved in a transaction can see that it occurs – very much like when one person hands over a one-dollar bill to a friend. In the case of a digital banknote, the validation process performed by the participants requires that the recipient can trace the banknote back to its origin, which in turn entails seeing every one of the banknote's previous holders. In the context of Corda, this is called the "backchain problem". While the system does not allow everyone to see everything, it does allow participants to have a view beyond their own transactions. Solving the backchain problem is an important design problem in central bank CBDC

https://www.bis.org/publ/arpdf/ar2022e3.htm より

ユースケースが求める技術への要求

ユースケース	プライバシー	スケーラビリティ（同時取引数）	スケーラビリティ（残高増）
ホールセール w-CDBC	低	低	高
リテール r-CDBC	高	高	低
クロスボーダー CDBC	？ まだこれから	中	中

SBI R3 Japan

SBI R3 Japan

CBDC on Corda

Cordaを利用したCBDC プロジェクト

Project Jasper
カナダ銀行、2016+
DLT ベースの RTGS再考
***W-CBDC** (国内、クロスボーダー)*

E-krona
スウェーデン国立銀行、2020+
R-CBDC

Project Icebreaker
スウェーデン国立銀行、ノルゲス銀行、イスラエル銀行、2023+
***R-CBDC** (国内、クロスボーダー)、PvP*

Project Helvetia
スイス国立銀行、BISIH、スイス取引所、2020+
***W-CBDC** (国内)*
dFMI DvP

Digital Tenge
カザフスタン国立銀行、
2021+
R-CBDC

ブータン
アジア開発銀行
ブータン王立通貨庁、2022+
W-CBDC* および *R-CBDC

Project Jura
スイス国立銀行、フランス銀行、BISIH、スイス取引所、2020+
***W-CBDC** (国内、クロスボーダー)、 dFMI DvP*

India CBDC Design Study
インド準備銀行、2021+
W-CBDC* および *R-CBDC

Project LionRock
香港金融管理局、2018+
***W-CBDC** (国内, クロスボーダー)*

National CBDC Project
GCC諸国／地域
2022+
***W-CBDC* および *R-CBDC* (国内)**

Project CBDCPh
フィリピン中央銀行、2022+
***W-CBDC*（国内）**

Digital Dirham
アラブ首長国連邦中央銀行
2022+
W-CBDC* (国内、クロスボーダー) および *R-CBDC

Project Ubin
シンガポール金融管理局 2017+)
DLT ベースの RTGS再設計
および***W-CBDC** (国内およびクロスボーダー)*

Project Inthanon
タイ銀行、2018+
DLT ベースの RTGS再設計
および***W-CBDC** (国内、クロスボーダー、DvP)*

Digital Real Challenge
Banco Central do Brasil、 Feberan と協力、2022+
***W-CBDC*、** *DvP*

Project Dunbar
Bank Negara Malaysia、シンガポール金融管理局、オーストラリア準備銀行および南アフリカ準備銀行、2022+
***W-CBDC* クロスボーダー**

PIC 向けの評価
アジア開発銀行
太平洋島嶼国 6 ヶ国、
2022+
W-CBDC*、*R-CBDC

Project Khoka
南アフリカ準備銀行、2020+
W-CBDC (国内)、CSDとのDvP

R3 主導
パートナー主導

SBI R3 Japan

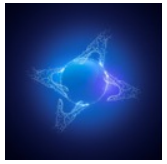
DvP – 配送と支払い,　　dFMI – デジタル金融市場インフラストラクチャ

4つの事例

- e-Krona（スウェーデン）

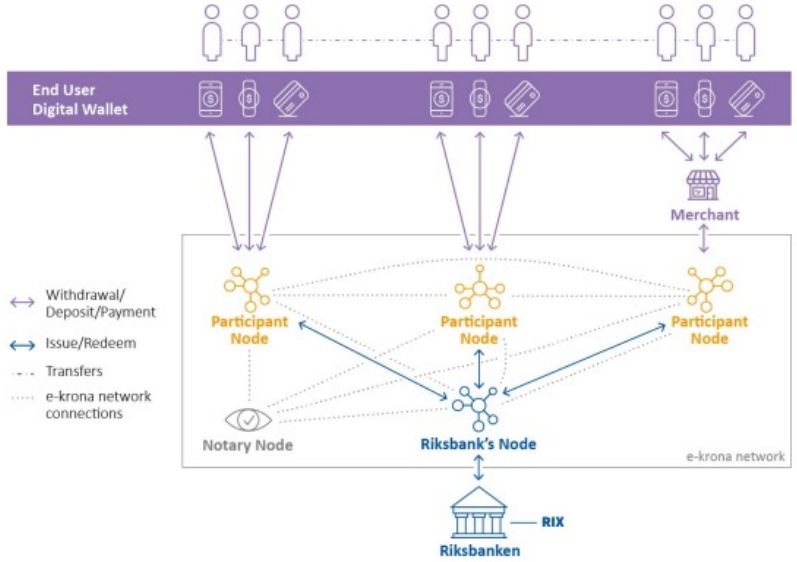
- The Digital Dirham（UAE）

- Digital Tenge（カザフスタン）



- Project Dunbar
  (BIS-SG, オーストラリア、マレーシア、シンガポール、南アフリカ)

e-Krona（スウェーデン）

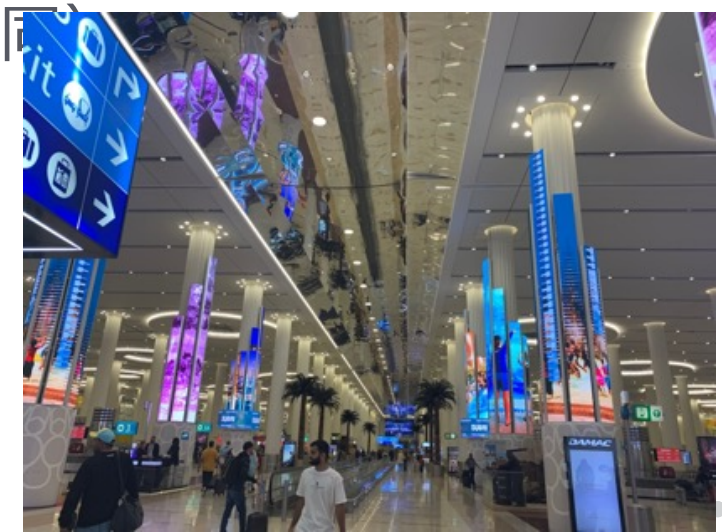


- モチベーション
  - ✓ **現金使用量の激減への対処（＝通貨主権の確保）**
    - FPS※の増加による「民間負債」による決済の増加
    - 中銀負債に引き戻すことによる金融インフラの脆弱化回避
    - ガバナンスとイノベーションの両立
- これまでの歩みと成果
  - ✓ Phase1：1層CBDCと既存インフラ結合
  - ✓ Phase2：オフラインによる仮決済の実現とパフォーマンス
  - ✓ Phase3：
    - 強制決済力の維持とプログラマブルマネーの共存
    - **クロスボーダー決済**（Project Icebreaker）

※ FPS: First Payment System

The Digital Dirham（UAE）

- モチベーション
  - ✓ **国のDX**の一環（キャッシュレス社会への移行）
  - ✓ 金融包摂
- これまでの歩みと成果
  - ✓ Project Aber@2020 ：サウジアラビアとの**クロスボーダー決済**技術実証
  - ✓ mBridge@2022：**クロスボーダー決済**のパイロット実施
    （香港、タイ、中国、BIS-HKと共同）
  - ✓ The Digital Dirham
    - ➢ mBridgeによる貿易決済のパイロット実施
    - ➢ インドとのCBDC同士のby-late決済のPoC
    - ➢ 国内向けCBDC（リテール、ホールセール）のPoC



SBI R3 Japan

Digital Tenge（カザフスタン）

- モチベーション
  - ✓ 金融包摂
  - ✓ **金融セクターの競争力確保**

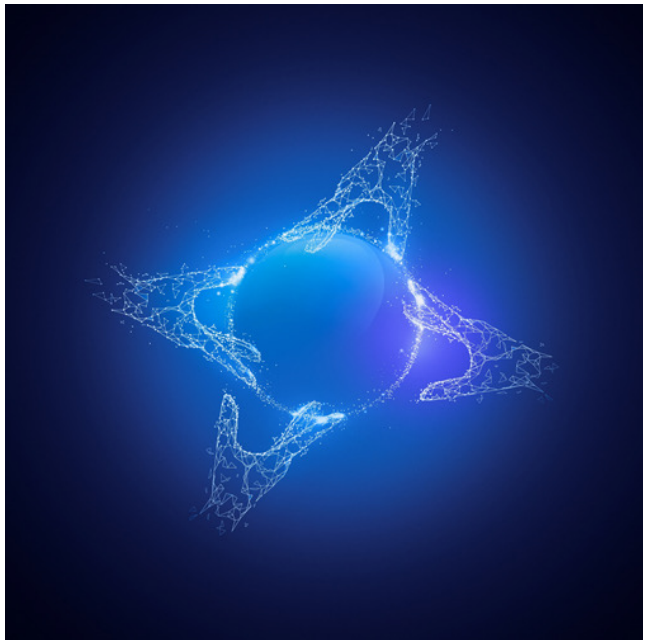
- これまでの歩みと成果
  - ✓ 2021:プロトタイプ開発
  - ✓ 2022:複数の参加者
  - ✓ 2023-2024：商用利用可能なレベルへ
  - ✓ 2025：参加者追加と**クロスボーダー決済**

SBI R3 Japan

Project Dunbar (BIS-SG, オーストラリア、マレーシア、シンガポール、南アフリカ)

- モチベーション
  - ✓ **クロスボーダー決済**を**クロスチェーン**で実行

corda × 



- これまでの歩みと成果
  - ✓ 2022/3：中間報告
  - ✓ 今後の検討課題
    - ➢ アクセスモデルのトレードオフ検討（ガバナンス、AML/CFT他）
    - ➢ ビジネスとの結合、コストとメリットの定量化、流動性要件
    - ➢ 他システムとの結合、インターオペラビリティ実現に向けた標準化、トレードオフの明確化

SBI R3 Japan

３つの実装パターン

３つの実装パターン

- RDBモデル（＝バランスモデル、アカウントモデル）
- NFTモデル
- UTXOモデル

３つの実装パターン

- RDBモデル
  - ✓Ethererum/Quorum
- NFTモデル
  - ✓独自技術（インドのリテールCBDC、日本（non-DLT））
- UTXOモデル
  - ✓Corda他

https://rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1218

RDBモデル

中央集権型システムからの直接的拡張

持ち主 （主＝変化しない）	残高（副）
佐藤さん 	 1,000,000円
藤本さん	100,000,000円
本木さん	1,000円
木村さん	500,000円

⭕Web系エンジニアにとってとっつきやすい
（RDBと同じ）

❌プライバシー確保が難しい（別技術が必要）

❌**「同時多発的な取引」**に弱い
（RDBのロック問題と根っこは同じ）

⭕**「取扱額が増える」**ことに強い

SBI R3 Japan

NFTモデル

硬貨（非ITの考え方）をそのままデータモデルに

シリアル付きトークン（主＝変化しない）	持ち主（副）
100円：a2b8c1d3e	 佐藤さん
100円：5f6g7h2i0	藤本さん
100円：j4k9l3m1n8	本木さん
100円：p7q0r6s5t2	木村さん
100円：u3v4w8x1y9	佐藤さん
100円：z5a6b2c9d1	藤本さん
100円：e8f9g0h4i3	本木さん
100円：j2k7l5m0n6	木村さん

- ⭕KVに慣れているエンジニアには使いやすい
- ⭕プライバシーの確保が容易
- ⭕「**同時多発的な取引**」に強い
- ❌「**取扱額が増える**」ことに弱い

UTXOモデル

分散台帳に最適化したデータモデル

Fungibleトークン	持ち主
1,000円	佐藤さん
100,000,000円	藤本さん
1,000,000円	本木さん
1,234円	木村さん
3,521円	佐藤さん
10,000円	藤本さん

⭕ 柔軟性が高い
（RDBモデルとNFTモデルの双方の特徴を実現可能）

❌エンジニアにとってとっつきにくい。
（昔の勘定系でも触っていない限り）

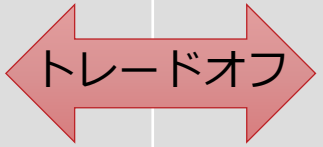
⭕プライバシー確保が容易

⭕「同時多発的な取引」＆「取扱金額増加」の双方に対応可能（トレードオフの関係）

SBI R3 Japan

まとめ：データモデル比較

データモデル	プライバシー	スケーラビリティ（同時取引数）	スケーラビリティ（残高増）
RDB	×	×	○
NFT	○	○	×
UTXO	○	○～×	×～○

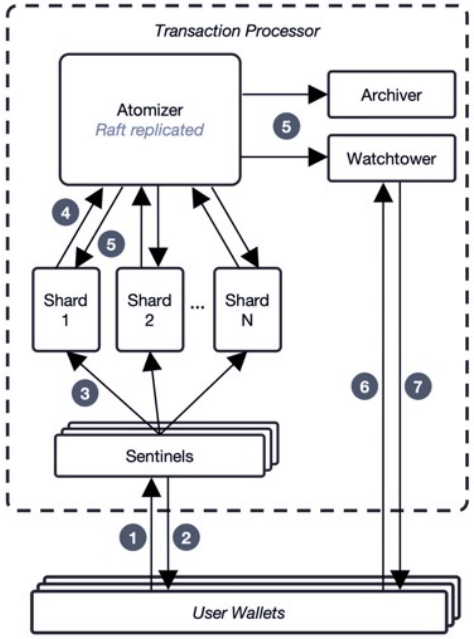


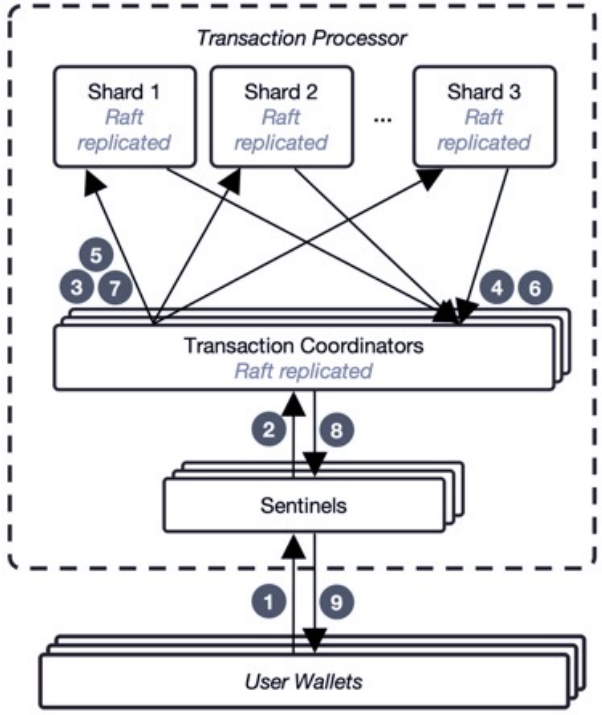
【Topic】Project Hamilton @2022/2

- ボストン連銀とMITによるPJ

- UTXOとHashによる管理
  - ✓ Raftによる共有
    ⇒17万件／秒＆RTT2秒以内

- 2PCによるシャーディング
  ⇒170万件／秒





https://dci.mit.edu/opencbdc

https://github.com/mit-dci/opencbdc-tx

【Topic】 Corda5におけるUTXO-マージ機能

Fungibleトークン	持ち主
1,000円	佐藤さん
100,000,000円	藤本さん
97円	藤本さん
1,023円	藤本さん
13,500円	藤本さん
9,870円	藤本さん

Fungibleトークン	持ち主
1,000円	佐藤さん
100,000,000円	藤本さん
24,490円	藤本さん

- 細分化したトークンのマージ機能
- 検索とアグリゲーション（集計）が高速化
- パフォーマンスとプライバシーの両立が容易に

SBI R3 Japan

まとめ

全体のまとめ

ビジネス観点

- 世界の９割が CBDC の研究中。
- 技術調査ではなく政策ツール
- 政策上の目的
  - ✓ 主：通貨主権、レジリエンス
  - ✓ 副：金融包摂、国のDX

技術観点

- Wholesale/Retailで技術要求は異なる
- クロスボーダーはこれから
- RDB/NFT/UTXOの３パターン

SBI R3 Japan

５つの重要な論点（2023-冬の陣資料）

1. 金融系の大規模商用の進展＝想定取引量
   - ✓ DTCC、Visa、Master等の動向
   - ✓ **各国CBDC**の動向（特に先進国動向）
   - ✓ 銀行が提供するステーブルコインの動向

2. 規制＆規則動向
   - ✓ ID管理に関する規制、規則の進展
   - ✓ トークン（NFT含む）への証券ルール
   - ✓ 税制見直し
   - ✓ **対ロシア／対中国関連規則**（SCM関連 / AML関連）

SBI R3 Japan

CBDCの落とし穴～ロイター記事より～（2021/5）

（前半）
- https://link.medium.com/1SrV2gRhRzb

（後半）
- https://link.medium.com/UFKkFZNhRzb

この時あげた課題
- 調達の不安定化
- マイクロマネジメント
- プライバシー

主な参考文献

- R3
  - ✓ https://r3.com/reports/taxonomy-design-choices-for-cbdc/
  - ✓ https://r3.com/products/digital-currency-accelerator/
- BIS
  - ✓ https://www.bis.org/about/bisih/topics/cbdc.htm
  - ✓ https://www.bis.org/publ/othp65.htm
  - ✓ https://www.bis.org/publ/othp64.htm
  - ✓ https://www.bis.org/publ/othp42.htm
  - ✓ https://www.bis.org/publ/othp33.htm
- 個別PJ
  - ✓ https://www.bankofengland.co.uk/the-digital-pound
  - ✓ https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html
  - ✓ https://www.federalreserve.gov/central-bank-digital-currency.htm
  - ✓ http://www.pbc.gov.cn/en/3688006/4671762/4688130/index.html
  - ✓ https://rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1218
  - ✓ https://www.riksbank.se/en-gb/payments--cash/e-krona/

SBI R3 Japan