Inter-bank Payments with Digital Payment Tokens

Hub and Spoke Model

Current x-border payments follow a hub and spoke model

b Bank

c Correspondent Bank

Point-to-point Model

Point-to-point transfers will reduce costs and delays

Key Enabler

HALF EPSILON

Digital Payment Token

- Inspired by Crypto-currencies
- Denominated in fiat currencies like SGD, USD, etc.
- Issued by a bank
- To be transferred point-to-point

Significant Interest in Singapore

HALF EPSILON

Project Ubin (2016 - 2020)

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

Commercialization (2021 -)

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

Problem

HALF EPSILON

Digital Payment Tokens are different from Crypto-currencies

Crypto-currencies have two requirements

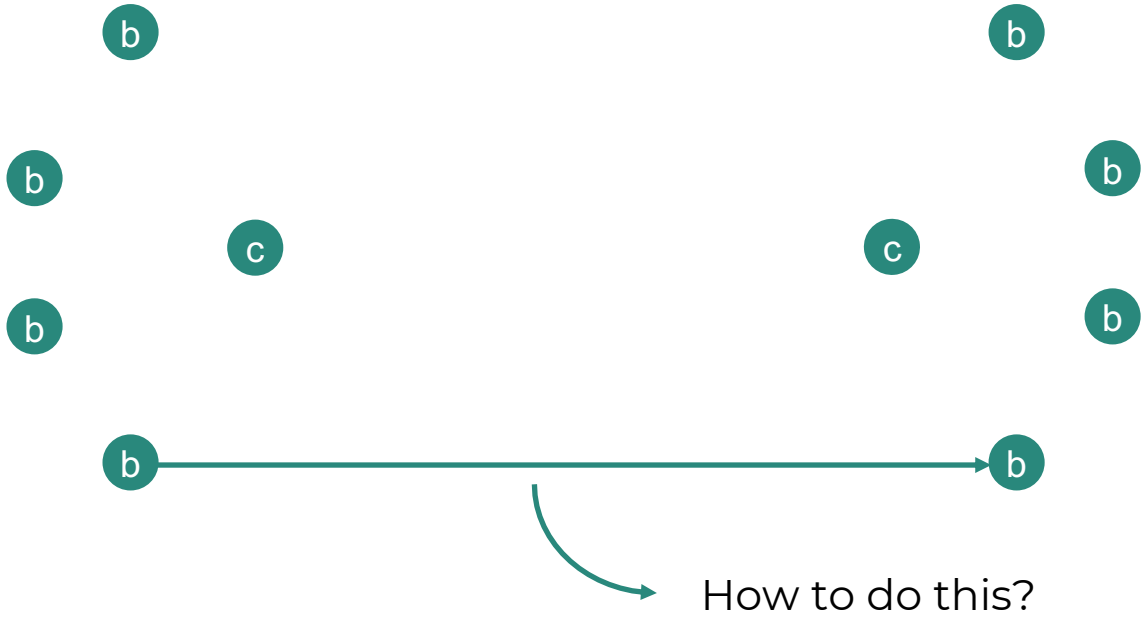
- Secure Double-spend Prevention
- No centralized control over transaction processing

DPTs 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 Digital Payment Tokens



b Bank

c Correspondent Bank

Current Attempts are Blockchain Inspired

HALF EPSILON

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

HALF EPSILON

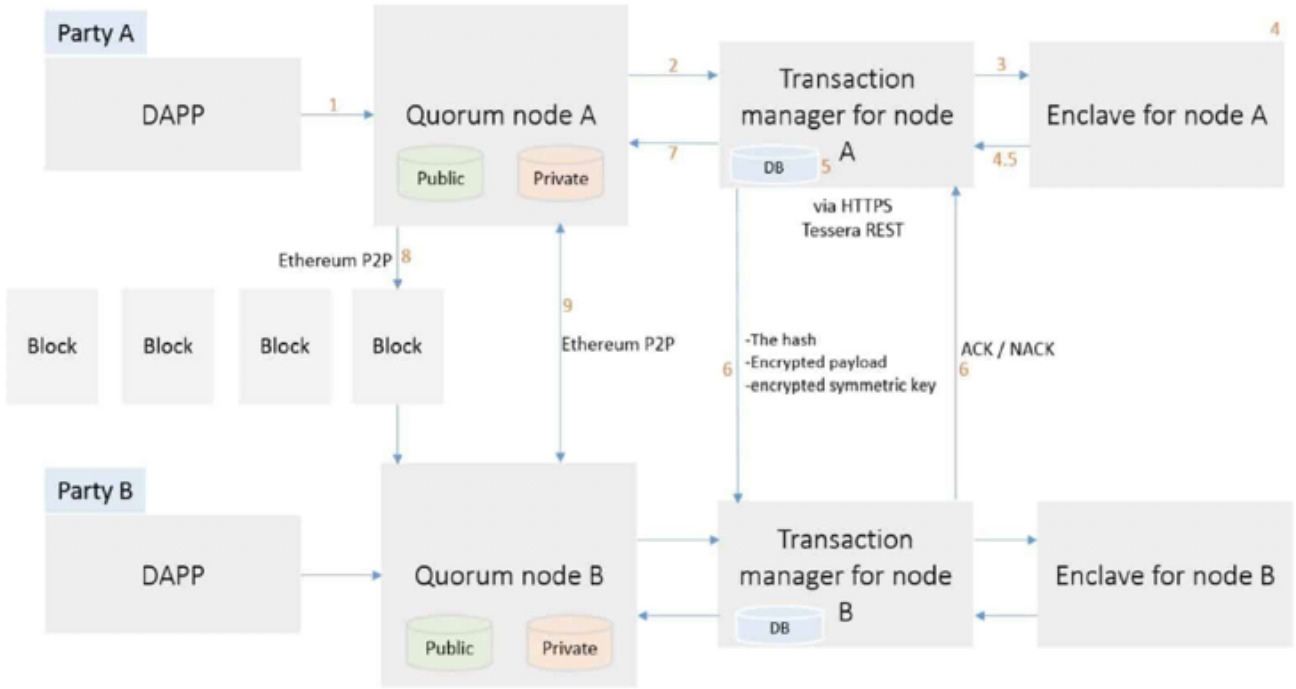
Public Blockchain with Smart Contract functionality.

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

ConsenSys Quorum

HALF EPSILON

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

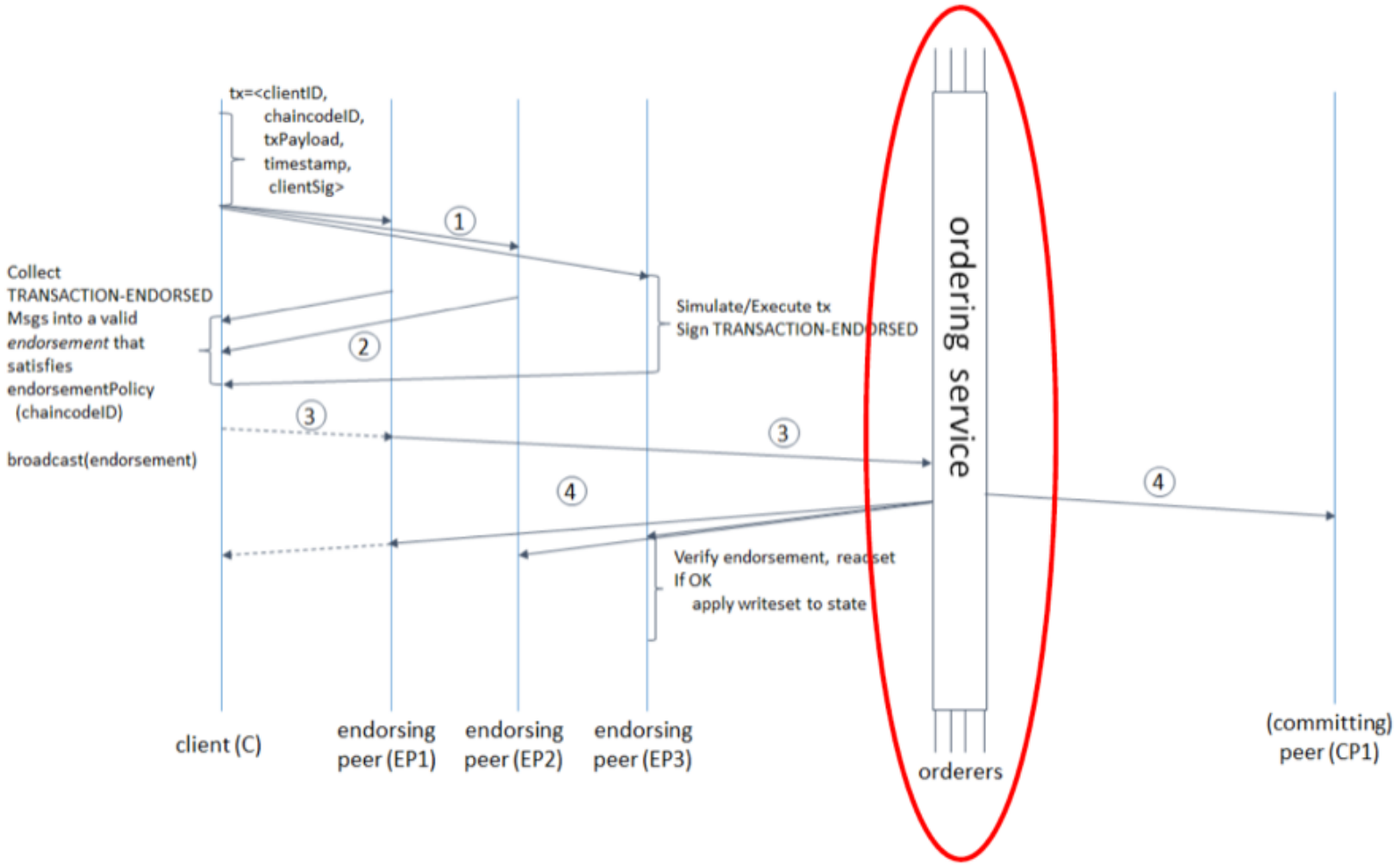


- Payload of confidential transactions is sent to parties involved in transaction. Payload hash is sent to all members to aid ordering via consensus.
- **Problem:** Payload hash does not contain enough information to ensure double-spend prevention when only two parties are involved in a tx. Confidential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

IBM Hyperledger Fabric

HALF EPSILON

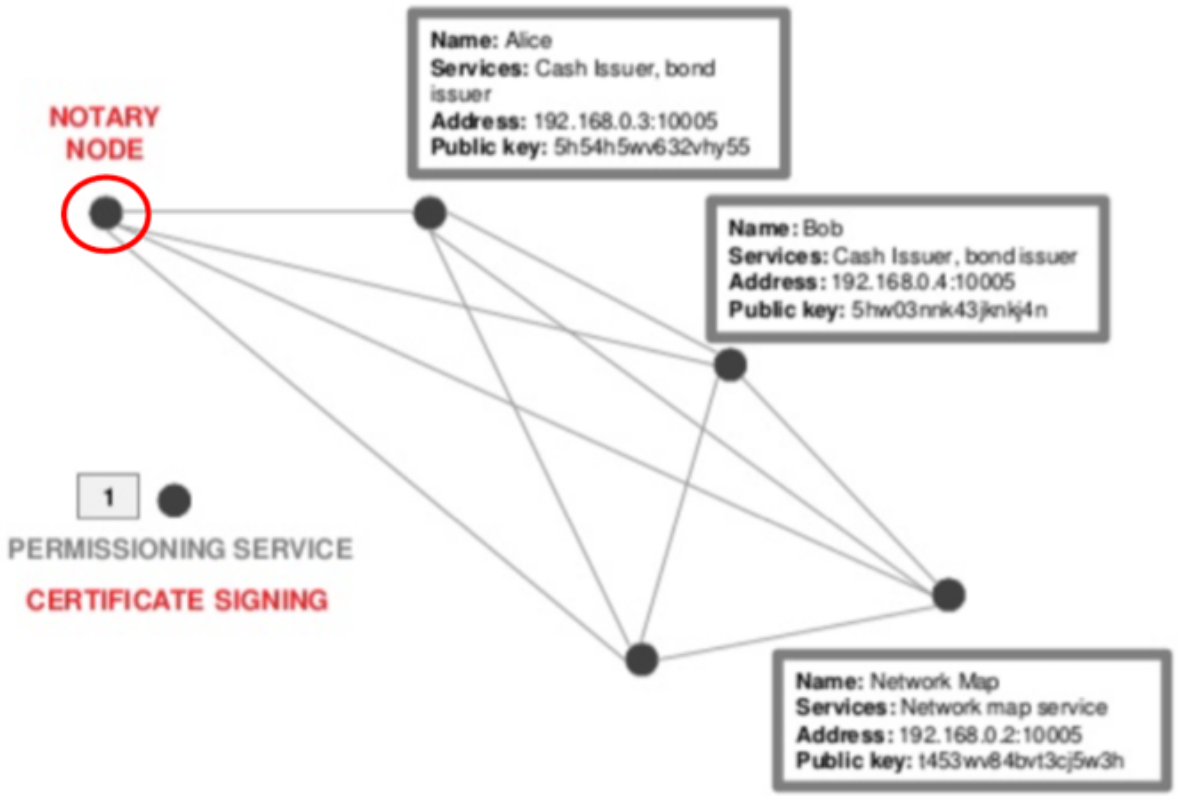
Philosophy: Blockchains are replicated databases.



- **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.

R3 Corda



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

Half Epsilon's Approach

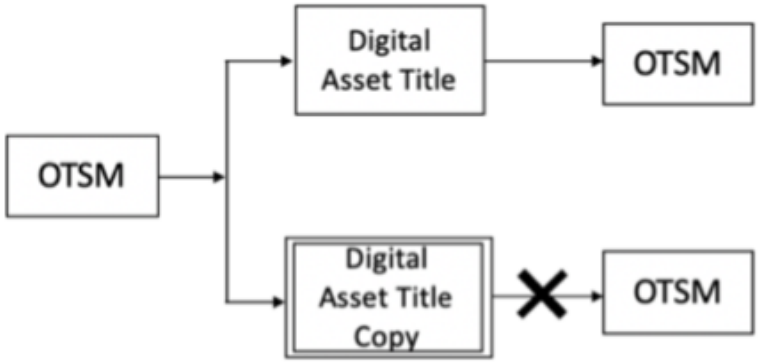
HALF EPSILON

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. No blockchain / DLT. Satisfies the four requirements.

OTSM: Key Technical Concepts

HALF EPSILON

- For peer-to-peer transfers rely on trusted hardware
- Since transfers will be over the Internet, rely on an asynchronous approach to value transfer. Single-shot transfers, no interactive sessions.
- HSMs are very good at maintaining small amounts of data very securely. Rely on advanced cryptographic concepts to maintain full recall of transaction history despite limited storage space.
- Ensure active-active replication of secure storage. An OTSM cluster is highly resilient and there are no practical limits on replication factor.

Achieving Point-to-point DPT Transfers

All Banks that have OTSMs can transfer DPTs to each other

b Bank

c Correspondent Bank

Bottom Line

HALF EPSILON

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

HALF EPSILON

Thank You!

If you liked this deck, share it!

Contact: pralhad@halfepsilon.com