
ELEMENTAL CONCEPT

Hyperledger Fabric Workshop

Architecture Overview

Paul Sitoh

10-11 November 2018

Disclaimer

- Applies to version 1.1
- Official documentation
- Conversation with peers in RocketChat (Hyperledger support channel)
- Reading the source code
- Real world implementation

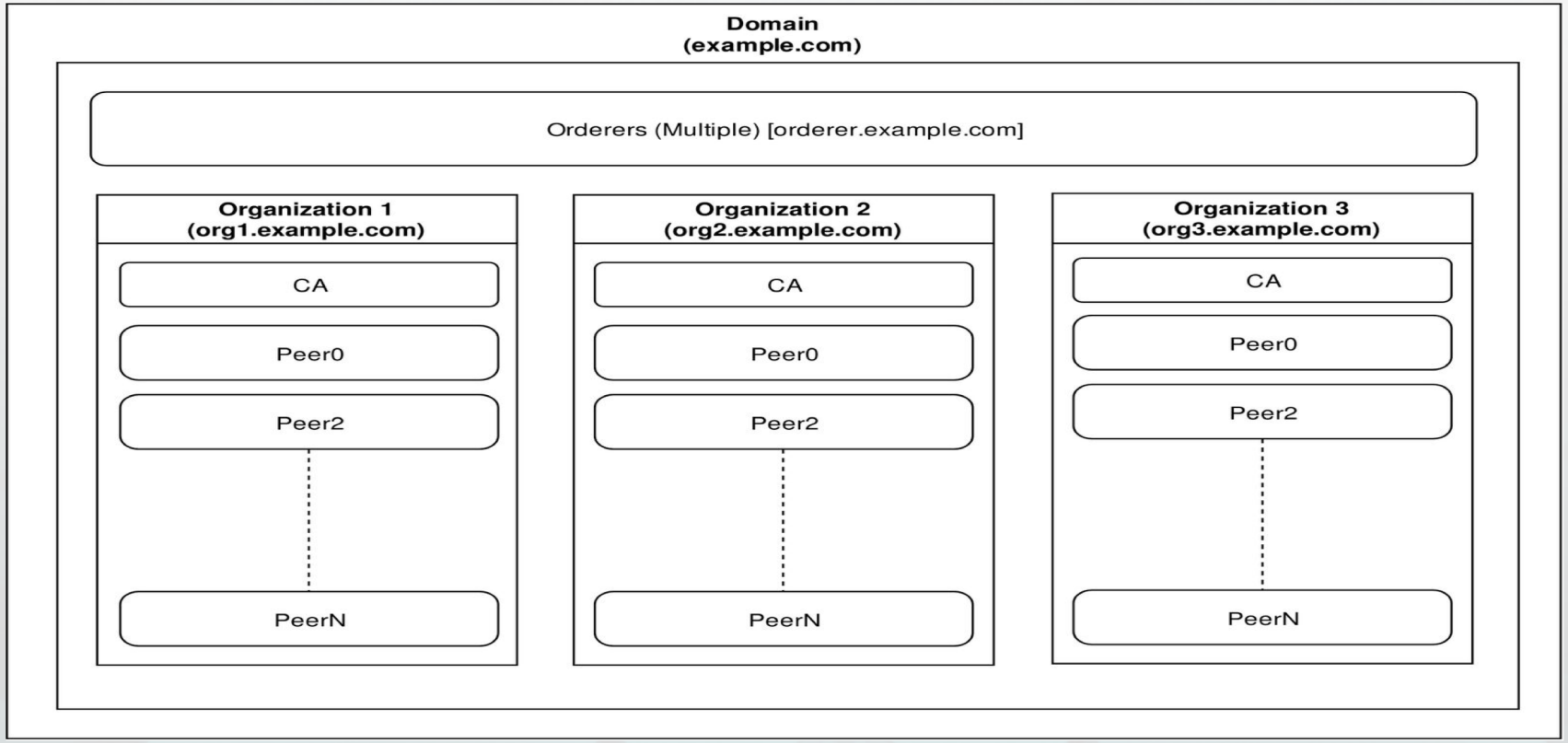
Agenda

- Fabric Network Architecture
- Transactions and consensus
- Peers
- Ledger, blocks and world state
- Identity service
- Governance
- Q&A

Fabric Network Architecture

Architecture overview

Fabric Network Architecture(1)



(1) https://medium.com/hyperlegendary/understanding-hyperledger-fabrics-architecture-3b37d81c3e96

Fabric Network Architecture

Glossary

- Peer
  - Responsible for maintaining a ledger and executing chaincode
- Orderer or Ordering services
  - Responsible for ordering transactions into blocks
- Organisation
  - An entity responsible for governing access to peers and the Fabric network or Consortium

Transactions and consensus

Architecture overview

Transactions and consensus

Let's set the scene with comparison …

Ethereum

- Order and execution model
  - Transaction set to a pool
  - Miner solve puzzle to gain right to add transaction to block
  - Miner choose which to transaction to add to a block
  - Transaction executed
- Smart contract must be deterministic
- Forked possible

Fabric

- Execution, Order and Validation(1)
  - *execute* a transaction and check its correctness, thereby endorsing it,
  - *order* transactions via a (pluggable) consensus protocol, and
  - *validate* transactions against an application-specific endorsement policy before committing them to the ledger
- Parallel execution possible
- No fork

(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/whatis.html#smart-contracts

Transactions and consensus

Back to fabric …

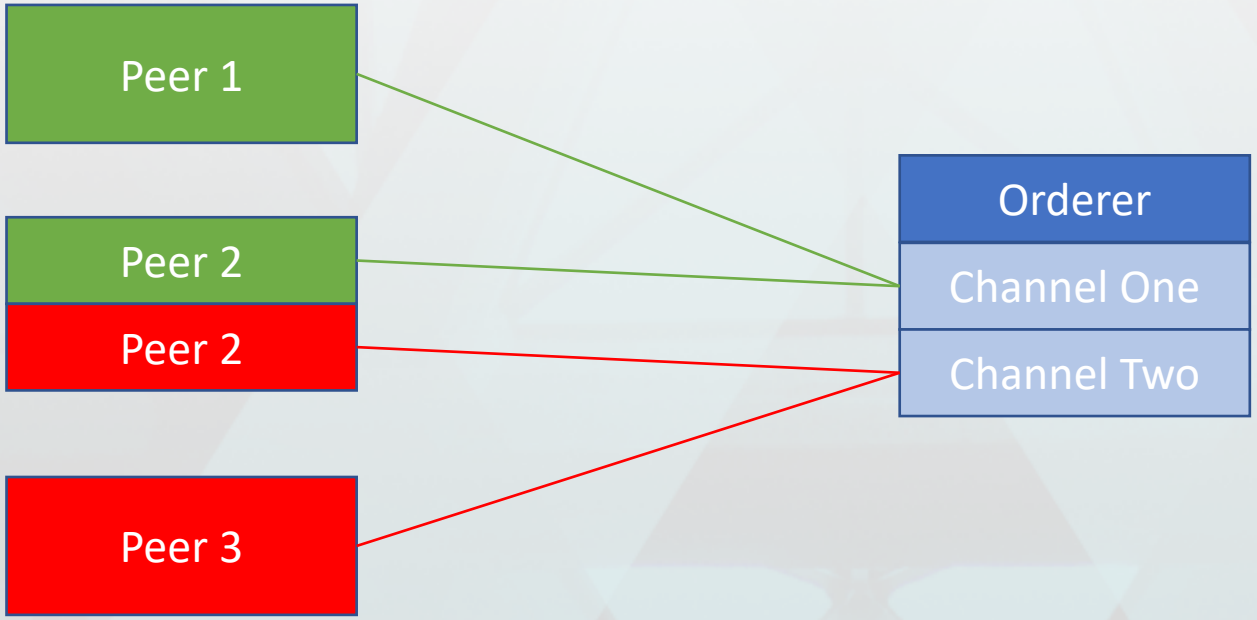
- Channels
- Deploy transactions
- Invoke transaction

Transactions and consensus

- Channels
  - All Fabric transactions occur through a mechanism known as Channels.
  - Channels segment communications between members or organizations in a Fabric network or consortium
- Deploy transactions
- Invoke transaction

Transactions and consensus

Channels



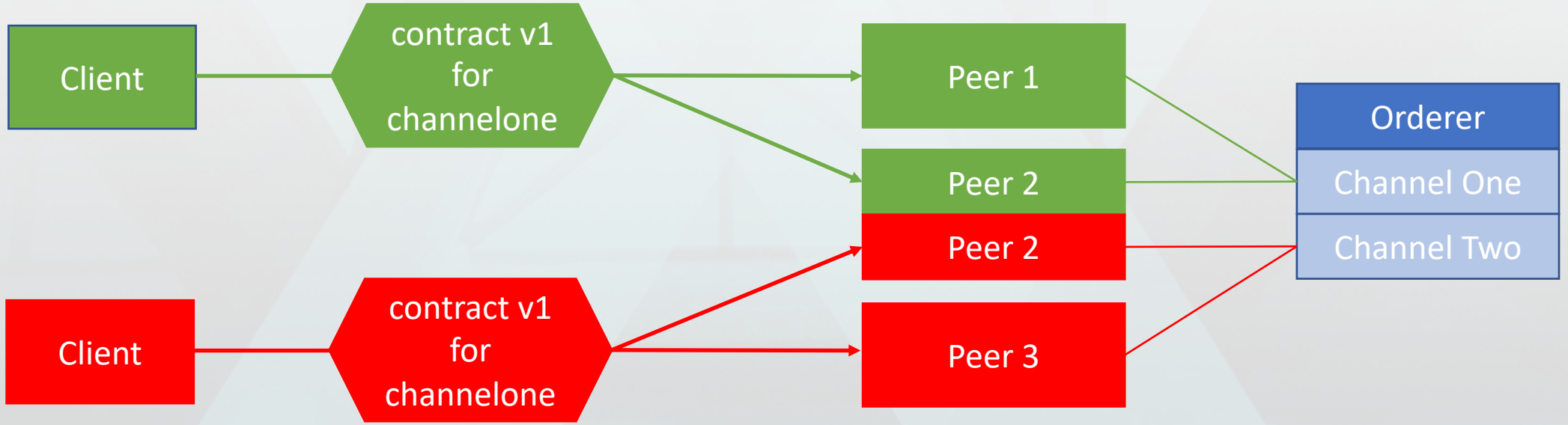
Transactions and consensus

Back to fabric …

- Channels
- Deploy transactions
  - Smart contract deployment is a two step operations (i.e. install and instantiate/upgrade)
  - Recorded in its own “system” ledger
- Invoke transaction

Transactions and consensus

Deploy transactions (install)

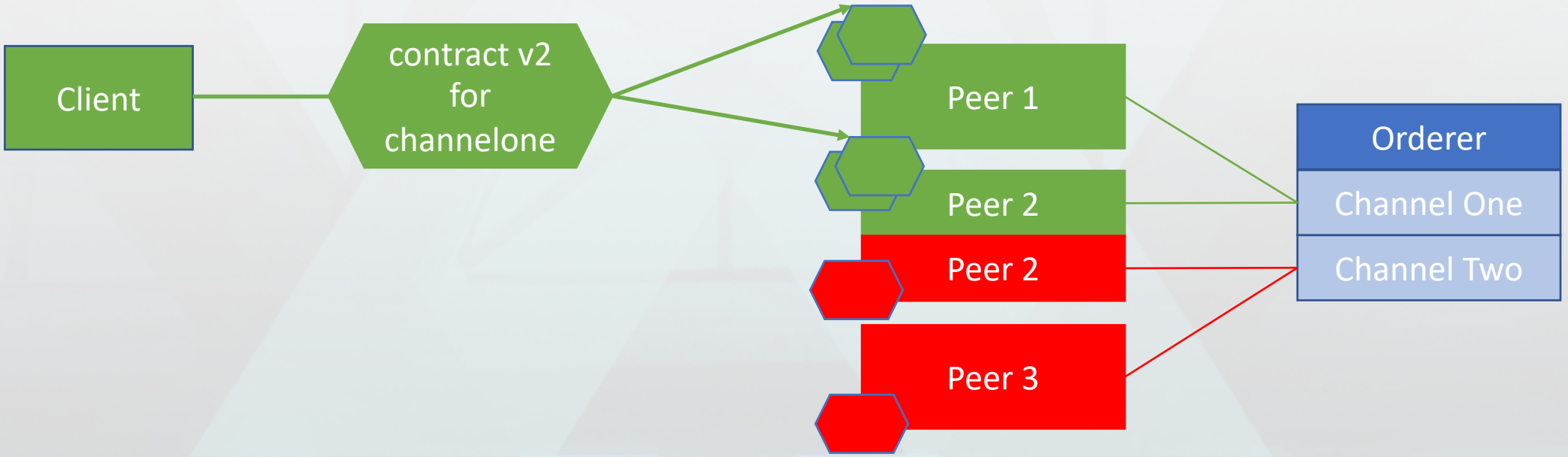


Transactions and consensus

Deploy transactions (instantiate)

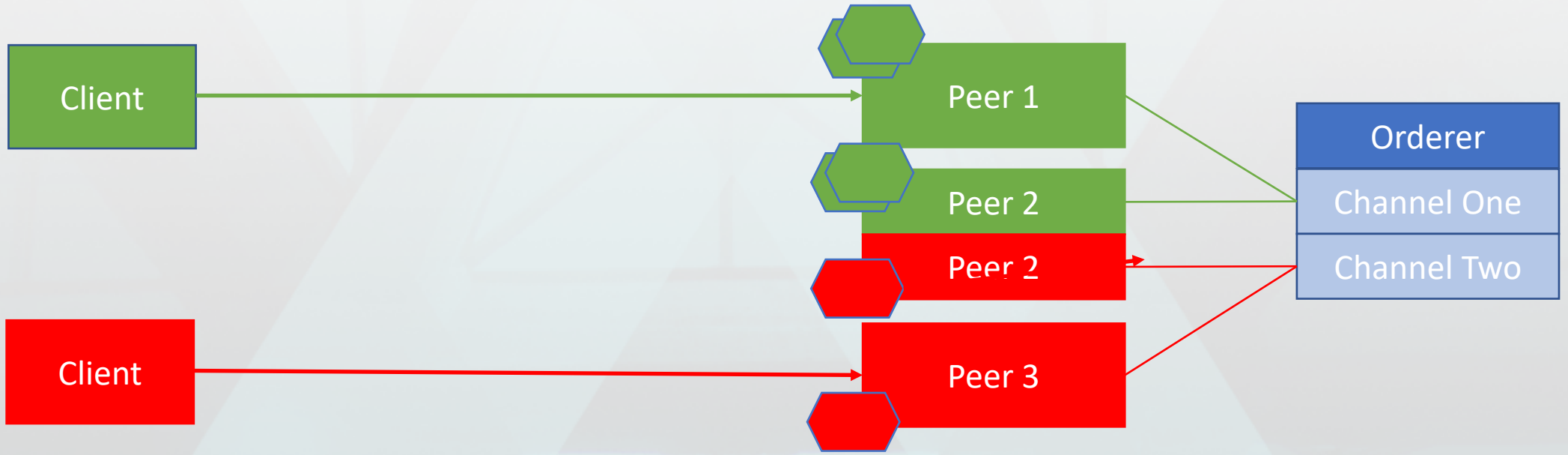
Transactions and consensus

Deploy transactions (install v2)



Transactions and consensus

Deploy transactions (upgrade)



Transactions and consensus

Back to fabric …

- Channels
- Deploy transactions
- Invoke transaction
  - Transaction where members interact with each other
  - Recorded in normal “ledger”

Transaction and consensus

Invoke transaction flow(1)

STEP 1

STEP 2

(1) https://hyperledger-fabric.readthedocs.io/en/release-1.2/txflow.html

Transaction and consensus

Invoke transaction flow(1)

STEP 3

STEP 4

(1) https://hyperledger-fabric.readthedocs.io/en/release-1.2/txflow.html

Transaction and consensus

Invoke transaction flow(1)

STEP 5

(1) https://hyperledger-fabric.readthedocs.io/en/release-1.2/txflow.html

Peers

Architecture over view

Peers

- Endorser peers
  - Simulate and endorse transactions [(1)]
- Committers
  - Verify endorsements and validate transaction results, prior to committing transactions to the blockchain[(1)].
- Anchor Peer
  - Used to initiate gossip communication between peers from different organizations. The anchor peer serves as the entry point for another organization's peer on the same channel to communicate with each of the peers in the anchor peer's organization. Cross-organization gossip is scoped to channels. In order for cross-org gossip to work, peers from one organization need to know the address of at least one peer from another organization in the channel. Each organization added to a channel should identify at least one of its peers as an anchor peer (there can be more than one). The anchor peer address is stored in the configuration block of the channel[(2)].

(1) https://medium.com/swlh/hyperledger-chapter-6-hyperledger-fabric-components-technical-context-767985f605dd
(2) https://hyperledger-fabric.readthedocs.io/en/release-1.2/glossary.html

Ledger, blocks and world state

Architecture over view

Ledger, blocks and world state

Ethereum

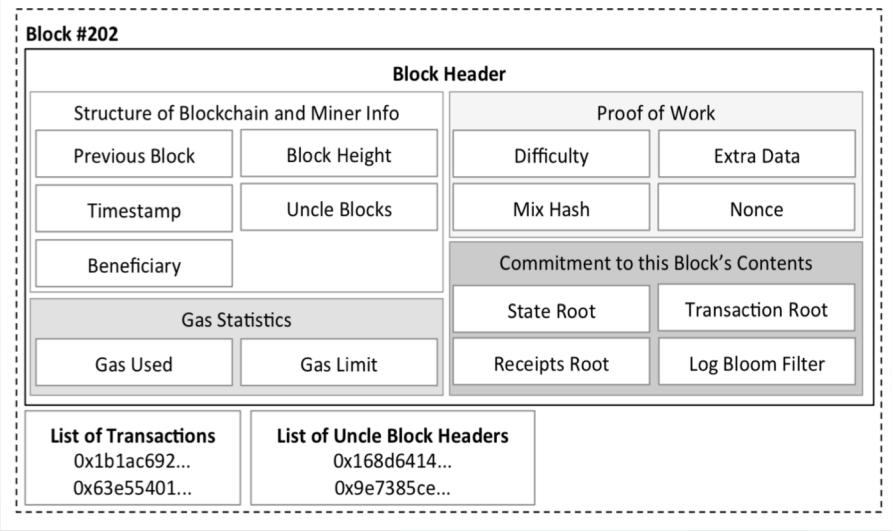
- Blockchain
- State global stack or heap base variable based (I think?)

Fabric

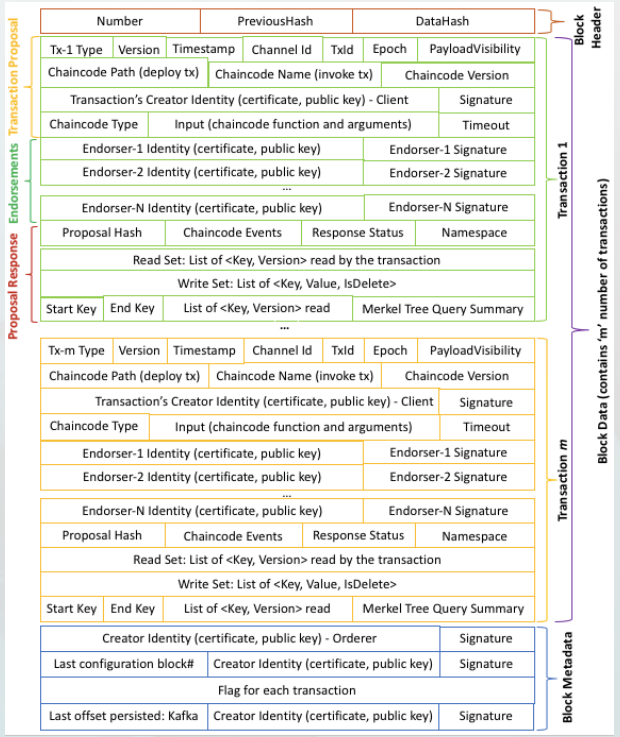
- Blockchain
- State - Key Value Store (World State)
  - LevelDB (default)
  - CouchDB
  - Relational - if you like

Ledger, blocks and world state

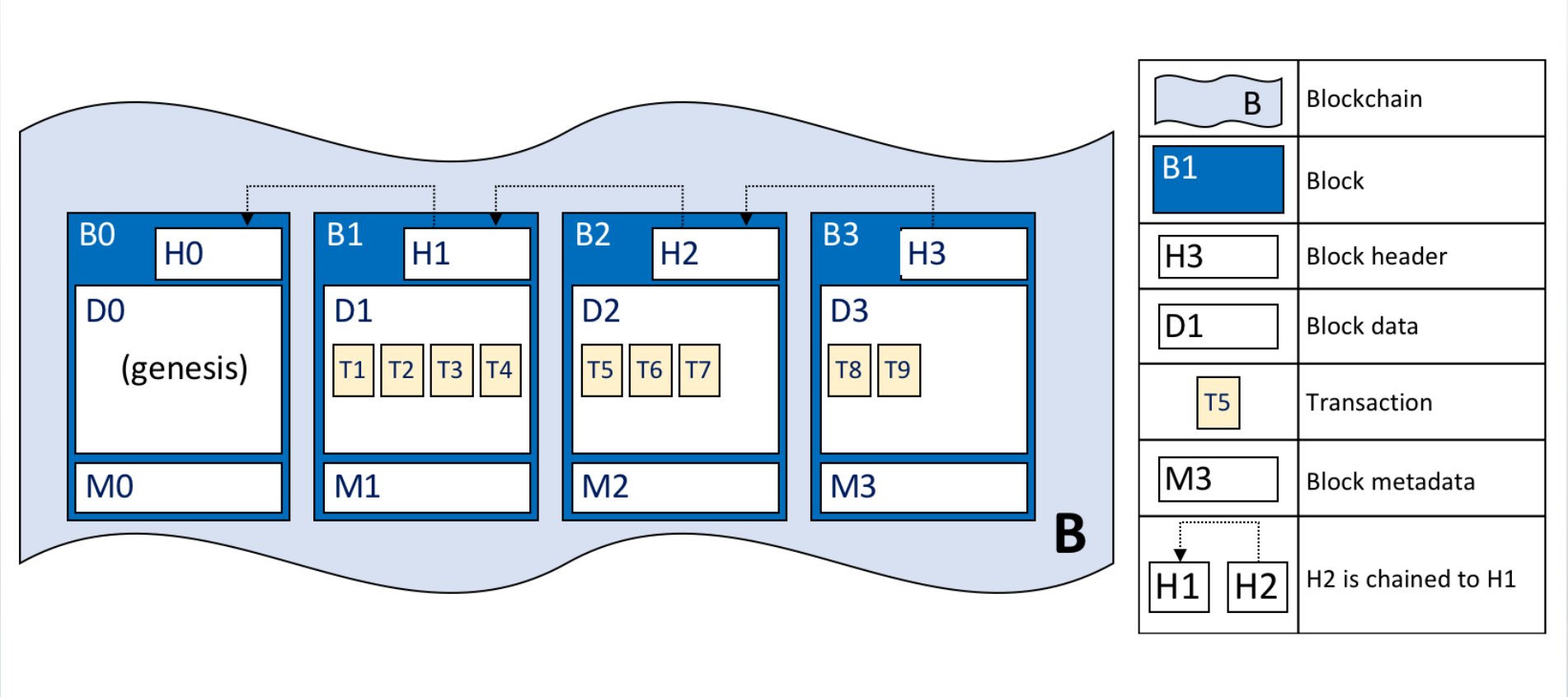
Ethereum



Fabric

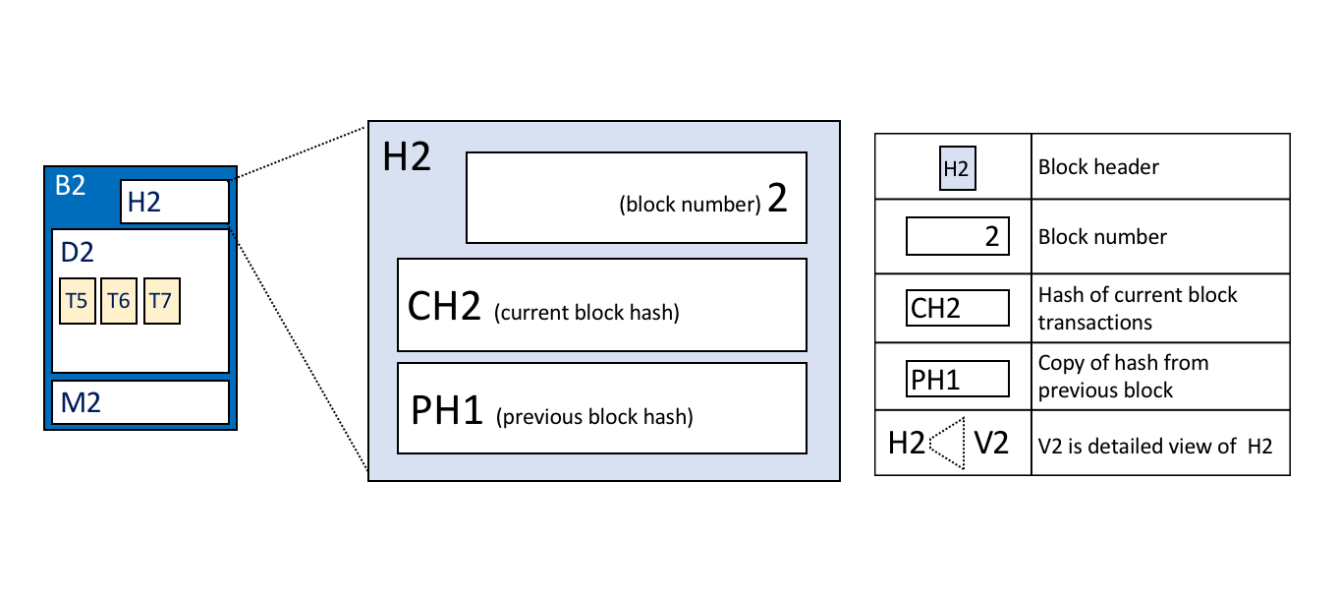


Ledger, blocks and world state(1)



(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/ledger/ledger.html

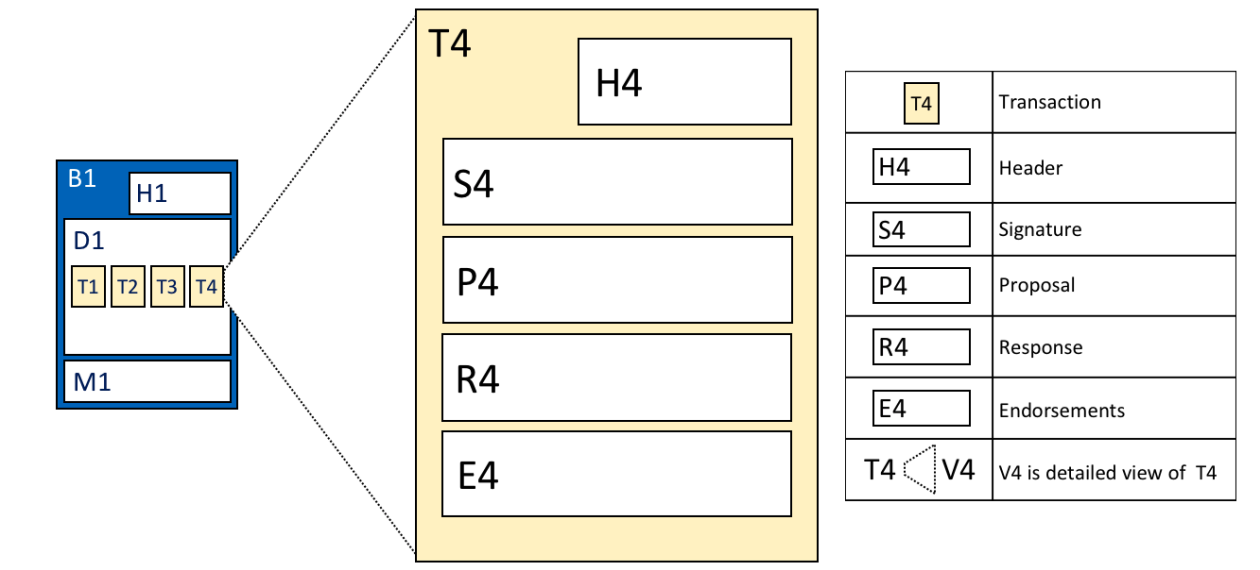
Ledger, blocks and world state (1)



- Block data
  - List of transactions arranged in order
- Block metadata
  - Time the block was written, certificate, public key and signature of block writer

(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/ledger/ledger.html

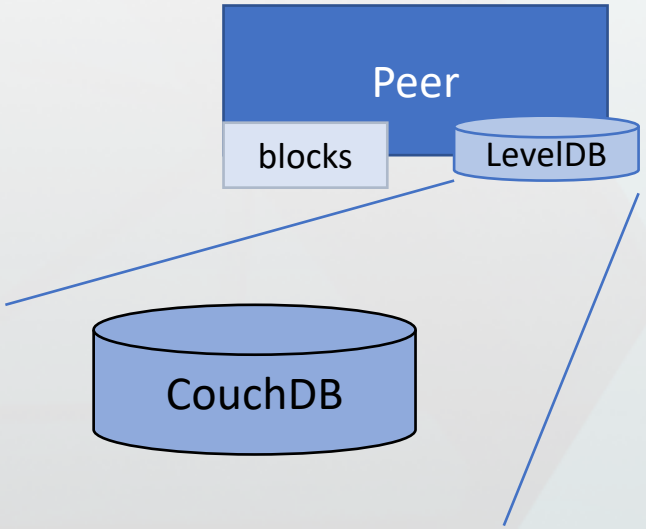
Ledger, blocks and world state (1)

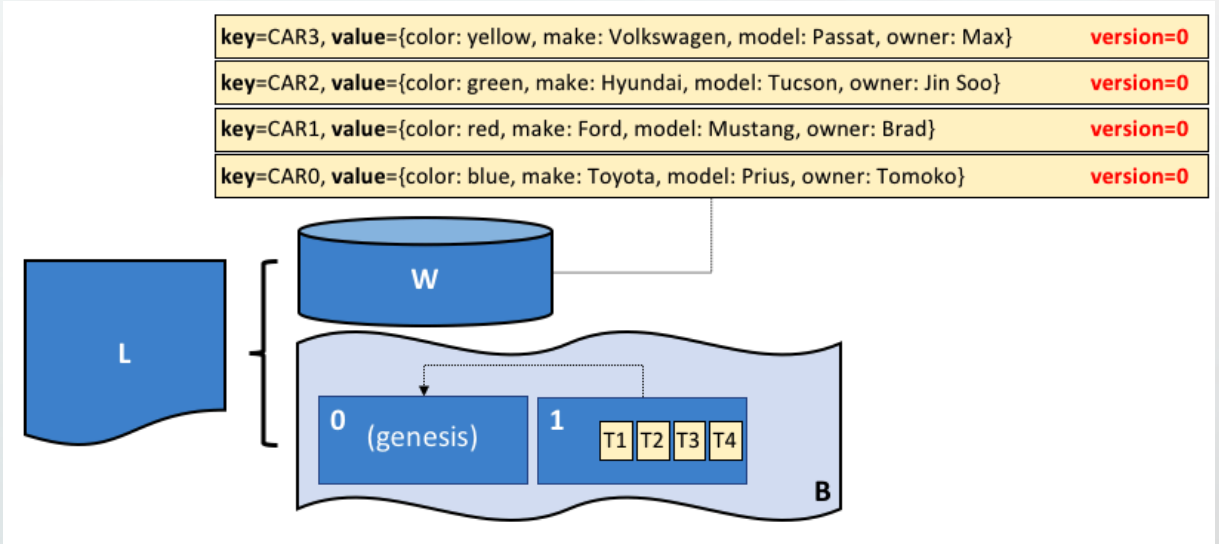


- Header – chaincode, func name, version
- Response – before and after values of world state

(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/ledger/ledger.html

Ledger, blocks and world state





(1)

(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/ledger/ledger.html

Identity service

Architecture overview

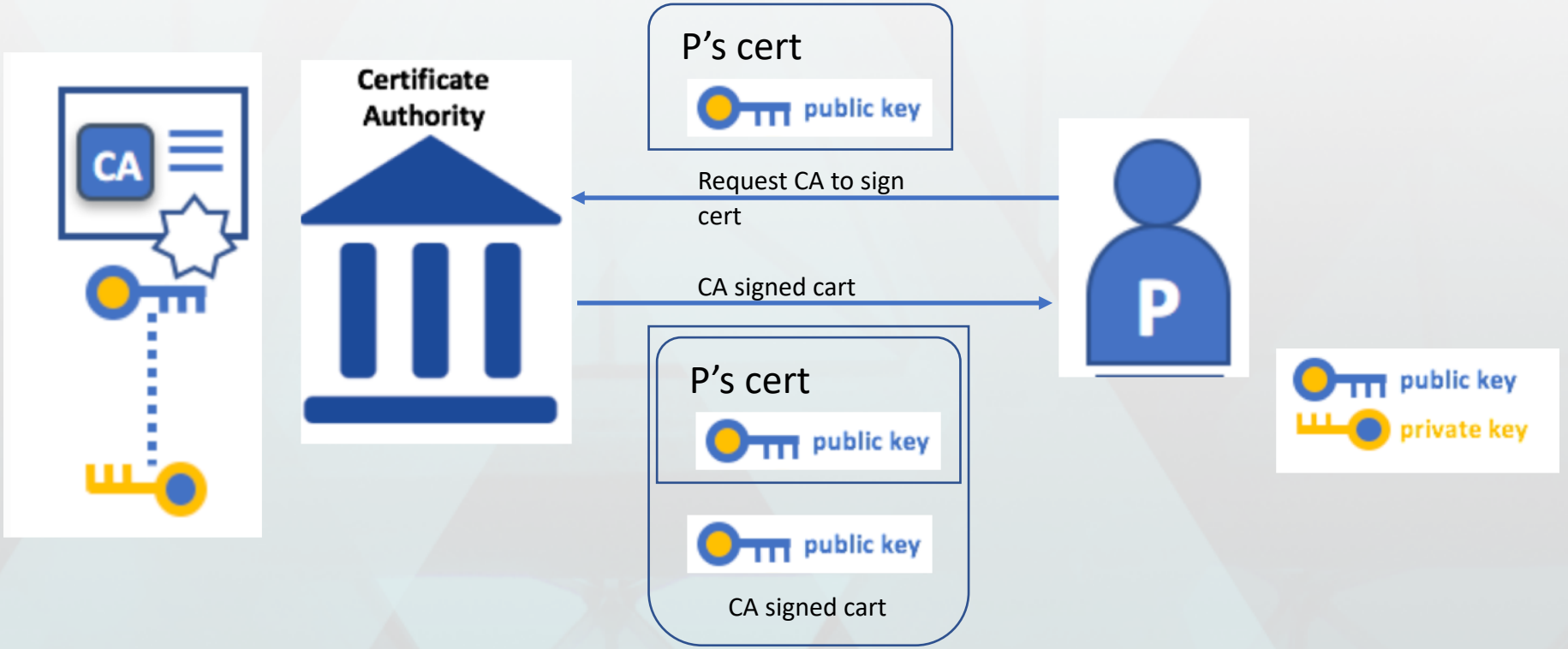
Identity service(1)

- All elements of Fabric, client, peers and orderers has a digital identity
- Fabric use a mechanism known as X.509 digital certificates similar to SSH/SSL mechanism (also known as Public Key Infrastructure)
- Use certificate authority(ies) to provide source of trust
- Fabric Certificate Authority (provided by Hyperledger community) use to identify users
- Membership Service Provider (MSP) is a kind of wallet used by all Fabric elements for identity management – generate using a tool call cryptogen

(1) https://hyperledger-fabric.readthedocs.io/en/release-1.2/identity/identity.html

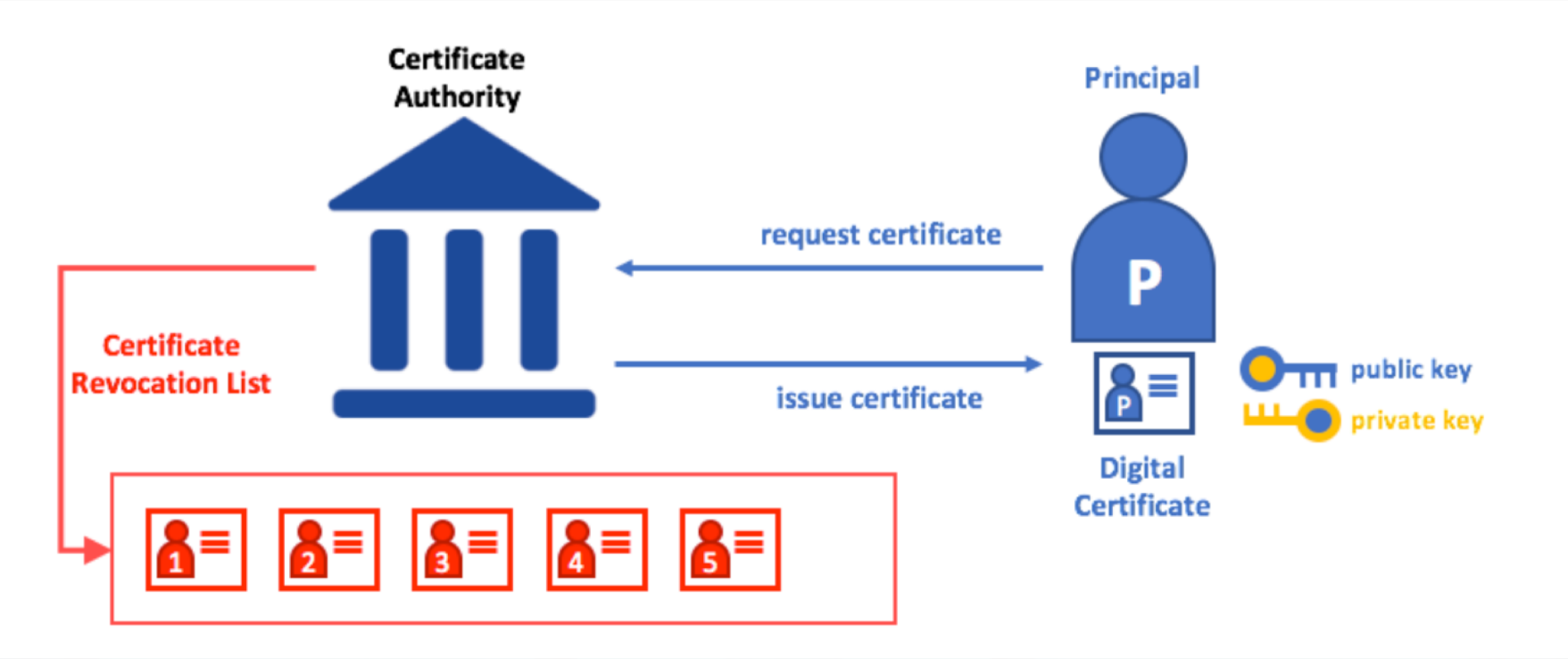
Identity service

Certificate Authority



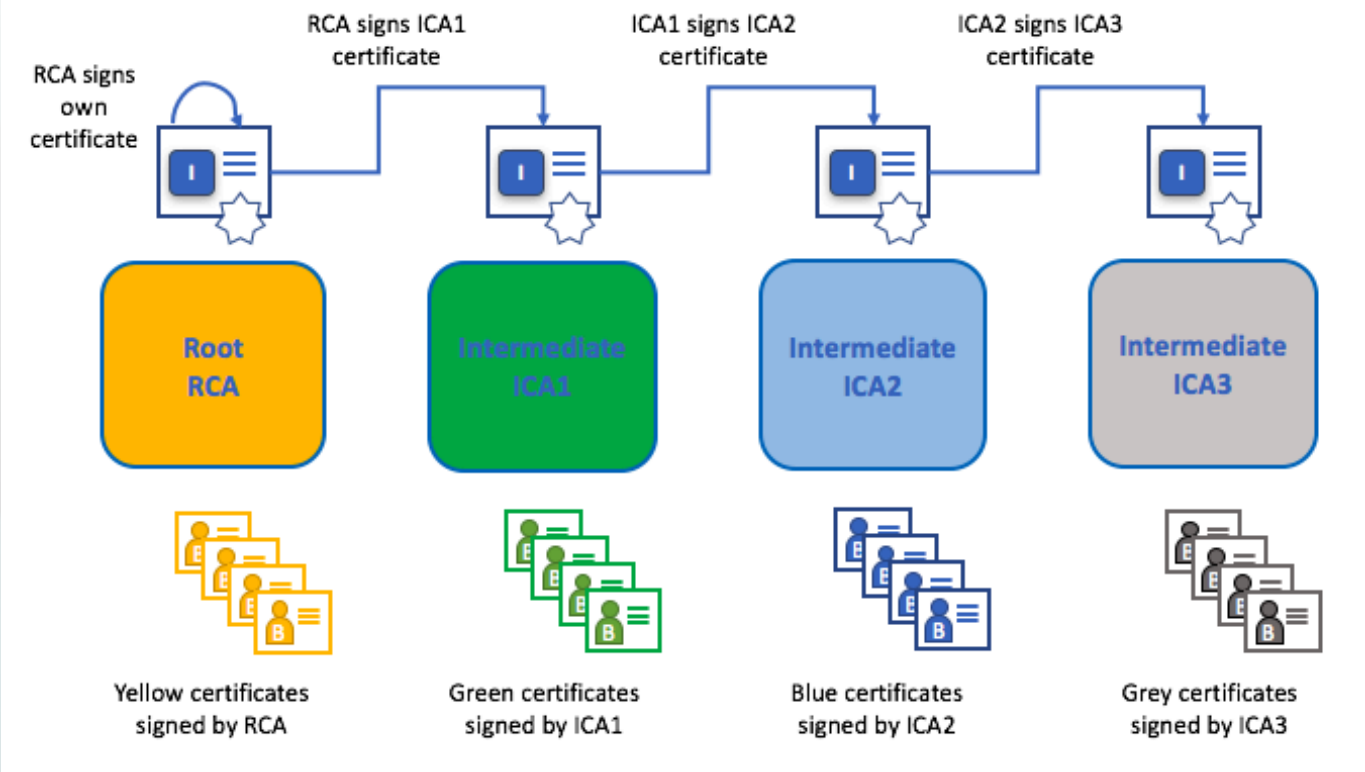
Identity service

Certificate Authority(1)



Identity service

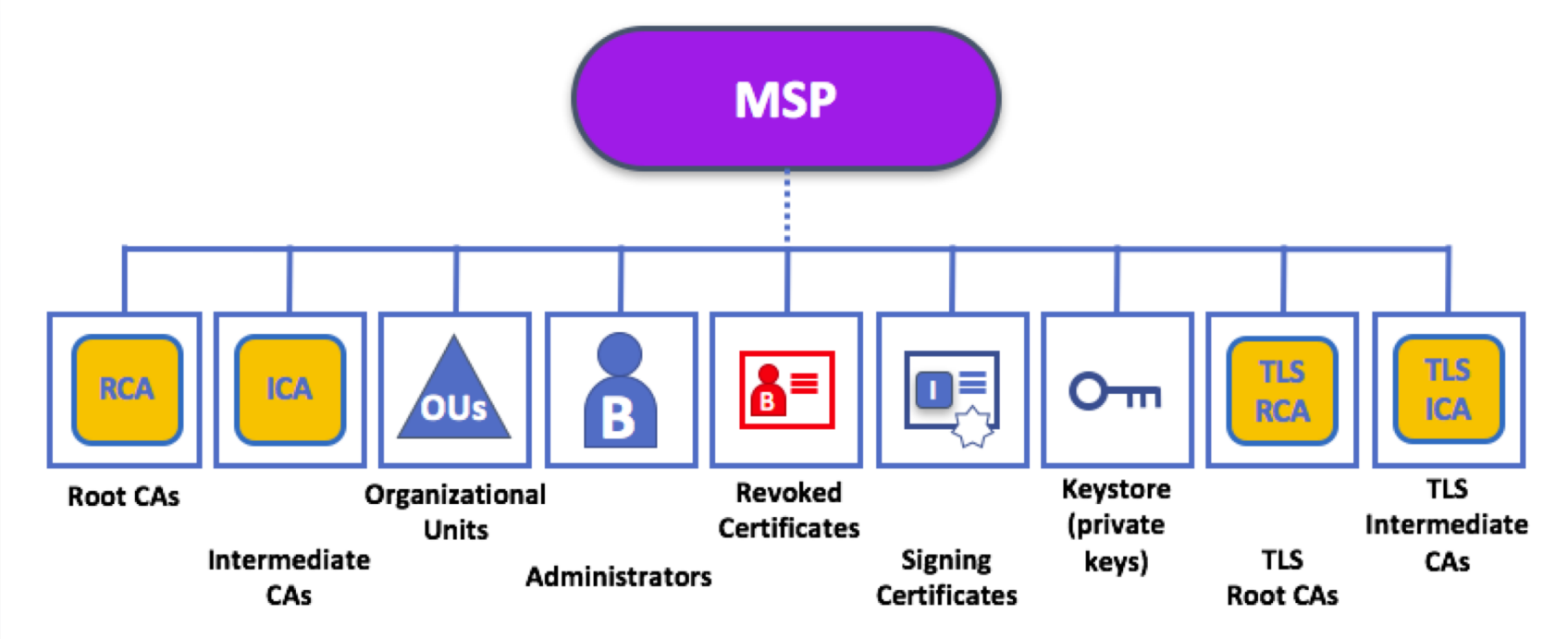
Certificate Authority[1]



(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/identity/identity.html

Identity service

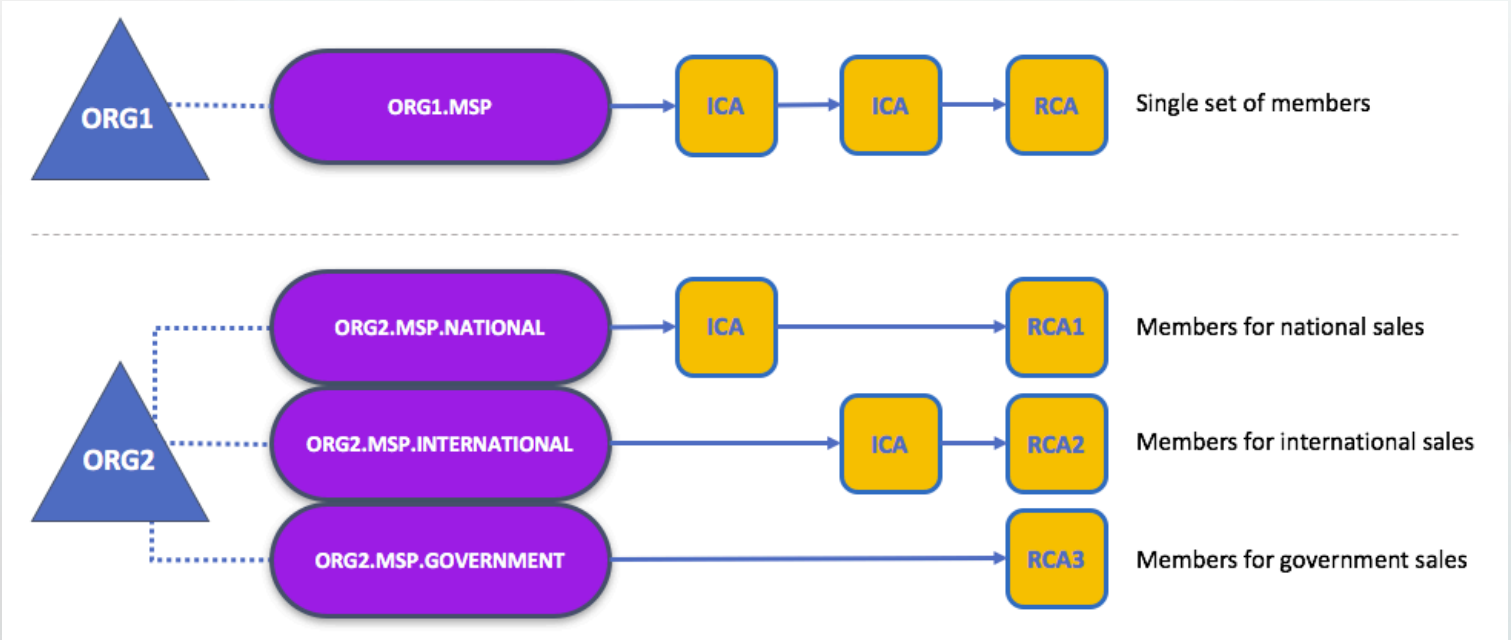
Membership Service Provider[(1)]



(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/membership/membership.html

Identity service

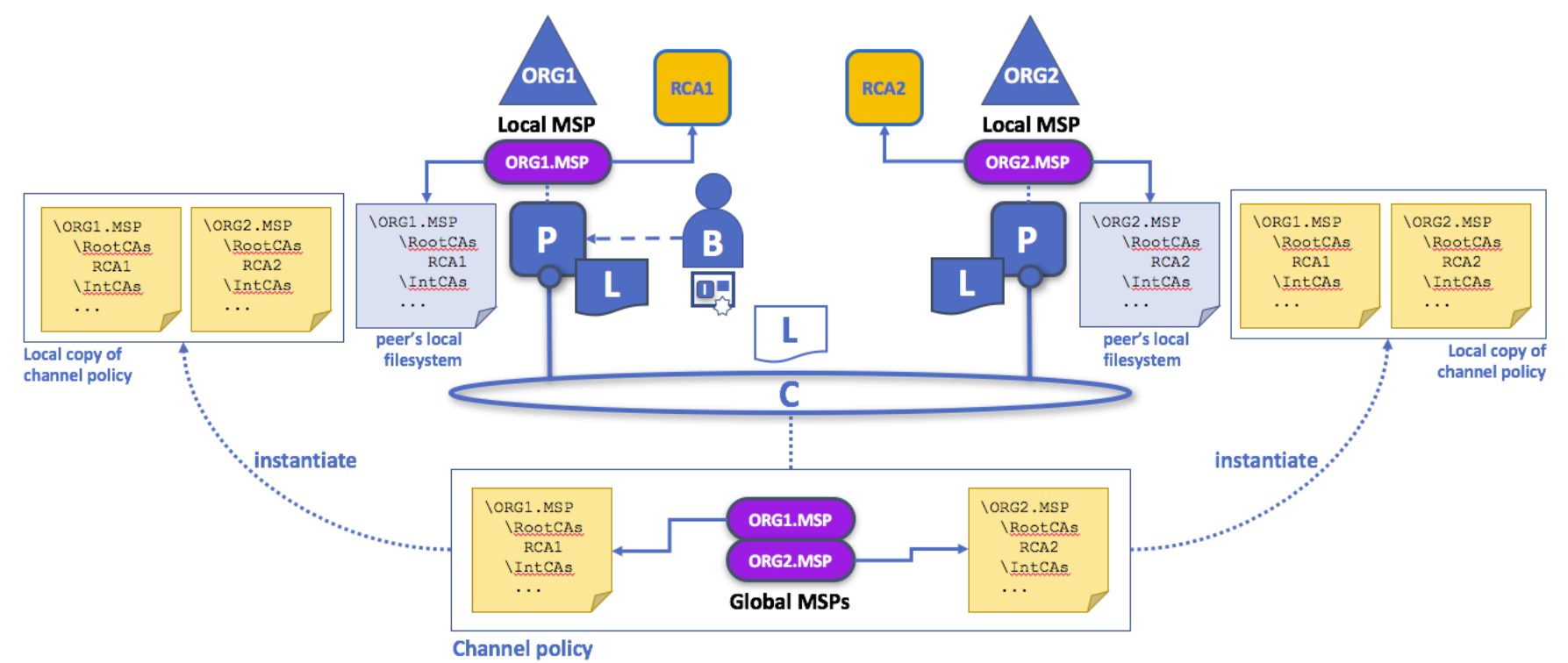
Mapping MSPs to multiple CAs(1)



(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/membership/membership.html

Identity service

Local and global MSP(1)



(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/membership/membership.html

Identity service

Local and global MSP(1)

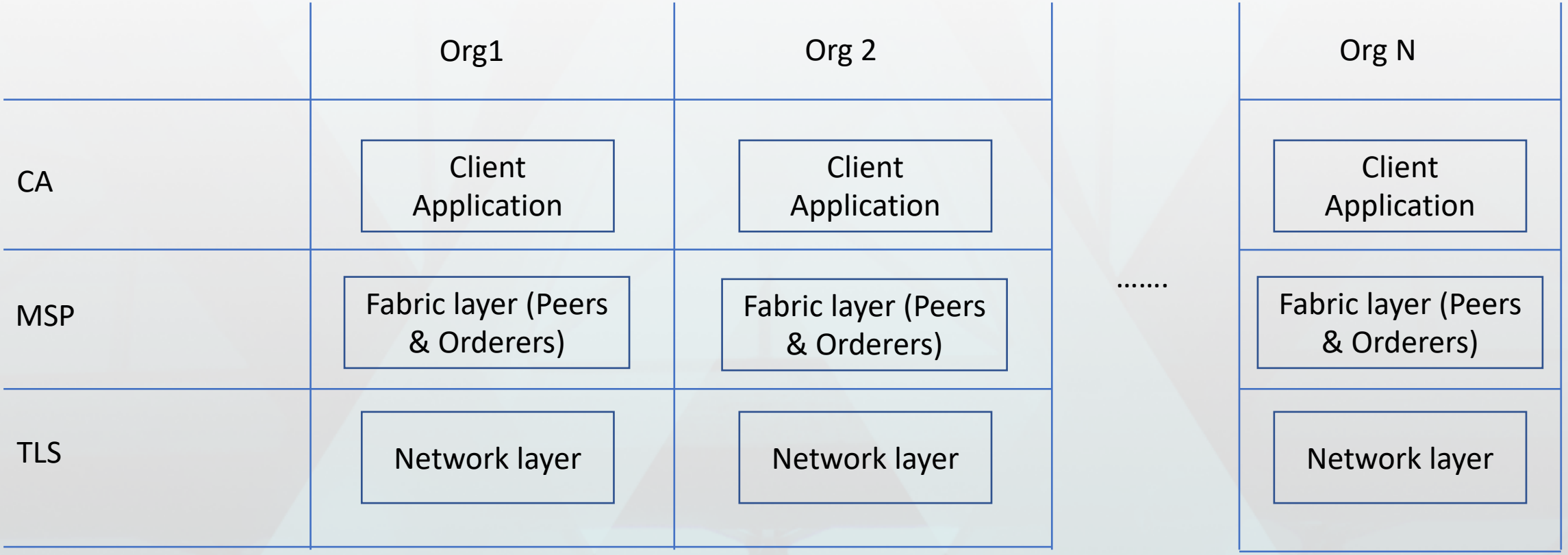
- An administrator B connects to the peer with an identity issued by RCA1 and stored in their local MSP.
- When B tries to install a smart contract on the peer, the peer checks its local MSP, ORG1-MSP, to verify that the identity of B is indeed a member of ORG1. A successful verification will allow the install command to complete successfully.
- Subsequently, B wishes to instantiate the smart contract on the channel. Because this is a channel operation, all organizations on the channel must agree to it.
- Therefore, the peer must check the MSPs of the channel before it can successfully commit this command.

(1) https://hyperledger-fabric.readthedocs.io/en/release-1.3/membership/membership.html

Fabric Governance Model

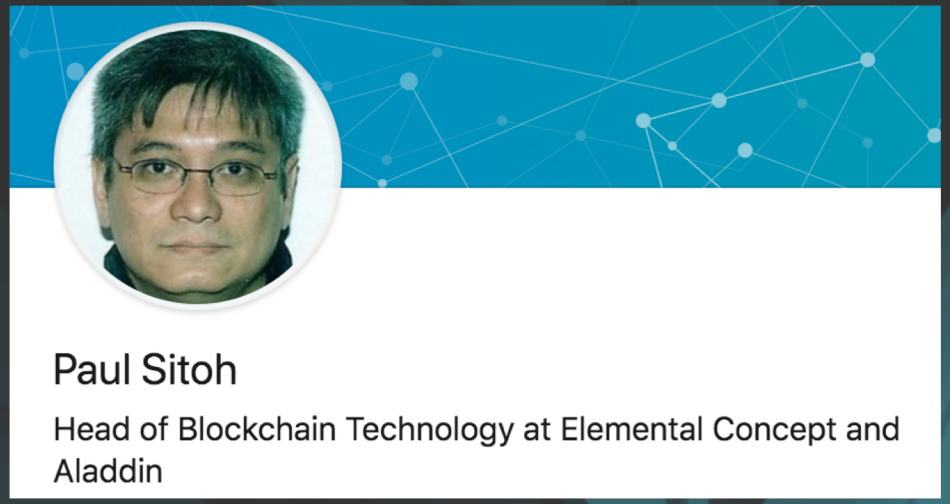
Architecture overview

Fabric Governance Model



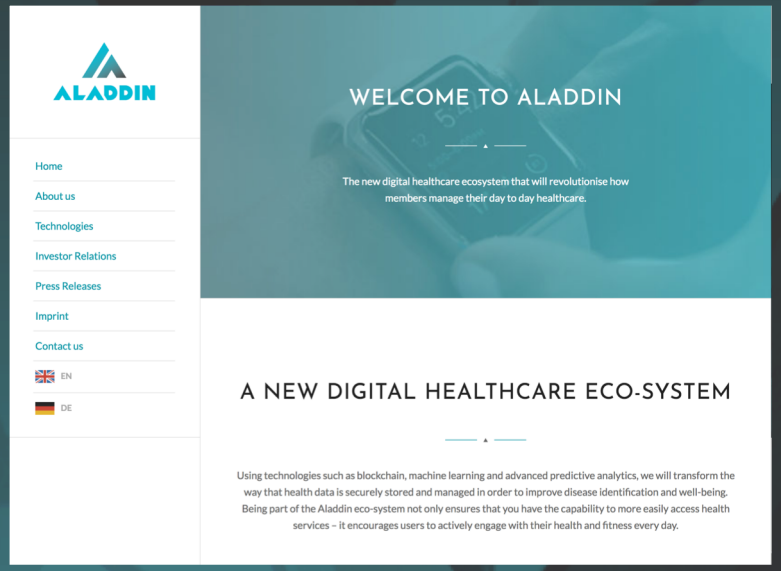
Q & A

Architecture overview



Paul Sitoh

Head of Blockchain Technology at Elemental Concept and Aladdin



paul@elementalconcept.com