

CBDCへの期待と論点

2022/06/02

近藤 佑樹

株式会社 日立製作所 研究開発グループ

サービスシステムイノベーションセンタ デジタルエコノミー研究部

自己紹介

近藤 佑樹 (こんどう ゆうき)

- 2008年 株式会社 日立製作所入社
 - 主に金融システムのソフトウェアエンジニアリング/システムアーキテクチャの研究開発
- 2016年 Hitachi America, Ltd., 出向
 - ブロックチェーンの研究開発
 - ブロックチェーンのユースケース開拓
 - Hyperledger OSSコミュニティ活動
- 2019年 出向復帰
 - トークン/DeFiの研究開発
 - Hyperledger Fabricへのトークン機能のOSSコントリビューション

CBDCのバリエーション

- フェーズや導入目的により、アーキテクチャ、データモデル、トランザクション処理方式を選択。
- 選択には、イノベーション、安全性、性能、プライバシー、ガバナンス、等のトレードオフ。

研究

性能重視

[アメリカ/Project Hamilton、エストニア]

中銀のガバナンス重視

[ロシア]

パイロット

ユーザビリティ重視

[スウェーデン、中国]

発行/償還機能の安全性重視

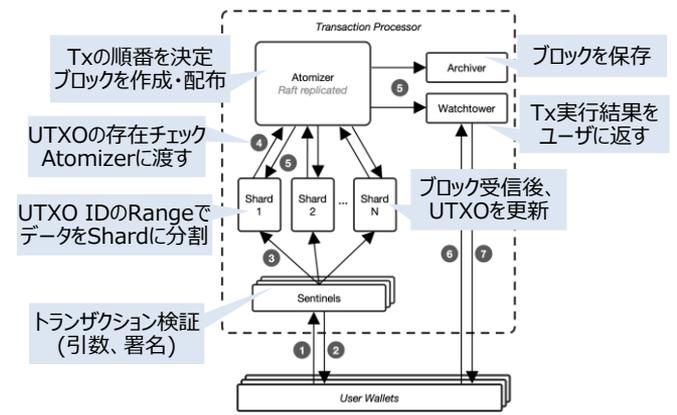
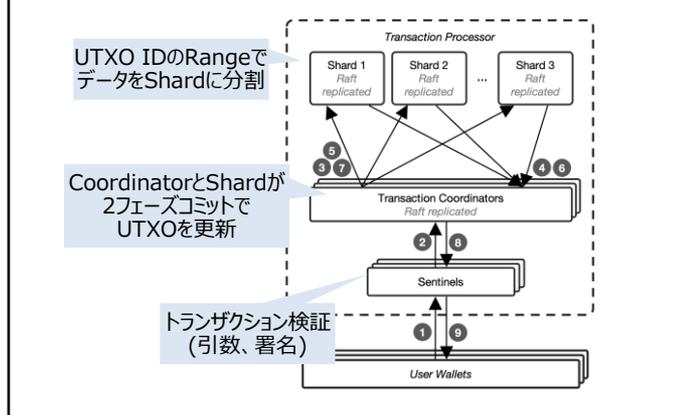
[ガーナ]

本番

KYC/AML重視

[ナイジェリア、東カリブ、バハマ]

- 大規模リテール決済システムの性能・信頼性要件達成を目指す、トランザクション処理機能の設計
- 外部の研究プロジェクトや有識者とコラボレーション。MITライセンスでソースコードを公開([OpenCBDC](https://opencbd.com))

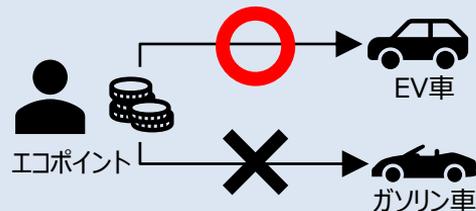
	#1: atomizer architecture	#2: two-phase commit(2PC) architecture
特徴	Ordering Serverがトランザクションの順番を維持。ブロックを生成。	Ordering Serverなし。トランザクションの順番を維持しない。ブロックを生成しない。
システム構成	 <p>The diagram shows a Transaction Processor containing an Atomizer (Raft replicated), Archiver, Watchtower, and multiple Shards (Shard 1, Shard 2, ..., Shard N). Below the processor are Sentinels and User Wallets. The flow is: 1. User Wallets send transactions to Sentinels. 2. Sentinels perform transaction verification (index, signature) and send to Atomizer. 3. Atomizer checks UTXO existence and splits data by UTXO ID range into Shards. 4. Shards execute transactions. 5. Atomizer orders transactions and creates/distributes blocks. 6. Archiver stores blocks. 7. Watchtower returns execution results to users. 8. Sentinels update UTXOs after block receipt.</p>	 <p>The diagram shows a Transaction Processor containing Transaction Coordinators (Raft replicated), Sentinels, and multiple Shards (Shard 1, Shard 2, ..., Shard 3). Below the processor are User Wallets. The flow is: 1. User Wallets send transactions to Sentinels. 2. Sentinels perform transaction verification (index, signature) and send to Transaction Coordinators. 3. Coordinators and Shards perform two-phase commit to update UTXOs. 4. Shards split data by UTXO ID range. 5. Shards execute transactions. 6. Sentinels return execution results to users.</p>
ファイナリティ	レスポンス 2sec(99% tile), 0.7sec(50% tile)	レスポンス 1sec(99% tile), 0.5sec(50% tile)
スループット	170K tps Orderingがボトルネック。ピーク性能は8shard。	1.7M tps Shard追加でリニアにスケール。ピーク性能は32shard。

CBDCへの期待と論点

- プログラマビリティによる、決済の効率化とコスト削減、イノベーションの促進

#1: エコポイント

- エコ商品・サービスの支払いに利用可能 (使途限定)



#2: NFT取引におけるDvP

- NFTの所有者変更と同時にデジタル通貨を支払い



#3: 自動車のIoT決済

- 電力チャージ代金をステークホルダに分配 (自動執行)



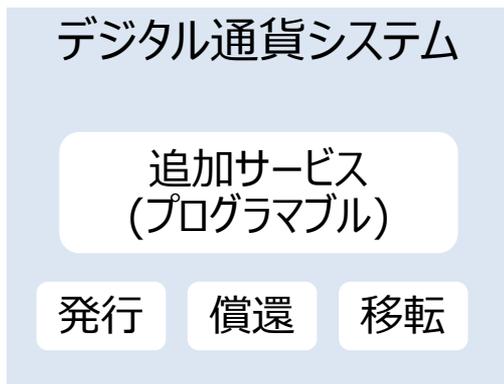
#4: レンタカーの課金 + 電子鍵制御

- レンタカー代金を支払うと、電子鍵を解除
- 料金が支払われなかったら、電子鍵をロック

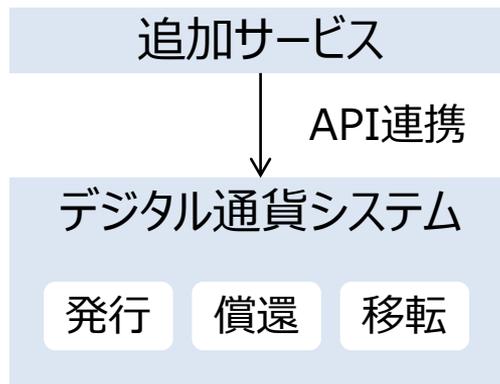


- 目的に応じて、様々なオプションを検討して、フィットする技術を選択。
- トレードオフの考慮 (例: イノベーションと安全性のトレードオフ)

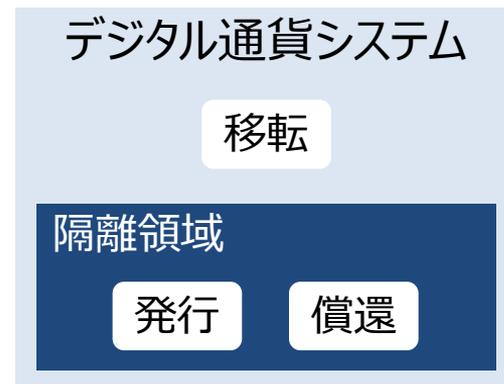
追加サービスのためのプログラマブル領域を持つ



追加サービスにAPIを提供



発行/償還機能を分離



HITACHI
Inspire the Next 