



# Secure Asset Transfer Protocol (SATP)

## *Updates: Use Cases, Compatibility with Standards, Implementation*

V. Ramakrishna (IBM), Thomas Hardjono (MIT)

IETF 117: Secure Asset Transfer Working Group

San Francisco, CA

July 25, 2023

SATP Use Cases: <https://datatracker.ietf.org/doc/draft-ramakrishna-sat-use-cases/>

SATP Architecture: <https://datatracker.ietf.org/doc/draft-ietf-satp-architecture/>

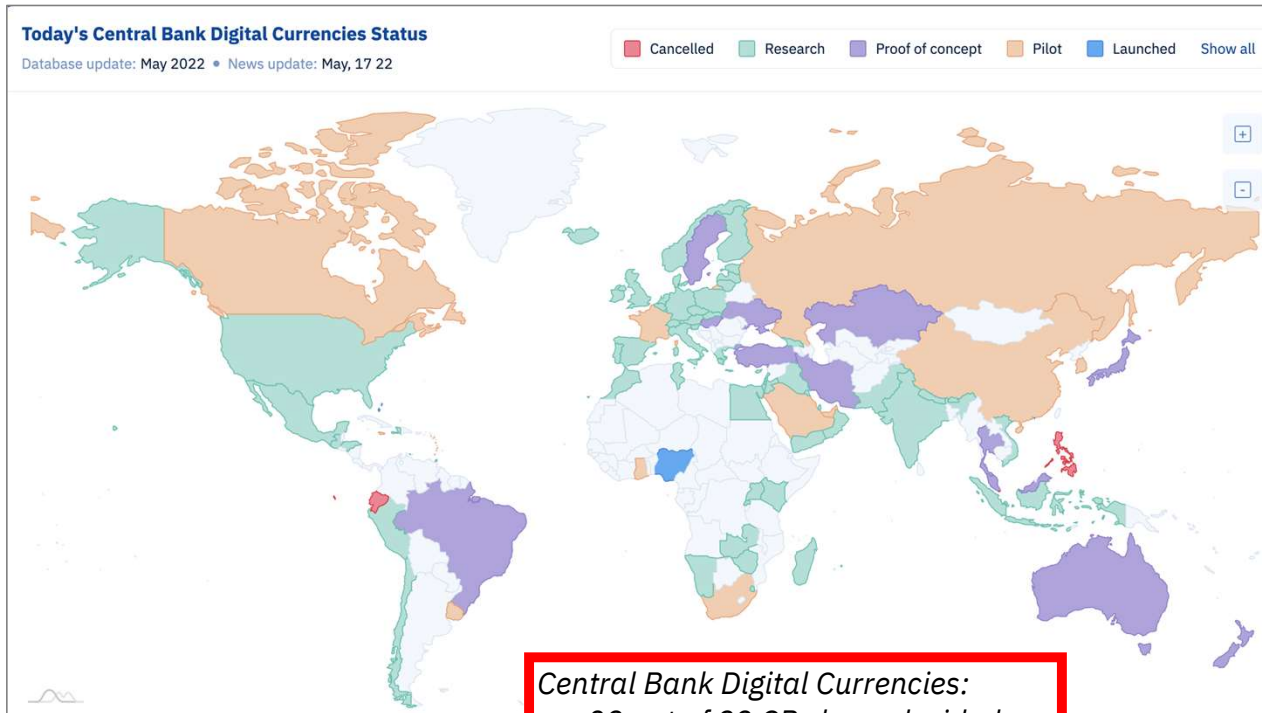
# Use Cases Draft Updates: CBDC-Inspired Content

- SATP Use Cases: <https://datatracker.ietf.org/doc/draft-ramakrishna-sat-use-cases/>
  - More elaboration of the CBDC landscape and addition of use cases
- DeFi and CBDC face interoperability challenges
  - Probably the most compelling and near-term application of SATP and Gateways

# DeFi and CBDC

- DeFi (Decentralized Finance)
  - A “new financial paradigm that leverages distributed ledger technologies to offer services such as lending, investing, or exchanging crypto assets without relying on a traditional centralized intermediary” (<https://www.bis.org/publ/work1066.htm>)
  - Scoped for the world of finance, DeFi offers architecture and protocols built on smart contracts deployed on blockchain or other distributed ledger technology
- CBDC (Central Bank Digital Currency)
  - A form of tokenized cryptocurrency that various central banks around the world are experimenting with as the digital equivalent of traditional central bank-issued money used by banks and other financial institutions as well as end users for commercial transactions and settlements
  - Just as with traditional fiat currency, central banks possess exclusive authority to mint and issue money

# Why CBDC is a Compelling Application

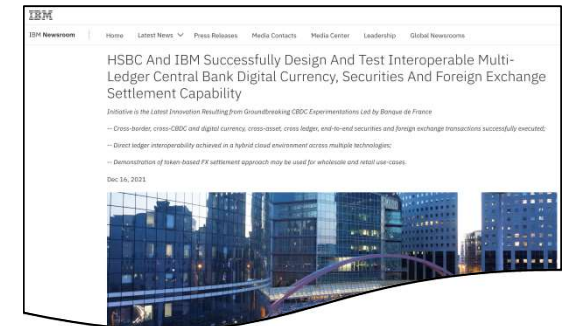


**Central Bank Digital Currencies:**

- 23 out of 93 CBs have decided on Blockchain based infrastructure
- 1 out of 93 have decided on legacy infrastructure



## Interoperable Multi-Ledger Central Bank Digital Currency, Securities And Foreign Exchange Settlement Capability



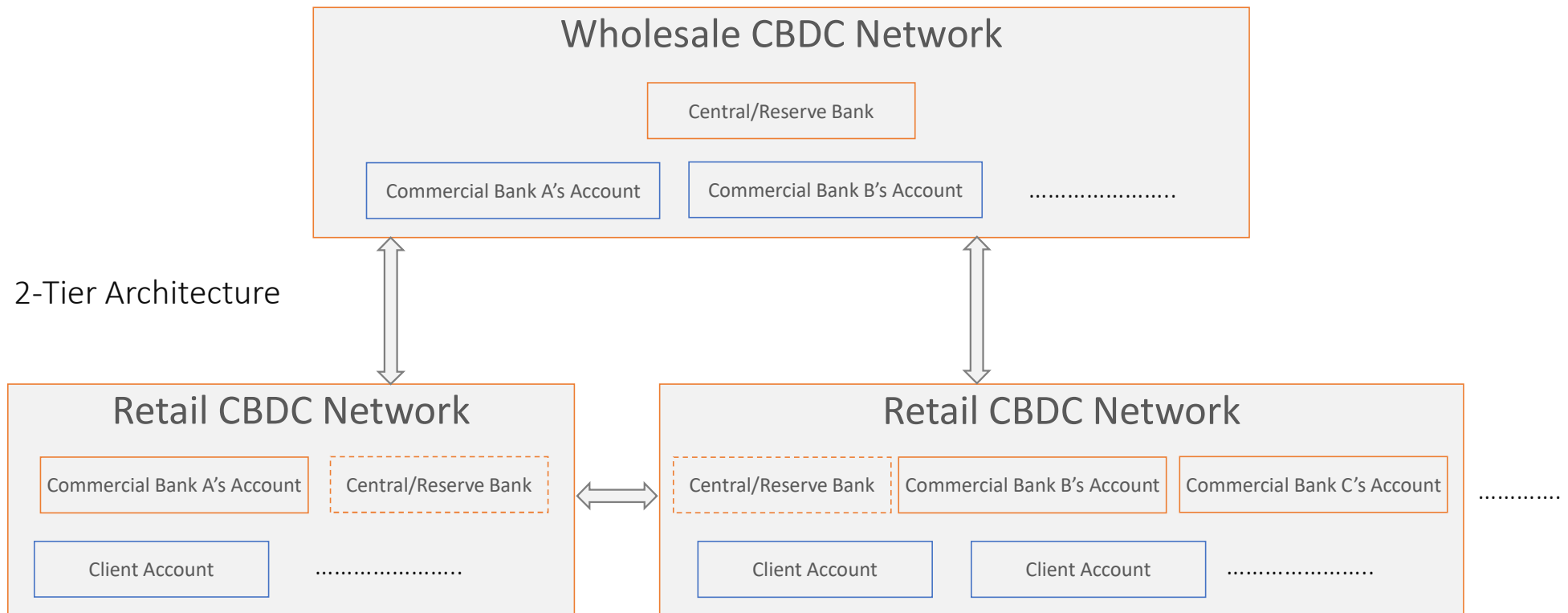
### HOW:

- **Multiple Permissioned network :** Hyperledger Fabric and Corda, with add-on from IBM Research enabling interoperability across protocols (Hyperledger Cacti/Weaver)

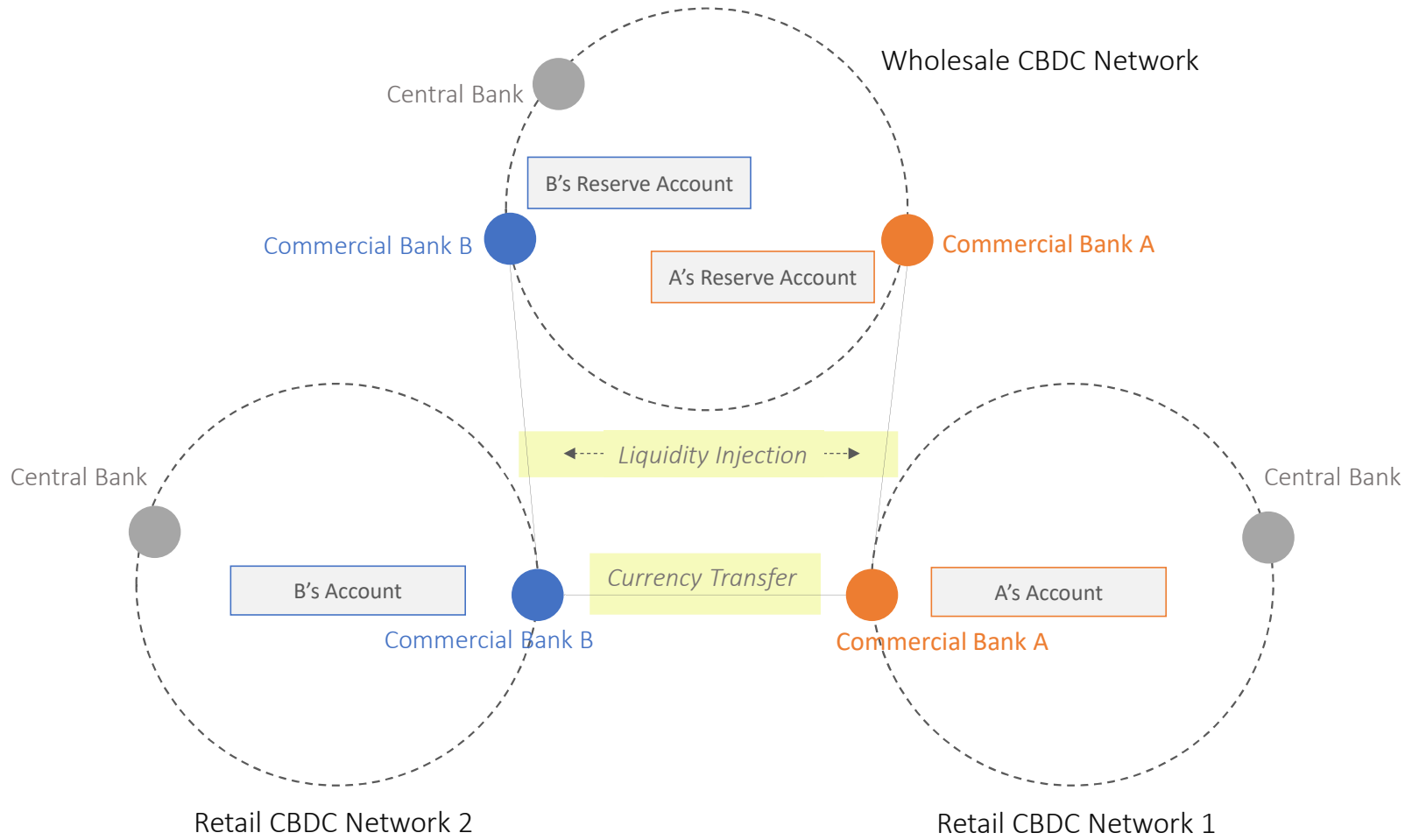
# CBDC Networks, Interoperability, and SATP

- Why multiple networks for CBDC?
  - CBDC cannot be managed by one single (national or global) system or ledger if it must satisfy typical performance scalability metrics
  - Also, there are different categories of CBDC:
    - Wholesale: facilitates inter-bank and cross-border settlements, and is available only to banks and other financial institutions
    - Retail: available to the public and can be used as a digital form of cash, and a substitute for legacy payment mechanisms
  - This will necessitate the deployment and use of different networks: wholesale/retail, public/private
- Different architectures have been proposed: 2-tier(indirect), direct, hybrid
  - 2-tier and hybrid models will have different networks for wholesale and retail operations
  - Tokenized currency assets must occasionally move across these networks: hence the need for SATP

# Central Bank Digital Currency (CBDC) Landscape



# CBDC Transfer (Asset Transfer)



# Multi-CBDC Economy

- CBDC is a national financial instrument
  - But CBDCs must facilitate cross-border payments and inter-bank settlements
- Two possible solutions:
  - Multi-CBDC ledger: shared ledger containing multiple CBDCs
    - Potential benefit to improve cross-border payments and protect monetary sovereignty, without necessarily becoming a monetary union
    - Transfer of CBDC from a wholesale CBDC network to Multi-CBDC network and vice versa
  - Alternative: direct interactions between wholesale CBDC networks of different countries
    - Transfer of CBDC from one wholesale network to another
- SATP across gateways representing wholesale CBDC networks and a Multi-CBDC network is an attractive means to permit CBDC asset transfer

## Relationship with Existing Standards

- *Question raised in IETF 116 (by John Levine): how does SATP differ from ISO 20022 and why not use the latter for the presented use cases?*
- We are aware of the facts that other standards for interoperability among systems and networks for business process management exist, and have scoped the SATP charter accordingly
  - The scope of SATP is defined narrowly and precisely
  - SATP is designed to accommodate other standards as and when applicable
  - SATP is designed to leverage and complement pre-existing standards that are widely in use
  - The intent of this WG is for the protocol to be compatible with other standards: specifically, to not preclude the use of other standards for aspects of digital asset management outside the scope of SATP

# The ISO 20022 Standard

- Comprehensive unified global standard for financial messaging
  - Specifies message syntax for common actions in financial business processes: e.g., payments, credit card transactions, settlements, funds, trade
  - Provides tools to model business processes: logical building blocks and schemas
  - Support for message constructions using common formats like XML, JSON, and ASN.1
  - Each part of an ISO 20022 message can be linked to business components and data
- The standard provides communication interoperability: the ability to communicate information in an unambiguous manner across system boundaries
- E.g. ExampleBank in Utrecht, the Netherlands (Bank Identifier Code (BIC) EXABNL2U) has been requested by its corporate customer ACME NV, Amstel 344, Amsterdam to transfer 12,500 US Dollars on 06 April 2022 from its account 8754219990.

```

<CdtTrfTxInf>
<IntrBkSttlmAmt
Ccy='USD'>12500</IntrBkSttlmAmt>
<IntrBkSttlmDt>2022-04-
06</IntrBkSttlmDt>
<Dbtr>
<Nm>ACME NV.</Nm>
<PstlAdr>
<StrtNm>Amstel</StrtNm>
<BldgNb>344</BldgNb>
<TwnNm>Amsterdam</TwnNm>
<Ctry>NL</Ctry>
</PstlAdr>
</Dbtr>
<DbtrAcct>
<Id>
<Othr>
<Id>8754219990</Id>
</Othr>
</Id>
</DbtrAcct>
<DbtrAgt>
<FinInstnId>
<BIC>EXABNL2U</BIC>
</FinInstnId>
</DbtrAgt>
</CdtTrfTxInf>

```

# SATP and ISO 20022

- SATP Architecture: <https://datatracker.ietf.org/doc/draft-ietf-satp-architecture/>
- Interoperability among networks managing digital assets involves more than just communicating desire or intent (i.e., through requests, responses, and notifications)
  - Need ACID properties to be enforced at a cross-network level (SAT Architecture draft)
  - Communication interoperability, which restricts itself to message syntax and semantics, is insufficient
  - SATP requires systems to carry out state updates in concert to achieve the desired outcome
- ISO 20022 does not solve the problem that SATP is trying to solve, and vice versa
  - Both standards are applicable to the scenarios listed in the SATP Use Cases draft: trade and finance
- ISO 20022 and SATP play complementary roles in the digital asset management ecosystem
  - We can leverage ISO 20022 for asset descriptors and context negotiation in Stage 0
  - Possible functions for ISO 20022: gateway ownership validation, owner status validation, asset profile identification, and communication of travel rule and transfer context information

# Reference Implementation of SATP in Hyperledger Cacti

- Hyperledger Mentorship 2023 project 2023
  - <https://wiki.hyperledger.org/display/INTERN/Cacti%3A+Implement+Standardized+Secure+Asset+Transfer+Protocol>
  - 2 authors are co-mentors: Rafael Belchior, V. Ramakrishna
  - Augment Cacti “relay” according to SATP draft specs
    - SATP-standard endpoints and SATP message parsing capabilities
    - Error handling and crash recovery support
  - ETA: late Q3 or early Q4



- Relay is a configurable module running gRPC services built on Rust
  - Not built for any specific DLT; compatible with any
  - Fits the specification for an SATP gateway

