BLOCKCHAINS

ARCHITECTURE, DESIGN AND USE CASES

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA

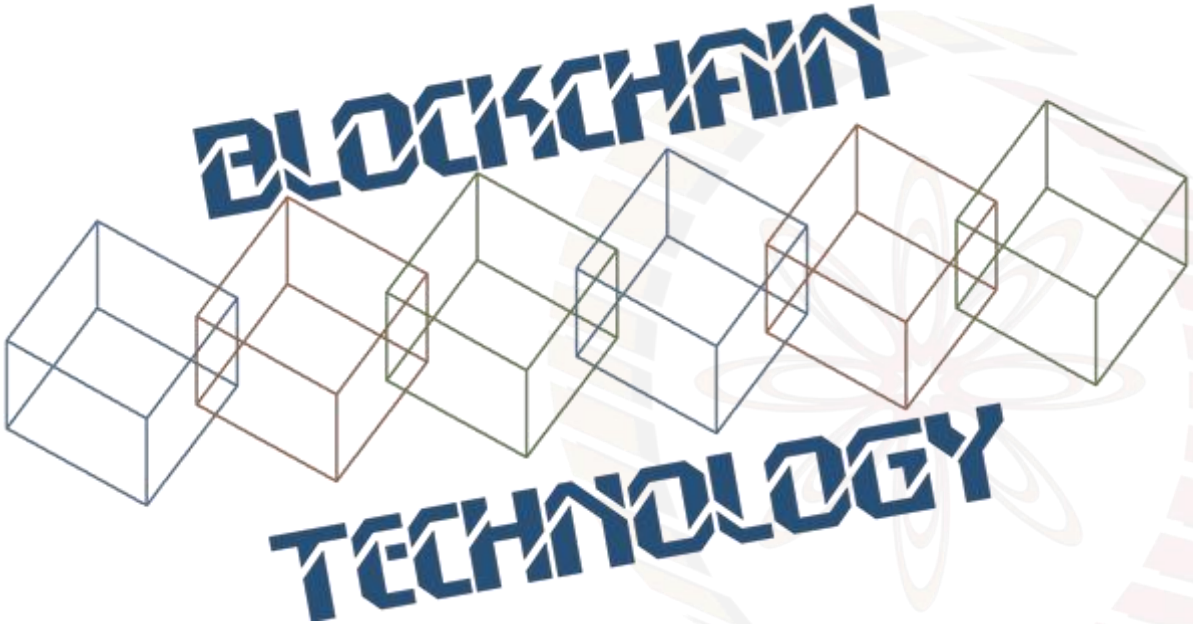


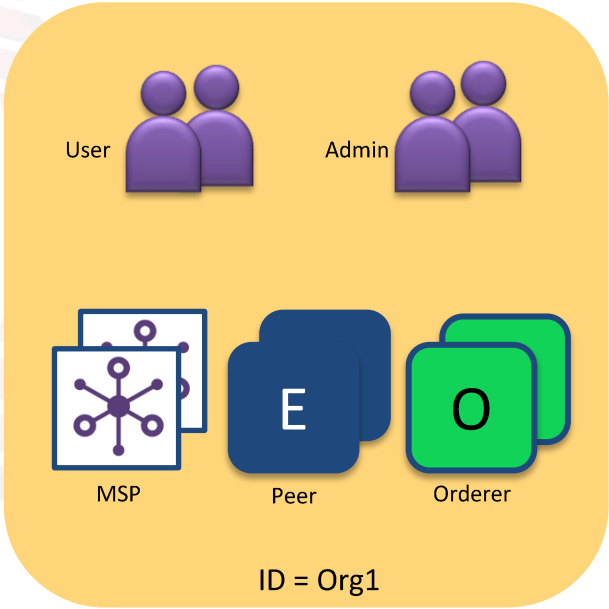
Image courtesy: http://beetfusion.com/

MEMBERSHIP AND IDENTITY MANAGEMENT

Organisations

Organisations define boundaries within a Fabric Blockchain Network

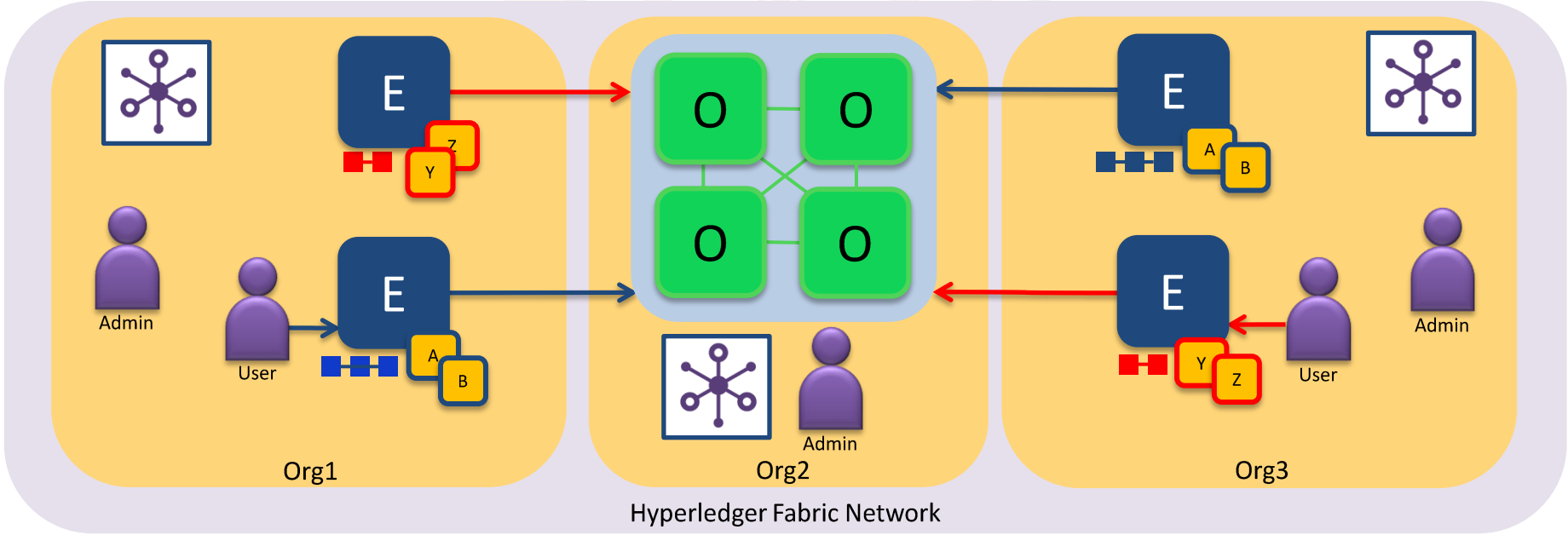
- Each organisation defines:
  - Membership Services Provider (MSP) for identities
  - Administrator(s)
  - Users
  - Peers
  - Orderers (optional)
- A network can include many organisations representing a consortium
- Each organisation has an ID



Consortium Network

An example consortium network of 3 organisations

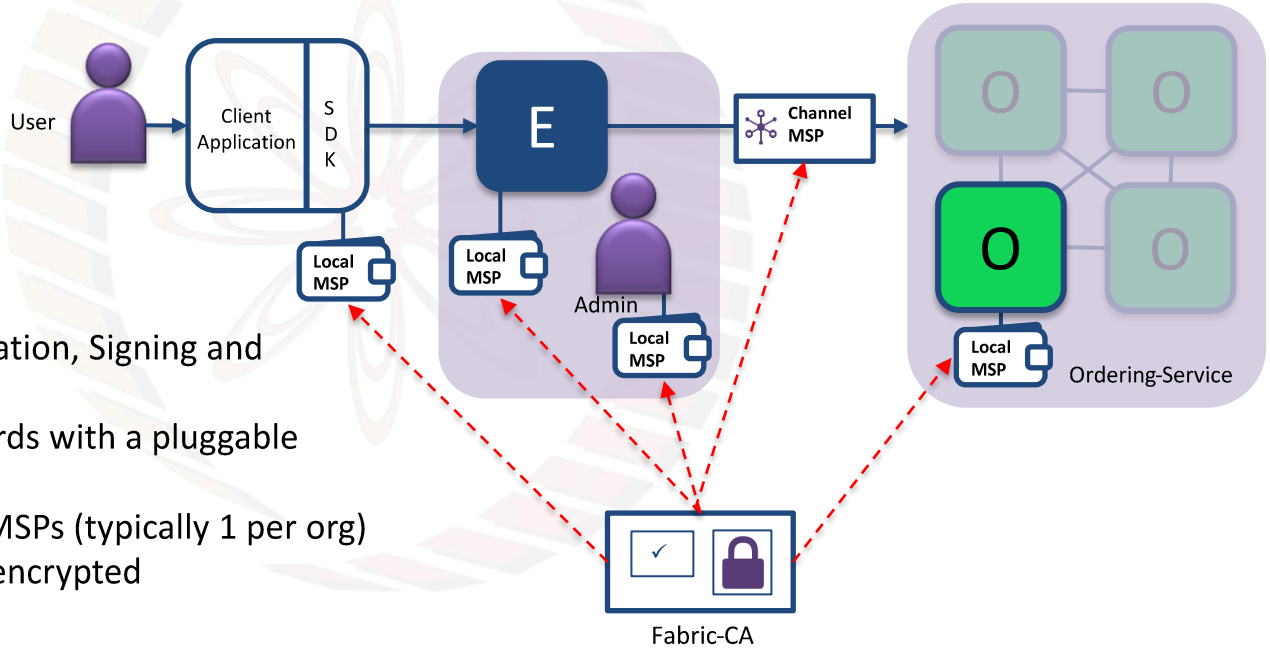
- Orgs 1 and 3 run peers
- Org 2 provides the ordering service only



Membership Service Provider (MSP) - Overview

A MSP manages a set of identities within a distributed Fabric network

- Provides identity for:
  - Peers and Orderers
  - Client Applications
  - Administrators
- Identities can be issued by:
  - Fabric-CA
  - An external CA
- Provides: Authentication, Validation, Signing and Issuance
- Supports different crypto standards with a pluggable interface
- A network can include multiple MSPs (typically 1 per org)
- Includes TLS crypto material for encrypted communications



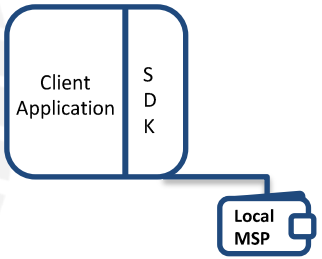
Transport Layer Security (TLS)

- Cryptographic protocols that provide communications security over a computer network
- Provides privacy and data integrity
- Symmetric cryptography is used to encrypt the data transmitted (privacy)
- Public-key cryptography is used to authenticate the identities of the communicating parties
- Include message integrity check to prevent loss or alteration of the data
- All component communication in Fabric secured using TLS (client-peer, peer-peer, peer-orderer, orderer-orderer)

User Identities

Each client application has a local MSP to store user identities

- Each local MSP includes:
  - **Keystore**
    - **Private key** for signing transactions
  - **Signcert**
    - **Public x.509 certificate**



- May also include TLS credentials
- Can be backed by a Hardware Security Module (HSM)

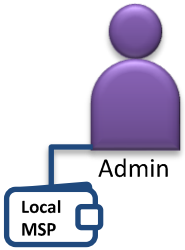
user@org1.example.com	
keystore	<private key>
signcert	user@org1.example.com-cert.pem

Admin Identities

Each Administrator has a local MSP to store their identity

- Each local MSP includes:
  - **Keystore**
    - **Private key** for signing transactions
  - **Signcert**
    - **Public x.509 certificate**

- May also include Transport Layer Security (TLS) credentials
- Can be backed by a Hardware Security Module (HSM)



admin@org1.example.com	
keystore	<private key>
signcert	admin@org1.example.com-cert.pem

Peer and Orderer Identities

Each peer and orderer has a local MSP

- Each local MSP includes:
  - **keystore**
    - **Private key** for signing transactions
  - **signcert**
    - **Public x.509 certificate**

- In addition Peer/Orderer MSPs identify authorized administrators:
  - **admincerts**
    - List of **administrator certificates**
  - **cacerts**
    - The **CA public cert** for verification
  - **crls**
    - List of **revoked certificates**

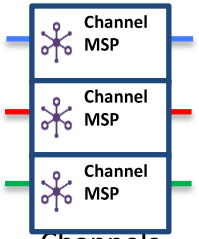
- Peers and Orderers also receive channel MSP info
- Can be backed by a Hardware Security Module (HSM)

peer@org1.example.com	
admincerts	admin@org1.example.com-cert.pem
cacerts	ca.org1.example.com-cert.pem
keystore	<private key>
signcert	peer@org1.example.com-cert.pem
crls	<list of revoked admin certificates>

Channel MSP Information

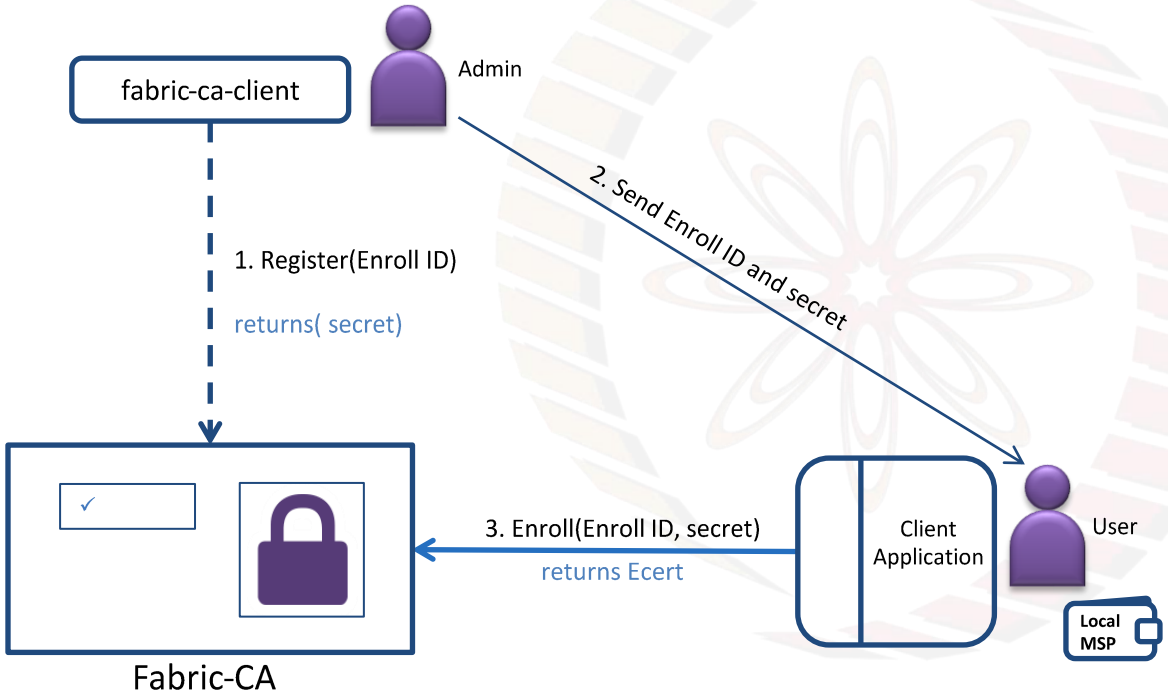
Channels include additional organisational MSP information

- Determines which orderers or peers can join the channel
- Determines client applications read or write access to the channel
- Stored in configuration blocks in the ledger
- Each channel MSP includes:
  - **admincerts**
    - Any public certificates for administrators
  - **cacerts**
    - The CA public certificate for this MSP
  - **crls**
    - List of revoked certificates
- Does not include any private keys for identity



ID = MSP1	
admincerts	admin.org1.example.com-cert.pem
cacerts	ca.org1.example.com-cert.pem
crls	<list of revoked admin certificates>

New User Registration and Enrollment



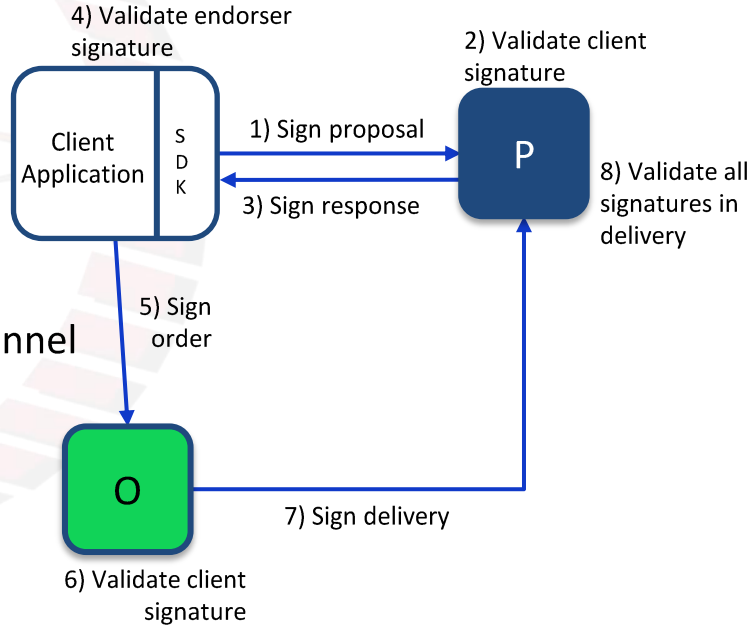
Registration and Enrollment

- Admin registers new user with Enroll ID
- User enrolls and receives credentials
- Additional offline registration and enrollment options available

Transaction Signing

All transactions within a Hyperledger Fabric network are signed by permissioned actors, and those signatures are validated

- Actors sign transactions with their enrolment private key
  - Stored in their local MSP
- Components validate transactions and certificates
  - Root CA certificates and CRLs stored in local MSP
  - Root CA certificates and CRLs stored in Org MSP in channel



Fun Reading

- Transport Layer Security (TLS), Wikipedia article: https://en.wikipedia.org/wiki/Transport_Layer_Security
- Digital Identity, Wikipedia article: https://en.wikipedia.org/wiki/Digital_identity
- Digital Signatures, Wikipedia article: https://en.wikipedia.org/wiki/Digital_signature
- X.509 Certificate, Wikipedia article: https://en.wikipedia.org/wiki/X.509


thank you!