

# Inter-bank Payments with Tokenized Fiat Currencies

# Hub and Spoke Model

Current x-border payments follow a hub and spoke model



-  Bank
-  Correspondent Bank

# Point-to-point Model

Point-to-point transfers will reduce costs and delays



- b** Bank
- c** Correspondent Bank

## Tokenized Fiat Currencies (TFCs)

- Inspired by Crypto-currencies
- Digital Bearer Assets, to be transferred point-to-point between institutions
- Denominated in fiat currencies like SGD, USD, etc.
- Issued by a bank

# Significant Interest in Singapore

## Experimentation Phase: Project Ubin (2016 - 2020)

- PoC: Tokenized SGD
- PoC: Inter-bank Payments
- PoC: DvP, PVP, DvD

## Commercialization Phase: Partior (2021 - )

- JV between DBS, JP Morgan and Tamasek
- DBS to issue SGD, JP Morgan to issue USD denominated digital payment tokens

# Problem

Digital Payment Tokens are different from Crypto-currencies

## **Crypto-currencies have two requirements**

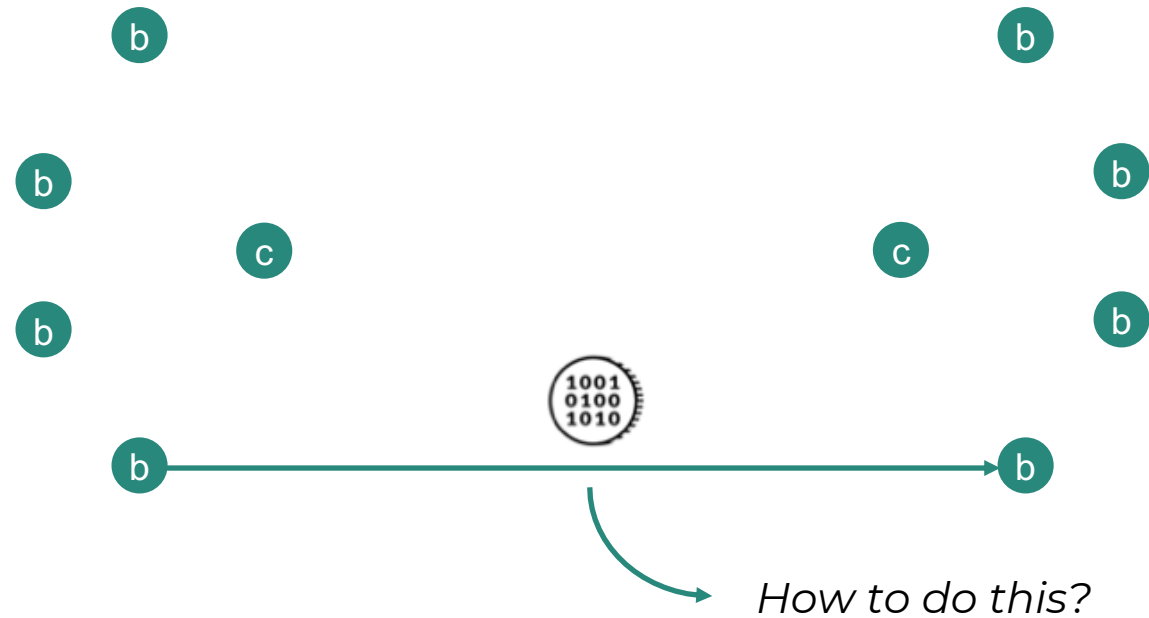
- Secure Double-spend Prevention
- No centralized control over transaction processing

## **TFCs have two additional requirements**

- Confidentiality – Parties not involved in the transaction should not be aware of it
- Compliance – Adherence to data residency, data hygiene and financial reporting guidelines

# Problem

No tech in the market delivers point-to-point transfer of Tokenized Fiat Currencies



- b** Bank
- c** Correspondent Bank

# Current Attempts are Blockchain Inspired

Let's look at four examples.

## Ethereum

Public Blockchain with Smart Contract functionality.

## ConsenSys Quorum

Permissioned version of Ethereum.

## IBM Hyperledger Fabric

IBM's permissioned Blockchain.

## R3 Corda

Distributed Ledger Technology (DLT).

None of these designs jointly satisfy the four requirements.



# Ethereum

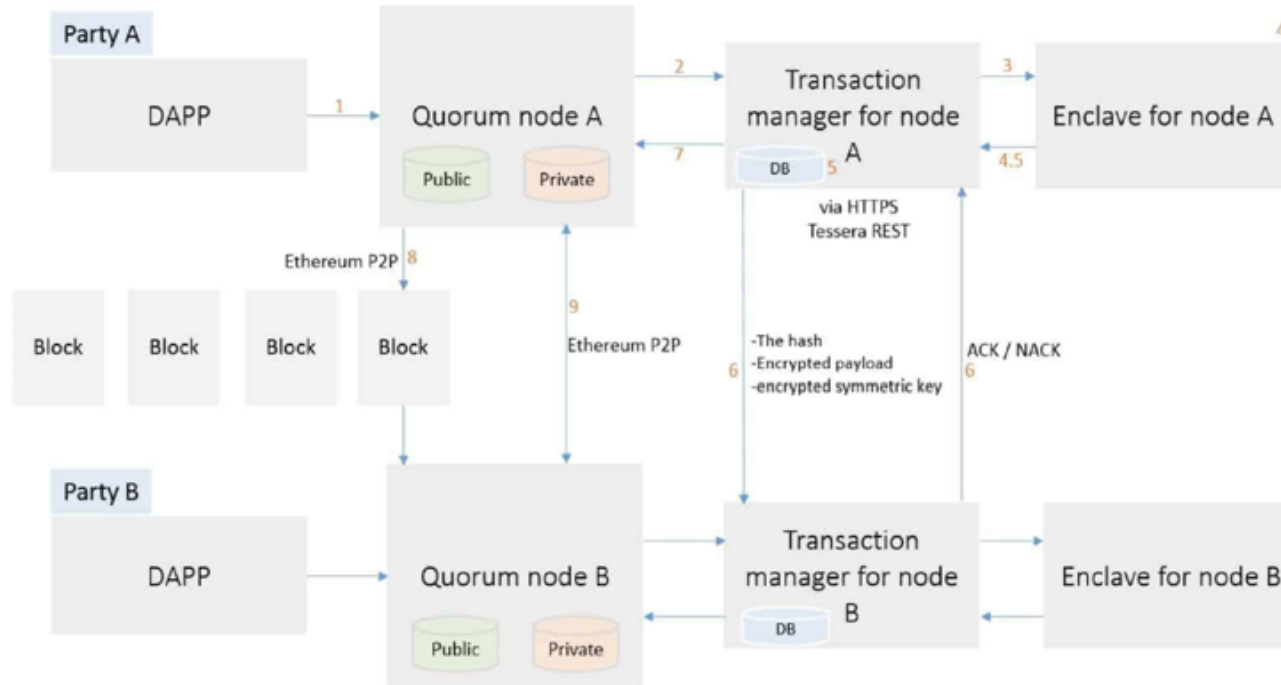
Public Blockchain with Smart Contract functionality.



- **Problem:** Ethereum is too public. Institutions do not want to compromise confidentiality of their transactions.

# ConsenSys Quorum

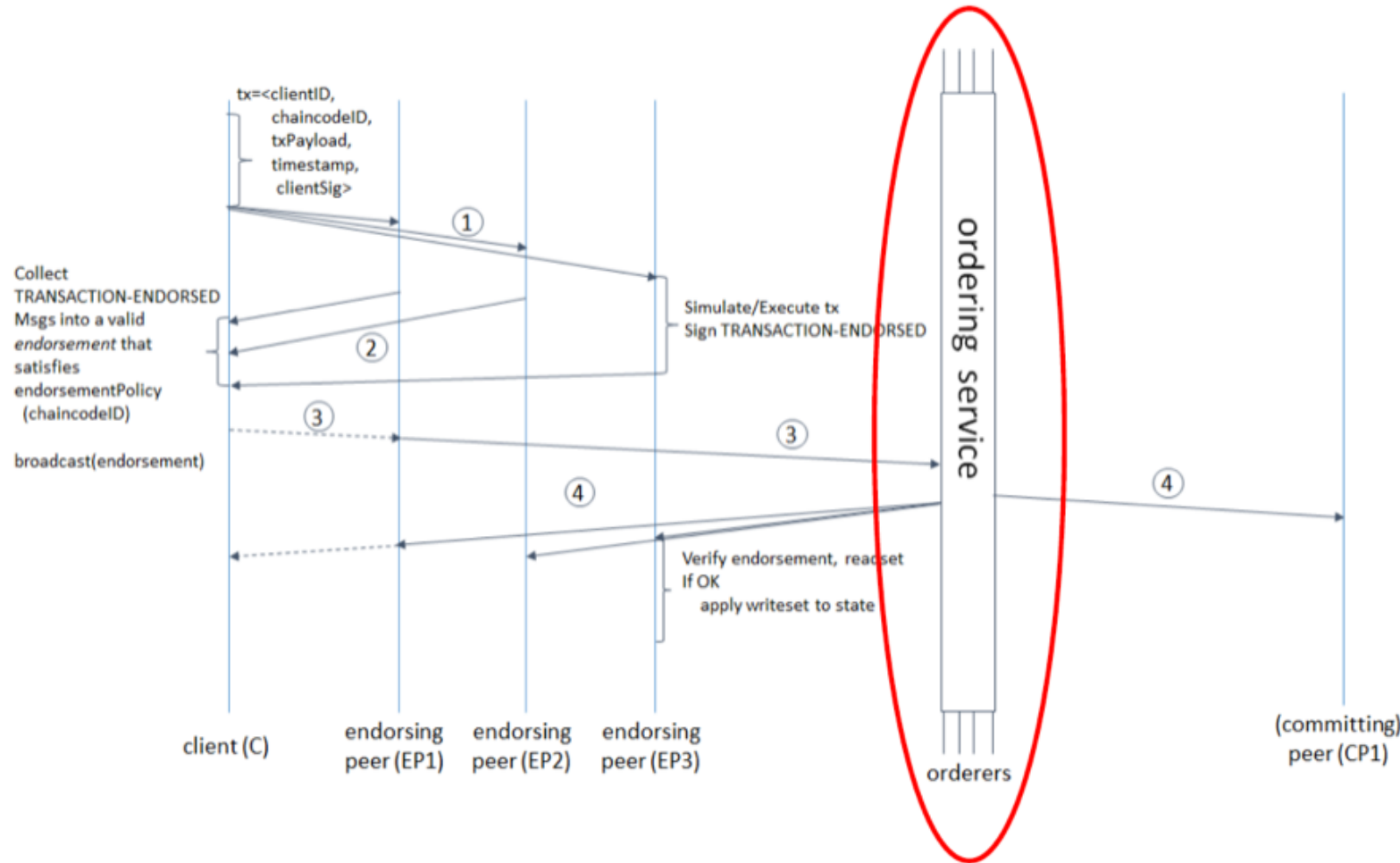
Permissioned version of Ethereum. Also has a confidential transactions mode.



- Payload of confidential transactions is sent to parties involved in transaction. Payload hash is sent to all members to aid ordering via consensus.
- **Problem:** Payload hash does not contain enough information to ensure double-spend prevention when only two parties are involved in a tx. Confidential digital asset transfers are impossible.

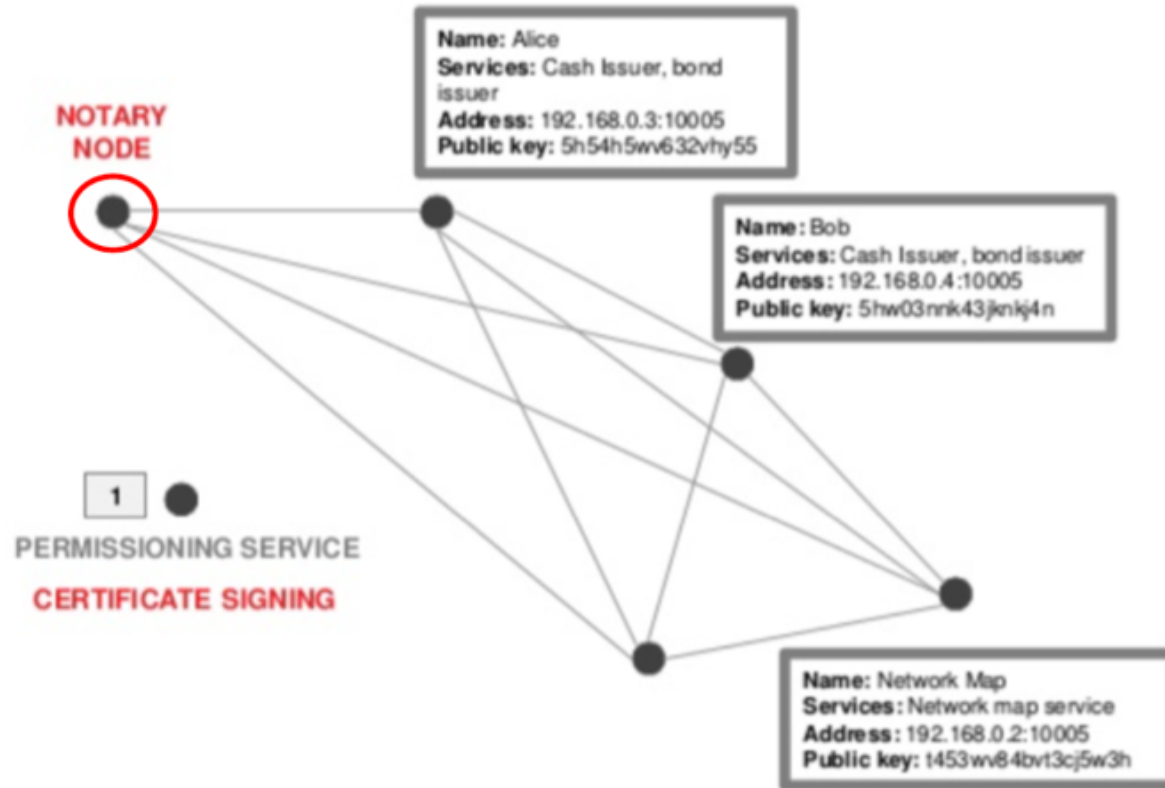
# IBM Hyperledger Fabric

Philosophy: Blockchains are replicated databases.



- **Problem:** If ordering service is operated by a centralized entity, decentralization requirement is not satisfied.
- **Problem:** If ordering service is operated by a decentralized set of peers then confidentiality and compliance requirements are not satisfied.

Cross-org replication of data, even encrypted data accrues tremendous liabilities on enterprises.



- The notary service is essentially a transaction ordering service.
- **Problem:** The notary service is centralized. Decentralization requirement is not satisfied.

# Half Epsilon's Approach

1. Ignore the Blockchain / DLT hype
2. Re-solve the double-spend prevention problem to satisfy the four requirements

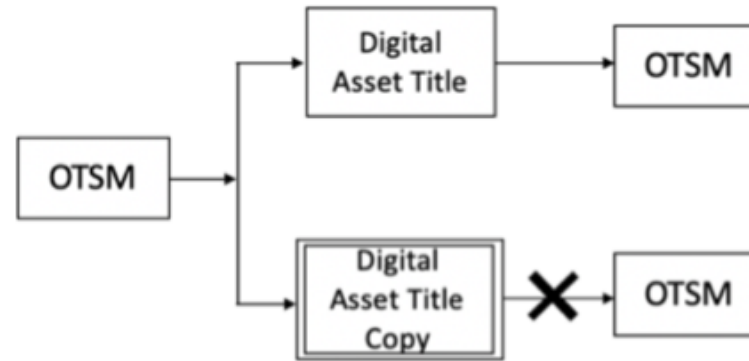


*This is very hard. But, we did it!*

# Product: One Time Spend Machine



OTSM – A Special Purpose  
FIPS 140-2 Level 3 HSM



OTSM prevents a digital asset from  
being spent multiple times.

	OTSM
Confidentiality	Yes
Security	Yes
Decentralization	Yes
Compliance	Yes

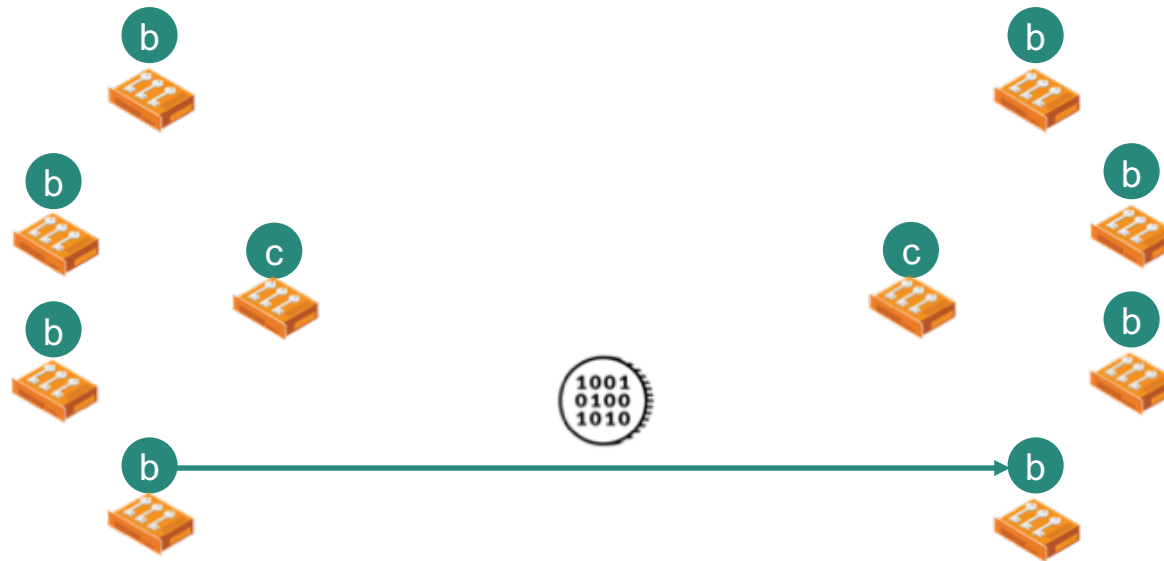
OTSM enables direct institution-to-institution transfers of tokens.

# OTSM: Key Technical Challenges

- How to securely create new tokens? Both fungible and non-fungible.
- How to securely store tokens?
- How to ensure double spend prevention at spending institution?
- How to ensure replay attack prevention at receiving institution?
- How to ensure asynchronous transfers?
- How to transport tokens from one institution to another?

# Achieving Point-to-point TFC Transfers

All Banks that have OTSMs can transfer TFCs to each other



- b** Bank
- c** Correspondent Bank



# Bottom Line

Every Solution to the double-spend prevention problem brings in massive change.

## **Digital Baking**

Enabled by resilient databases

## **Crypto-economics**

Enabled by Nakamoto consensus

## **One Tap Payments**

Enabled by secure ICs in stored value cards and mobile phones

## **Fast and low cost Inter-bank cross-border payments**

Enabled by the One Time Spend Machine

# Thank You!

If you liked this deck, share it!

Contact: [pralhad@halfepsilon.com](mailto:pralhad@halfepsilon.com)