Concepts & Deep Dive

raj@acloudfan.com

@acloudfan

http://ACloudFan.com

Discount Coupon Links to UDEMY courses:

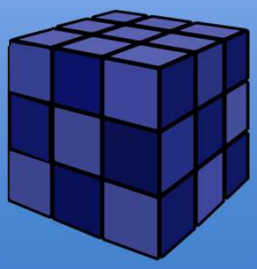
https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

This deck is part of a online course on "Hyperledger Fabric Development with Composer"



Client Nodes

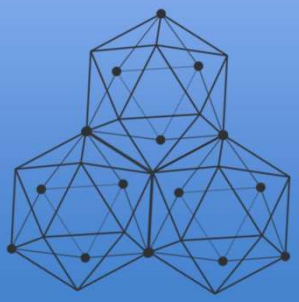
raj@acloudfan.com

@acloudfan

http://ACloudFan.com

Learning Objectives:

- Client
- Endorsement policy

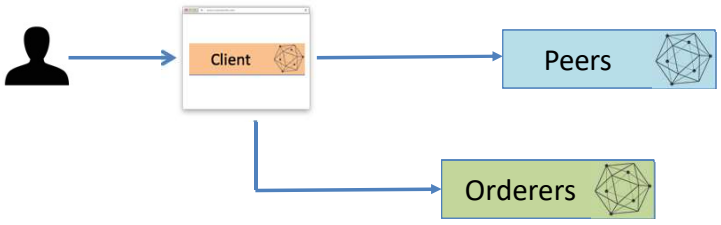


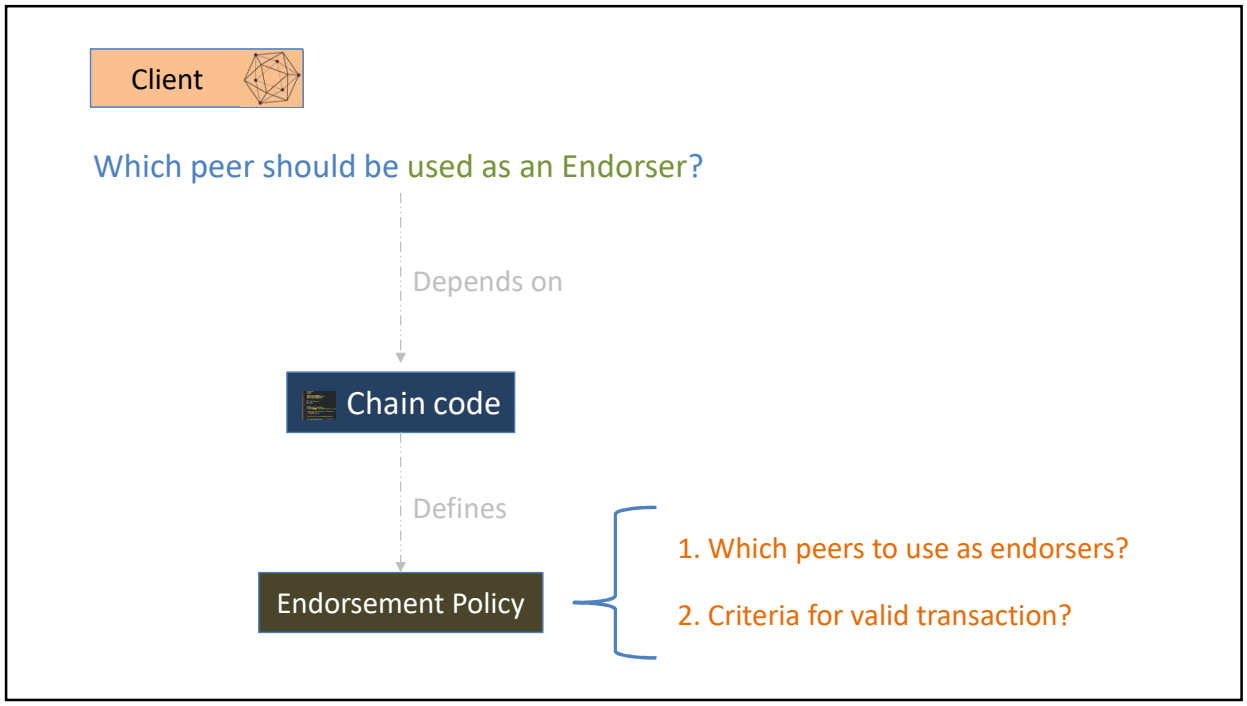
Client

- Client node acts on behalf of the end user
  - a.k.a *Submitting-Client*
- Creates Txn Request and send Endorser(s)

Client

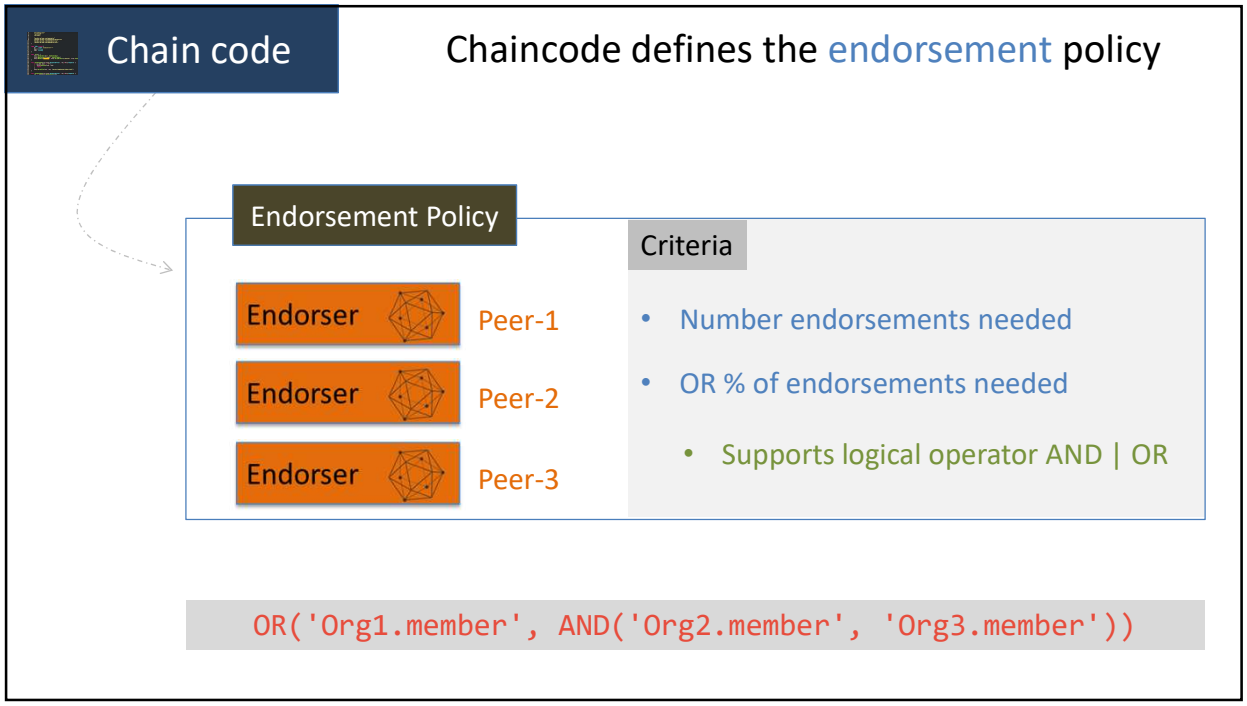
- Connects to a Orderer for broadcasting validated transaction

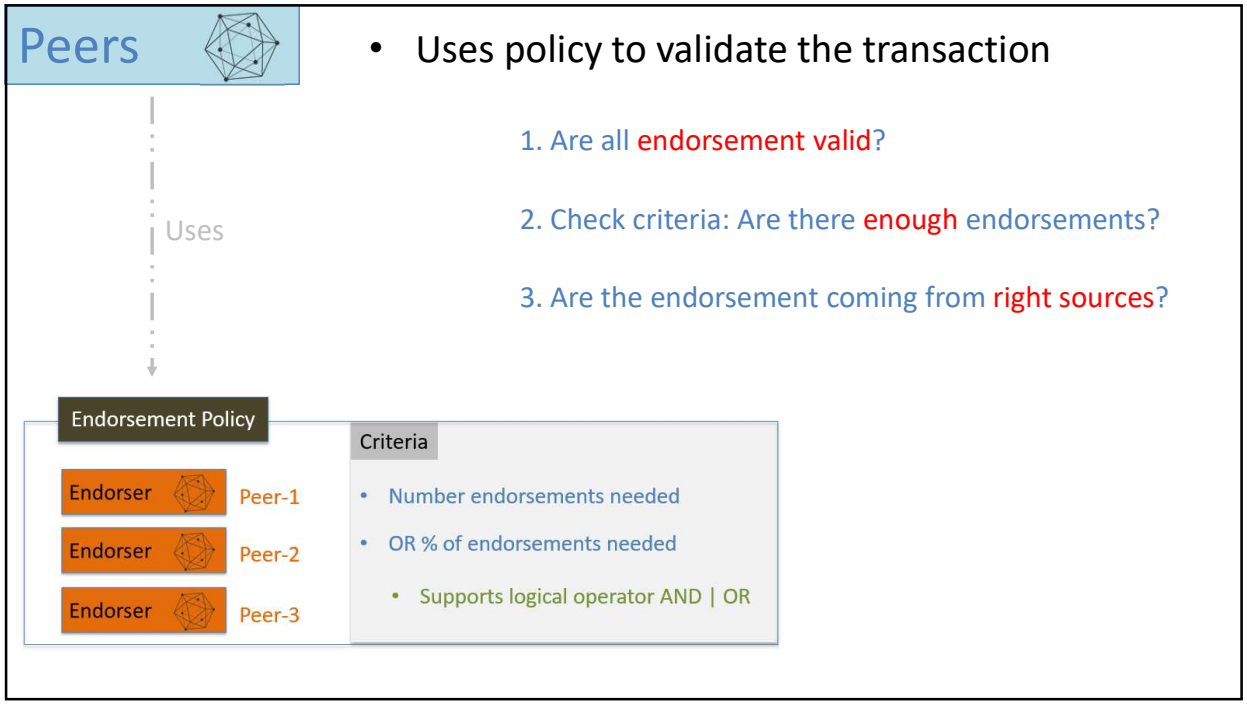




Endorsement Policy

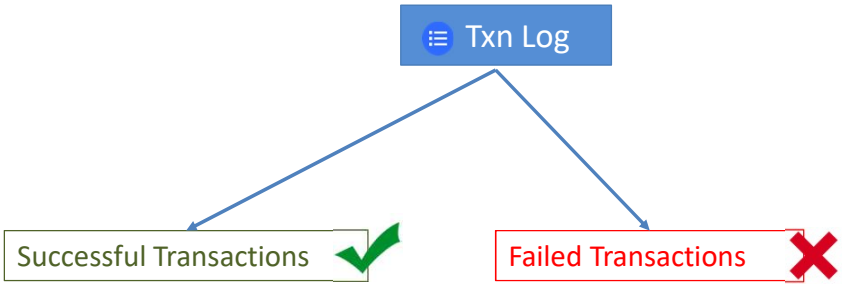
- Association of Endorsement Policy is Optional
- Specified at the time of deployment of chaincode
- Default policy:
  - Any 1 Endorsing peer from default MSP/Organization


Chain code
Chaincode defines the endorsement policy
Endorsement Policy
Endorser
Peer-1
Endorser
Peer-2
Endorser
Peer-3
Criteria
Number endorsements needed
OR % of endorsements needed
Supports logical operator AND | OR
OR('Org1.member', AND('Org2.member', 'Org3.member'))


Peers
Uses
Uses policy to validate the transaction
1. Are all endorsement valid?
2. Check criteria: Are there enough endorsements?
3. Are the endorsement coming from right sources?
Endorsement Policy
Endorser
Peer-1
Endorser
Peer-2
Endorser
Peer-3
Criteria
Number endorsements needed
OR % of endorsements needed
Supports logical operator AND | OR

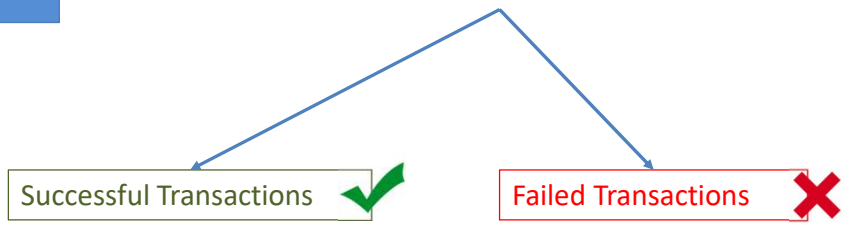
Peers

Adds the transaction to the ledger



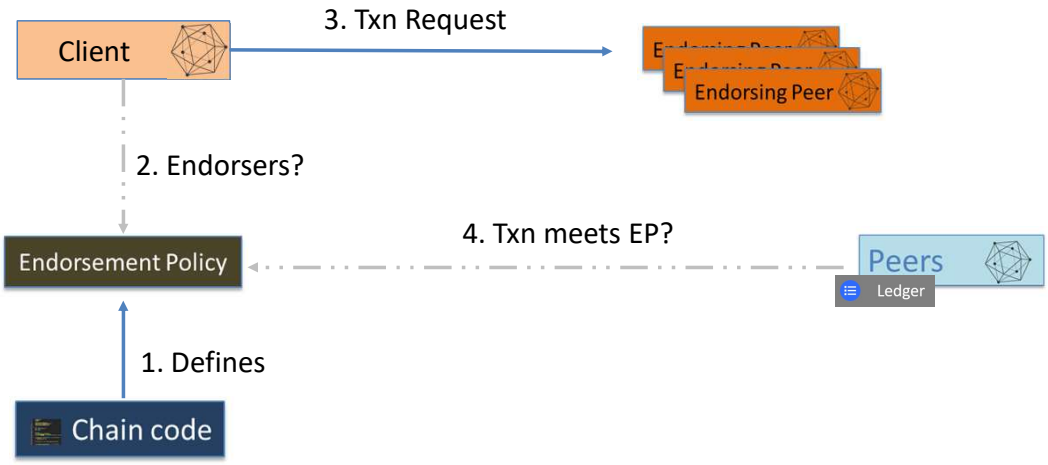
Txn Log

- A chronological record of all state changes



- Transaction history may be used for re-creating the state
  - State data maintained in network may be thought of as optional
- Peers in the network maintain local copy of the ledger

Summary



Orderer Nodes

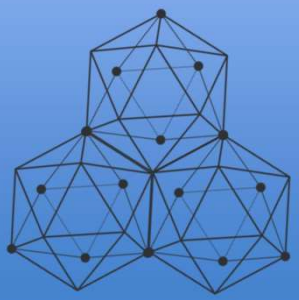
Learning Objectives:

- Functions
- Implementation

raj@acloudfan.com

@acloudfan

http://ACloudFan.com



Orderer 

Communication channel for fabric

- Also referred to as Ordering Service
- Responsible for consistent ledger state across the network
  - Consensus mechanism
  - Ensures order of transactions
- Creates the blocks & gurantees atomic delivery

Orderer 

Implemented with Message Oriented Middleware

SOLO

Single node = Good for development | dev mode

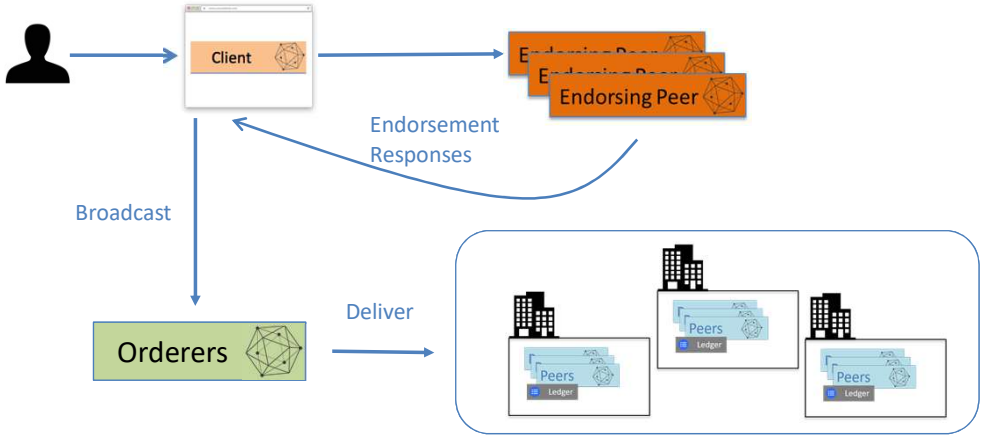
Single point of failure

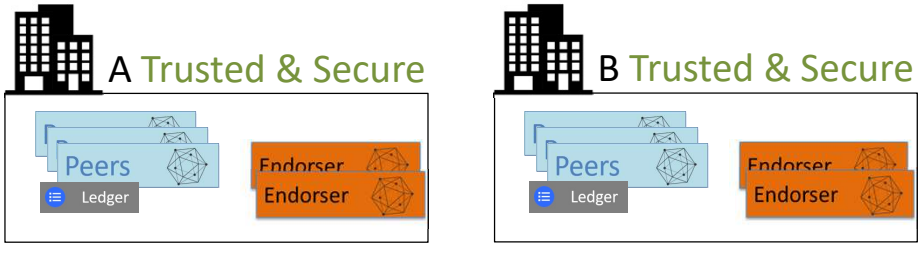
Clustering for high throughput, scalability & fault tolerance

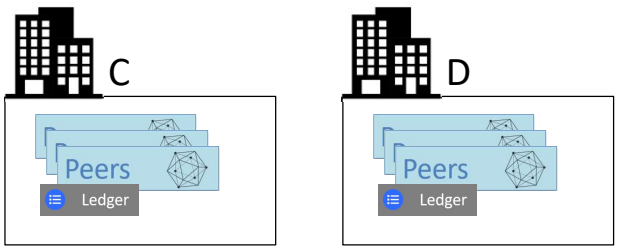
Supports multiple channels | Asynchronous

Client

- Client broadcasts the endorsed transaction using Orderer







Example:
For specific **ChaincodeID**:

All endorsements done by members **A** & **B** only

Summary

Orderer 

Communication
Order of transactions

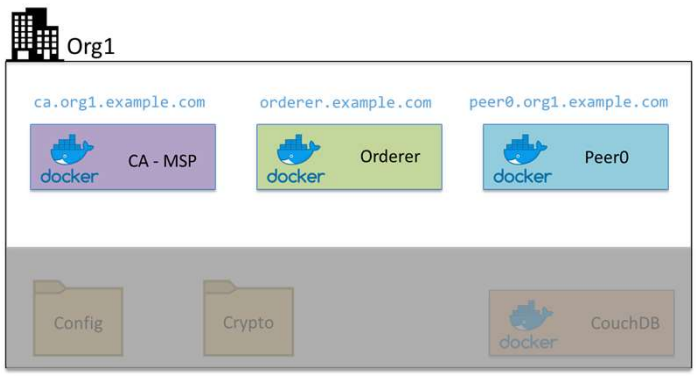
Consensus

- Implemented with Messaging System

SOLO

kafka

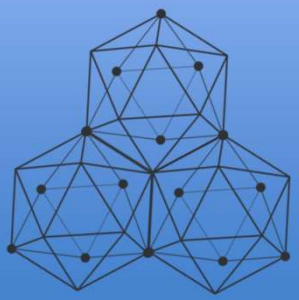
Dev Setup: Ledger



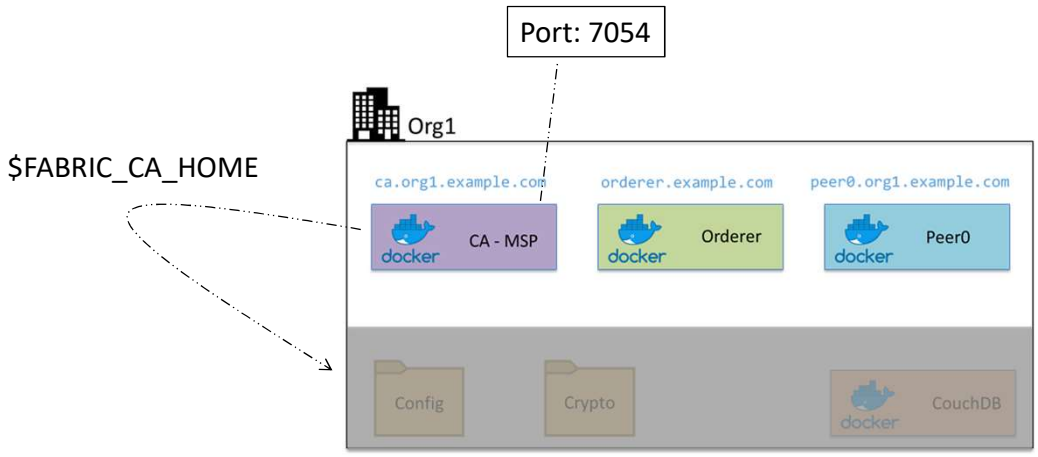
raj@acloudfan.com

@acloudfan

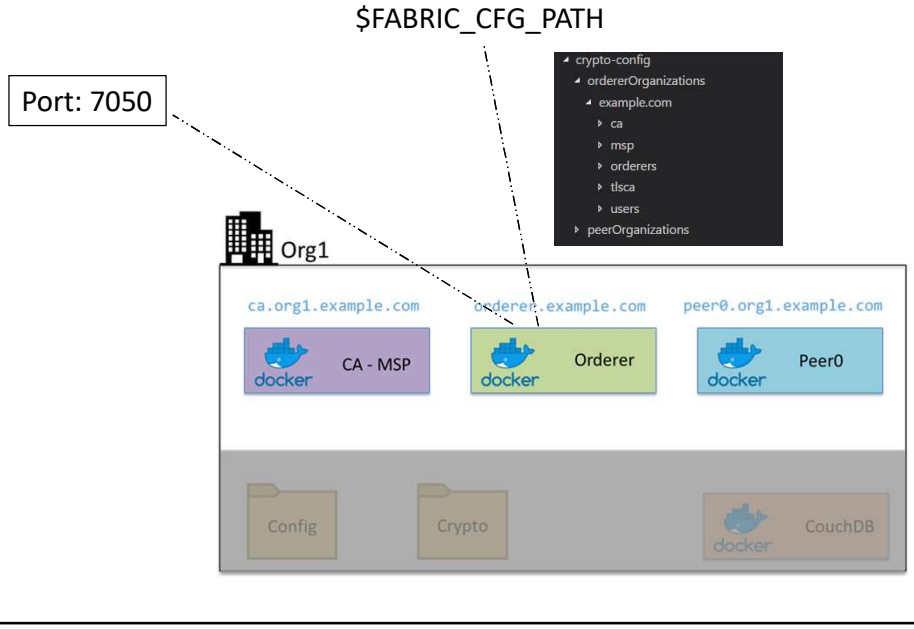
http://ACloudFan.com



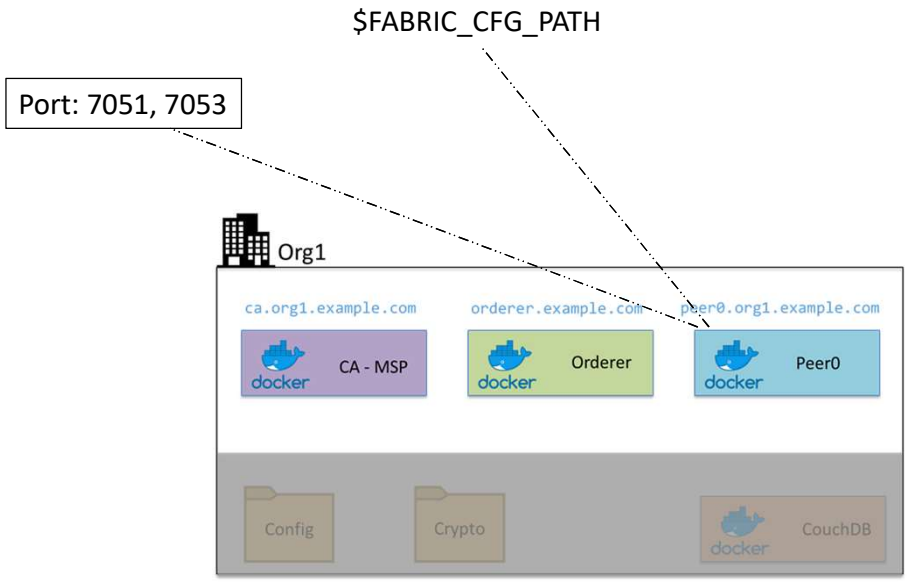
{Dev Setup}



{Dev Setup}



{Dev Setup}



MSP & CA

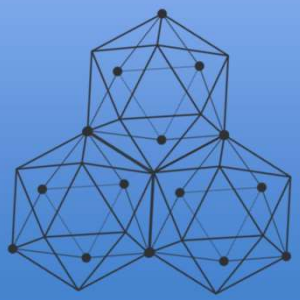
raj@acloudfan.com

@acloudfan

http://ACloudFan.com

Learning Objectives:

- Membership Services
- Certification authority



Public Key Infrastructure (PKI)

= Identity of an *Entity*

> PKI Refers to a set of Rules, Policies, Roles that governs the issuance & management of the certificates

Membership Service Provider (MSP)

> Abstract component of the system that provides credentials to clients, and peers for them to participate in a Hyperledger Fabric network

Alternate Implementation may be plugged in without impacting transaction flow

Membership Services

PKI based implementation of the MSP

Authenticate

Authorize

Is the user/peer's certificate valid?

Is the peer allowed to participate?

Can this user issue identities?

Can the user deploy chaincode?

Membership Services

PKI based implementation of the MSP

Identity Management

- Issuance
- Validation
- Revocation

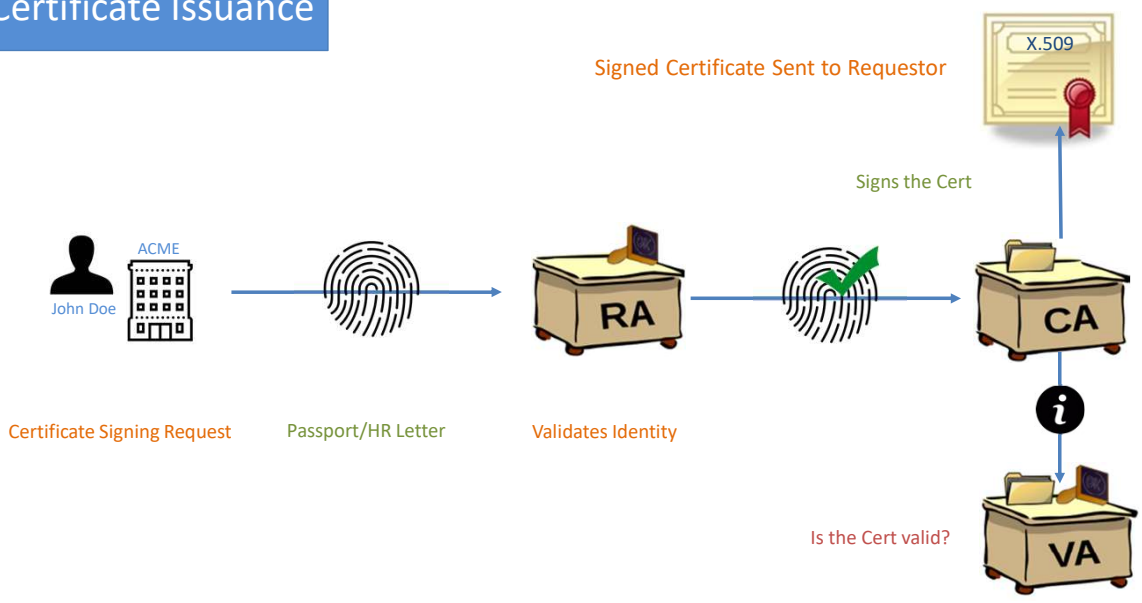
Certification Authority

A Trusted party that affirms the identity of an entity (a.k.a. certificate subject) by signing the certificate containing the entity's public key

Registration Authority

Validation Authority

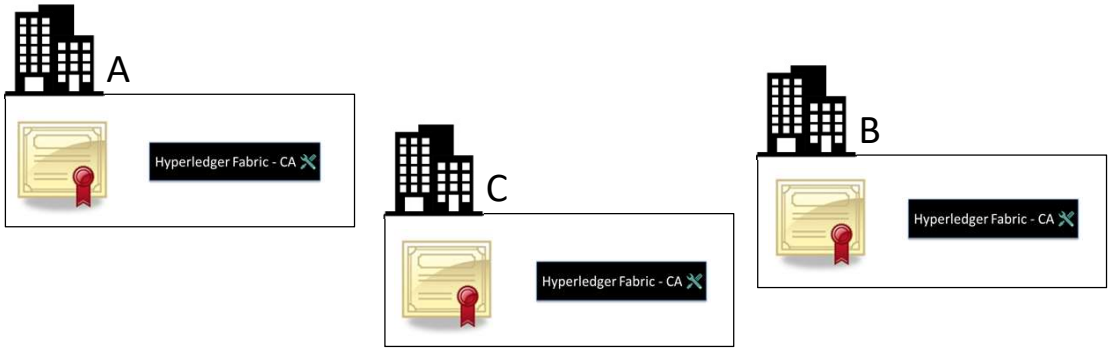
Certificate Issuance



RA = Registration Authority *CA = Certification Authority* *VA = Validation Authority*

Hyperledger Fabric - CA Certificate Issuance and management on Fabric

- Issues a Root Certificate to each member
- Members manage identities within their organizations



Concepts & Deep Dive

raj@acloudfan.com

@acloudfan

http://ACloudFan.com

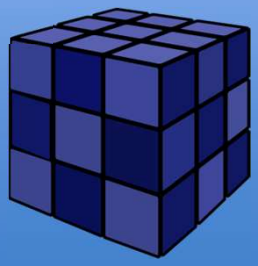
Discount Coupon Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

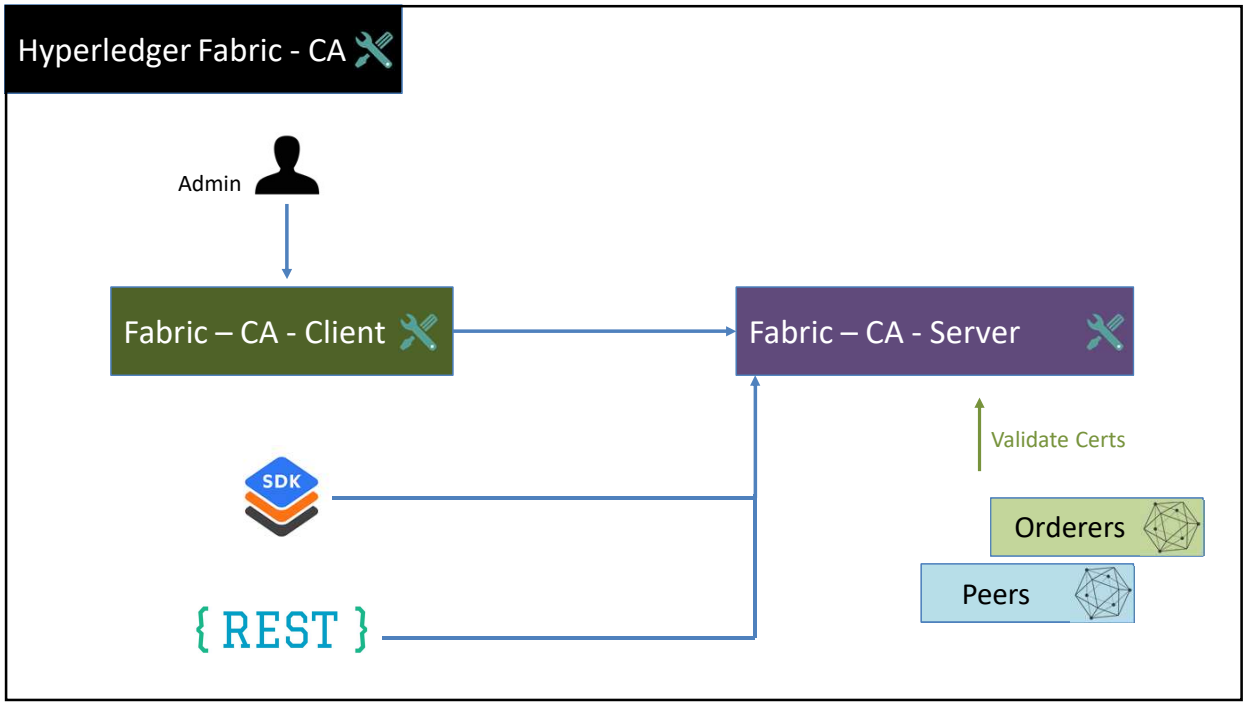
https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

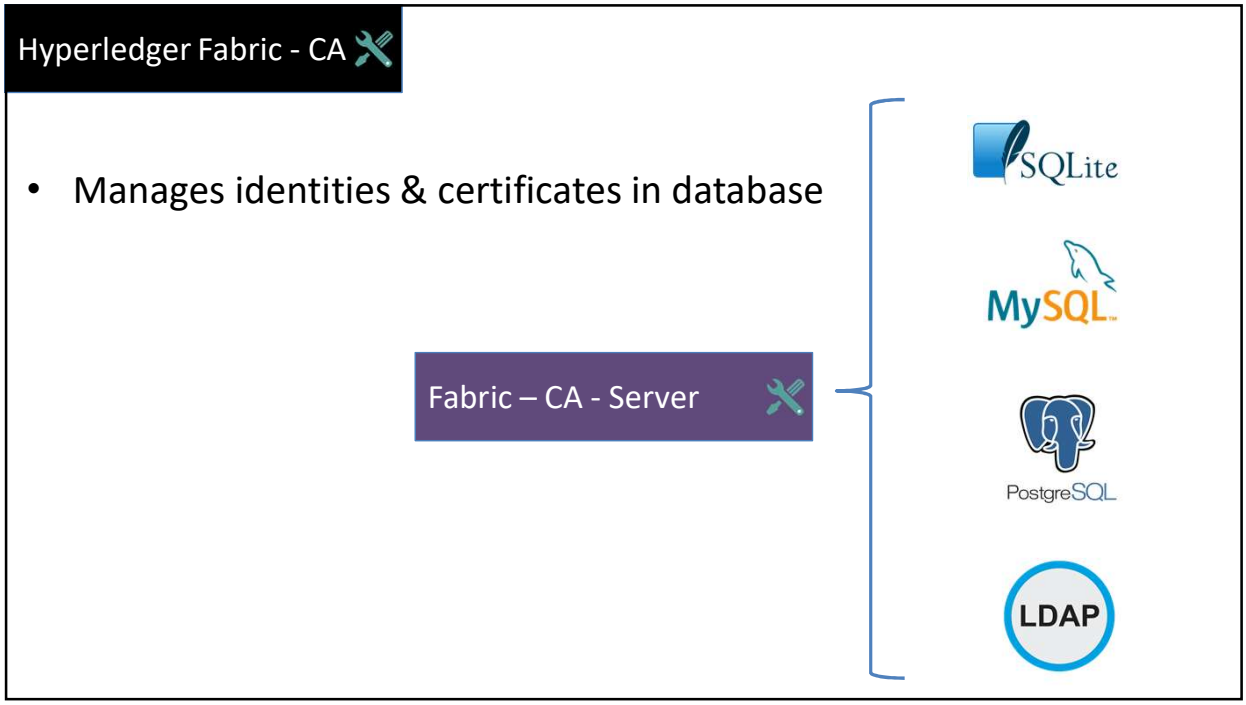
https://www.udemy.com/rest-api/?couponCode=DKRST1099

mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com



This deck is part of a online course on "Hyperledger Fabric Development with Composer"


Hyperledger Fabric - CA
Admin
Fabric – CA - Client
Fabric – CA - Server
Validate Certs
SDK
Orderers
Peers
{ REST }


Hyperledger Fabric - CA
• Manages identities & certificates in database
Fabric – CA - Server
SQLite
MySQL
PostgreSQL
LDAP

Dev Environment Topology

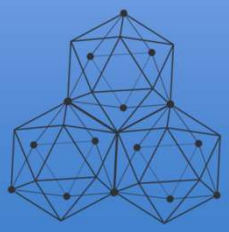
raj@acloudfan.com

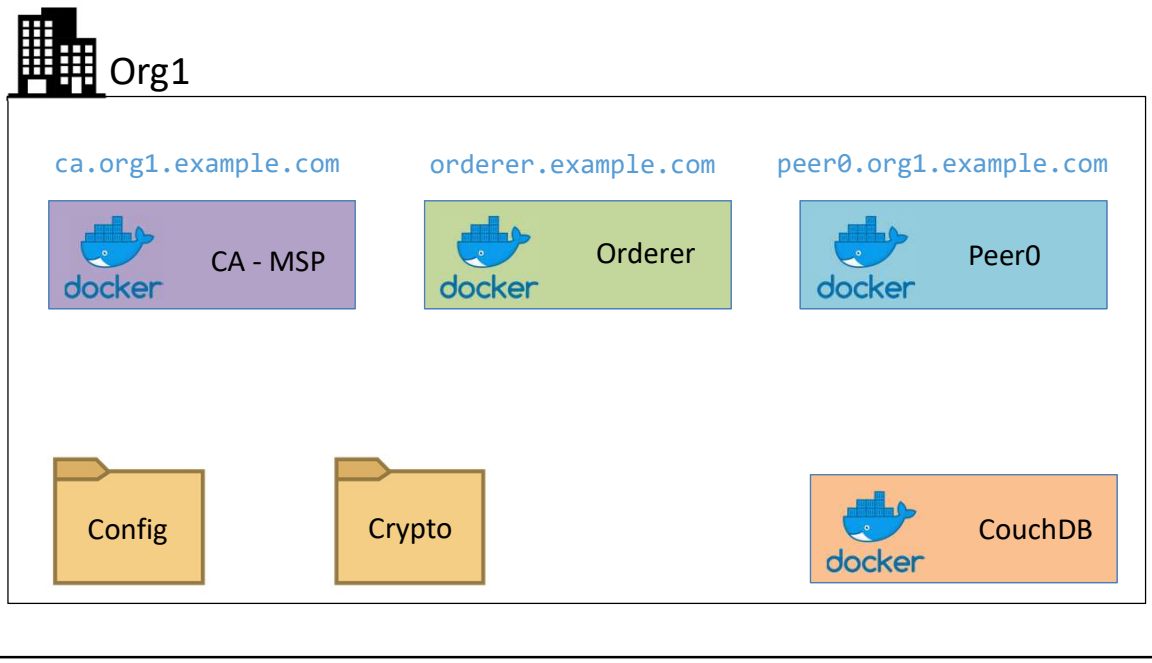
@acloudfan

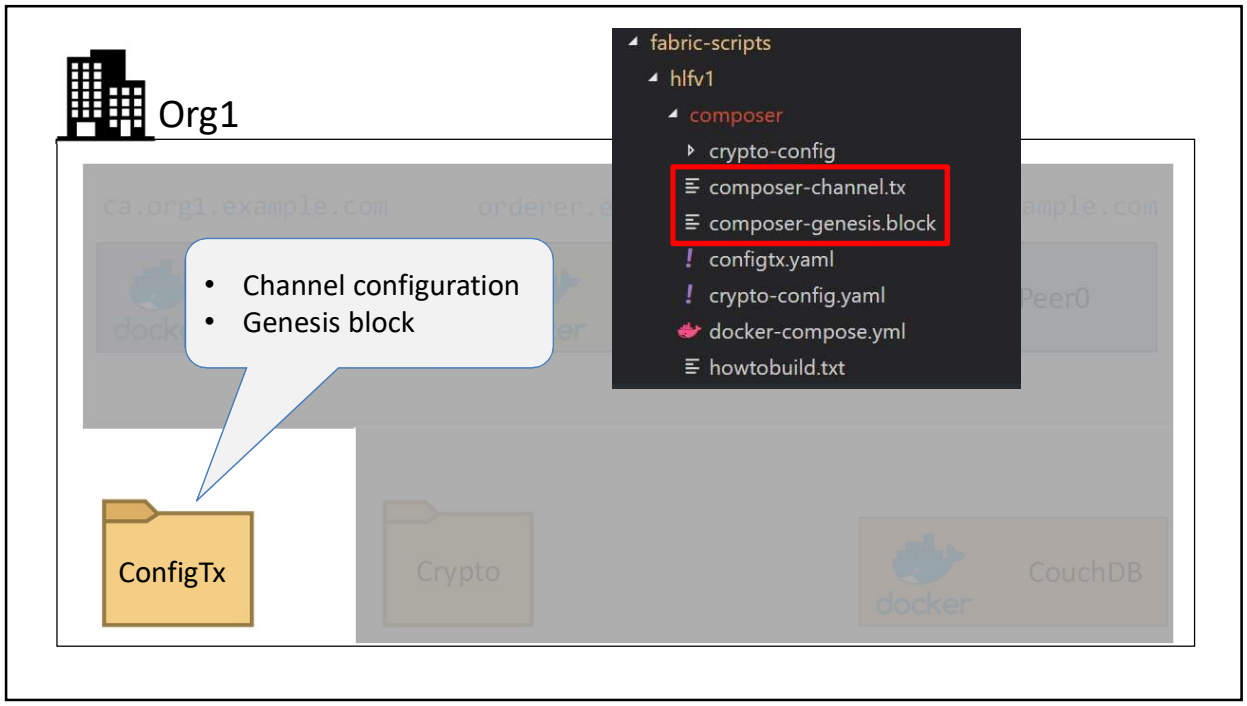
http://ACloudFan.com

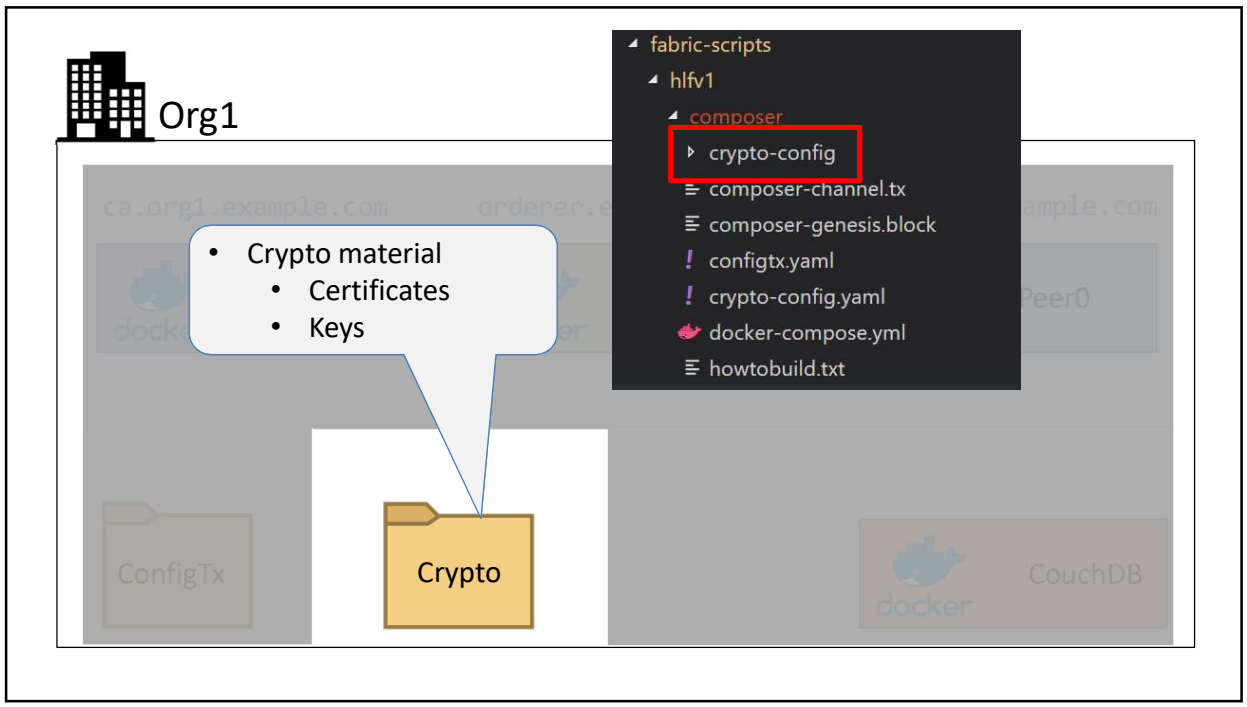
Learning Objectives:

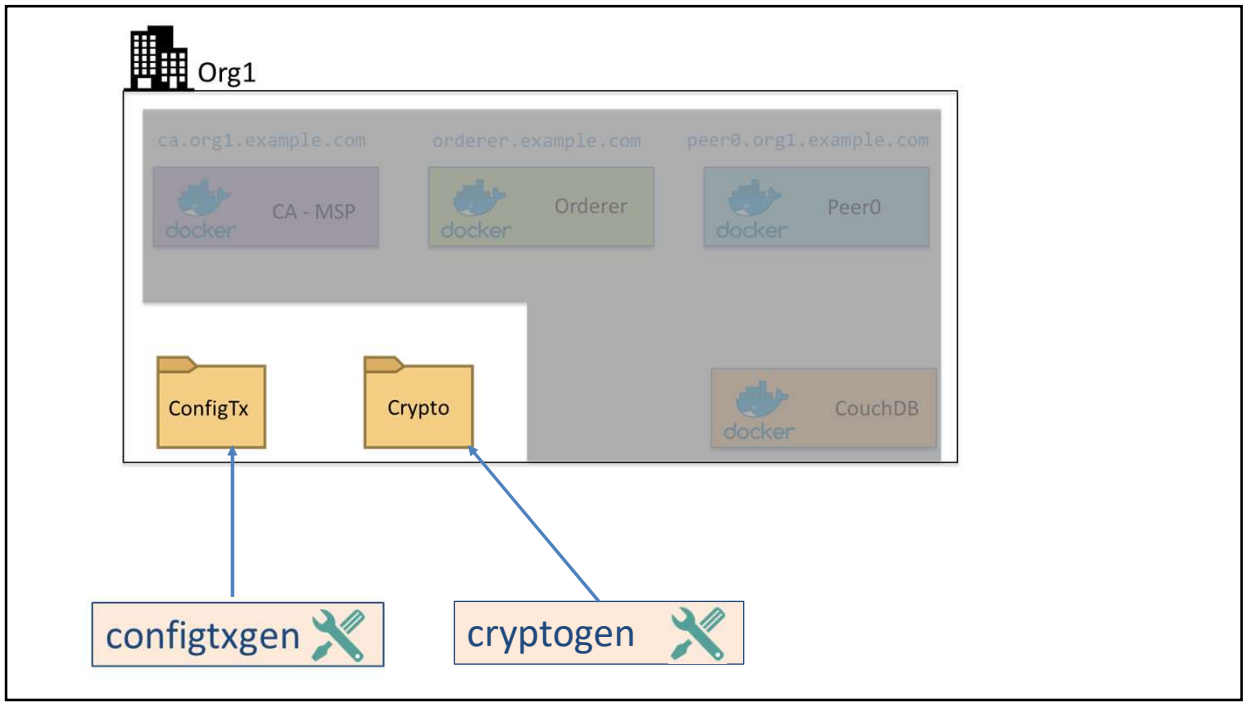
- Overview of the setup






Org1
fabric-scripts
hlfv1
composer
crypto-config
composer-channel.tx
composer-genesis.block
configtx.yaml
crypto-config.yaml
docker-compose.yml
howtobuild.txt
Channel configuration
Genesis block
ConfigTx
Crypto
CouchDB


Org1
fabric-scripts
hlfv1
composer
crypto-config
composer-channel.tx
composer-genesis.block
configtx.yaml
crypto-config.yaml
docker-compose.yml
howtobuild.txt
Crypto material
Certificates
Keys
ConfigTx
Crypto
CouchDB



What is Hyperledger?

Discount Coupon Links to UDEMY courses:

https://www.udemy.com/hyperledger/?couponCode=DKHLF1099

https://www.udemy.com/ethereum-dapp/?couponCode=DKETH1099

https://www.udemy.com/rest-api/?couponCode=DKRST1099

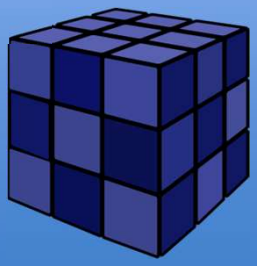
mentoring, seeking Blockchain part time work, project guidance, advice … …
http://www.bcmentors.com

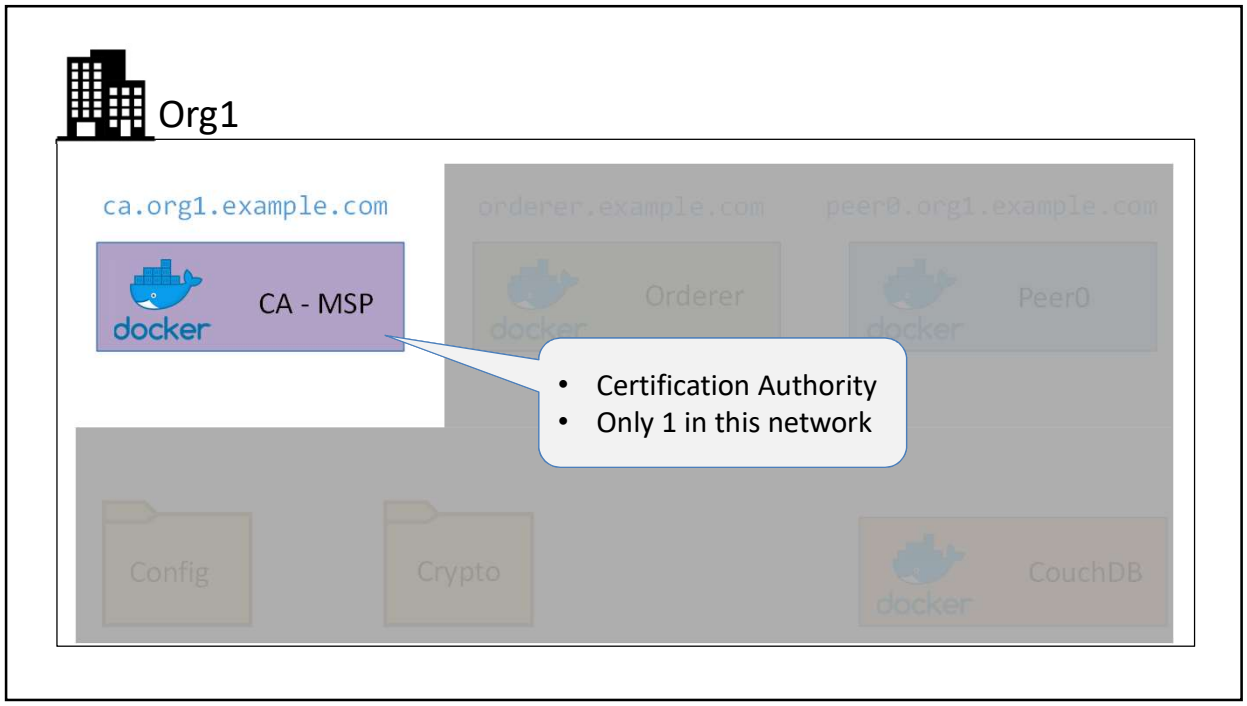
This deck is part of a online course on "Hyperledger Fabric Development with Composer"

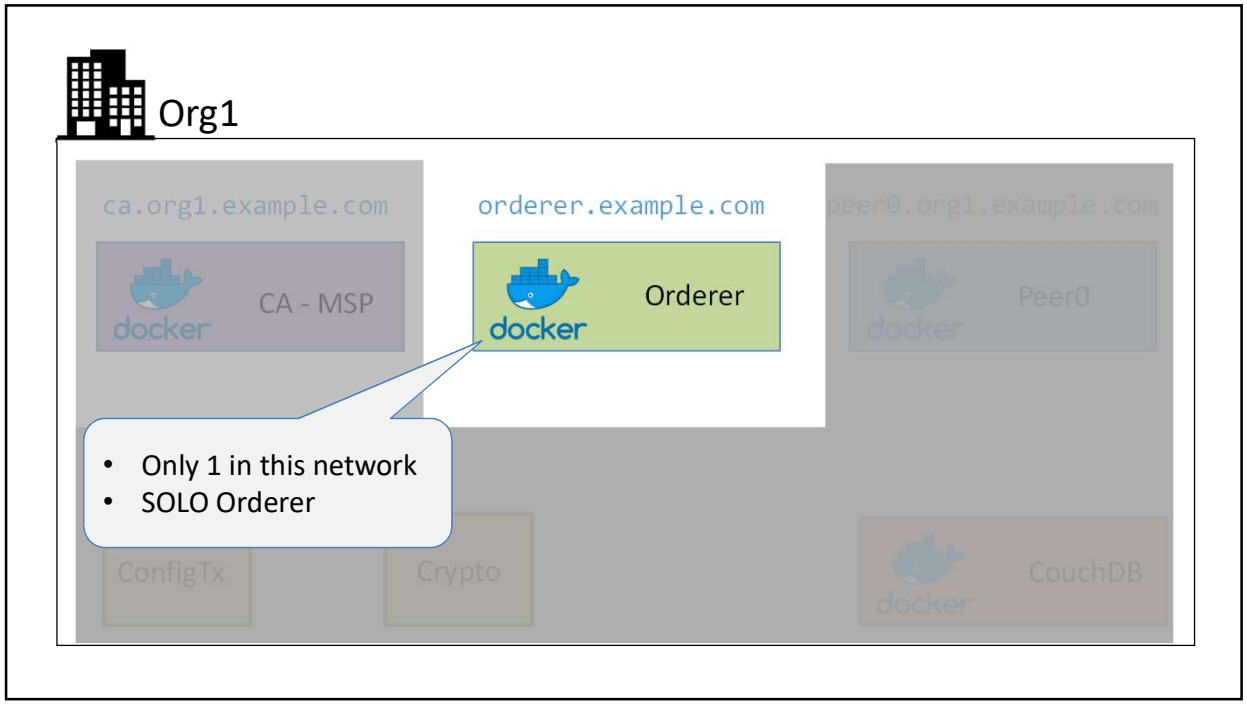
raj@acloudfan.com

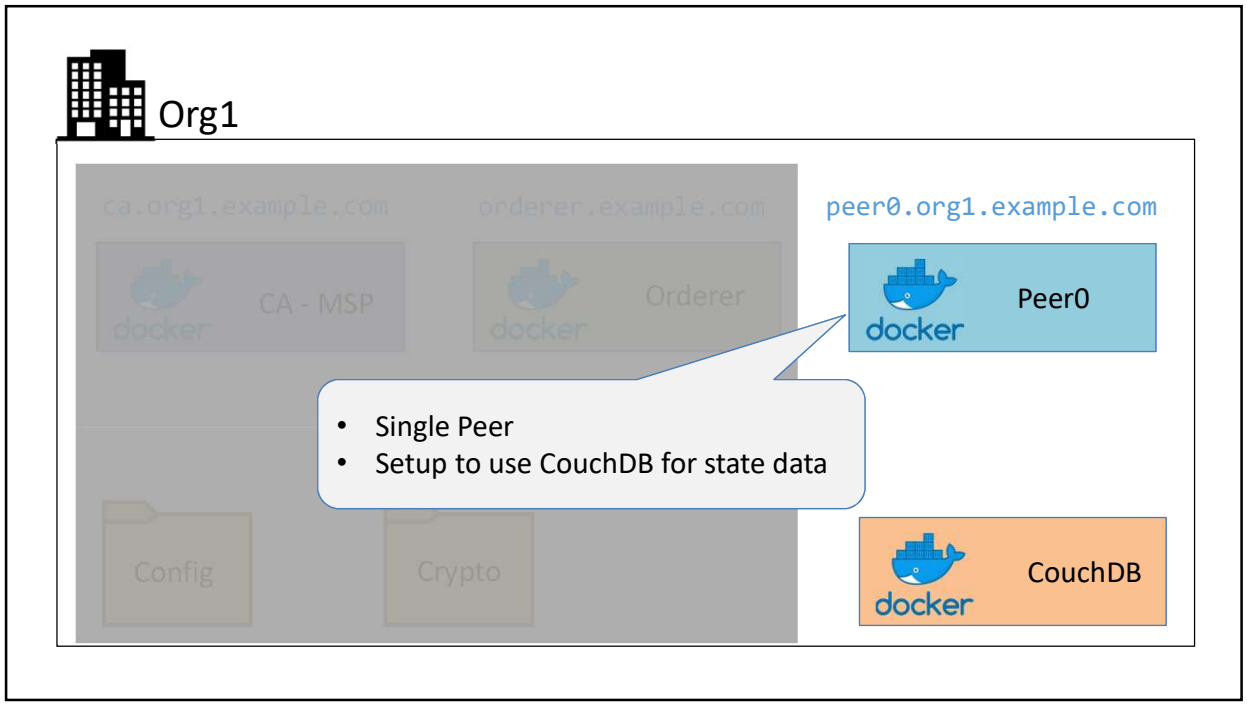
@acloudfan

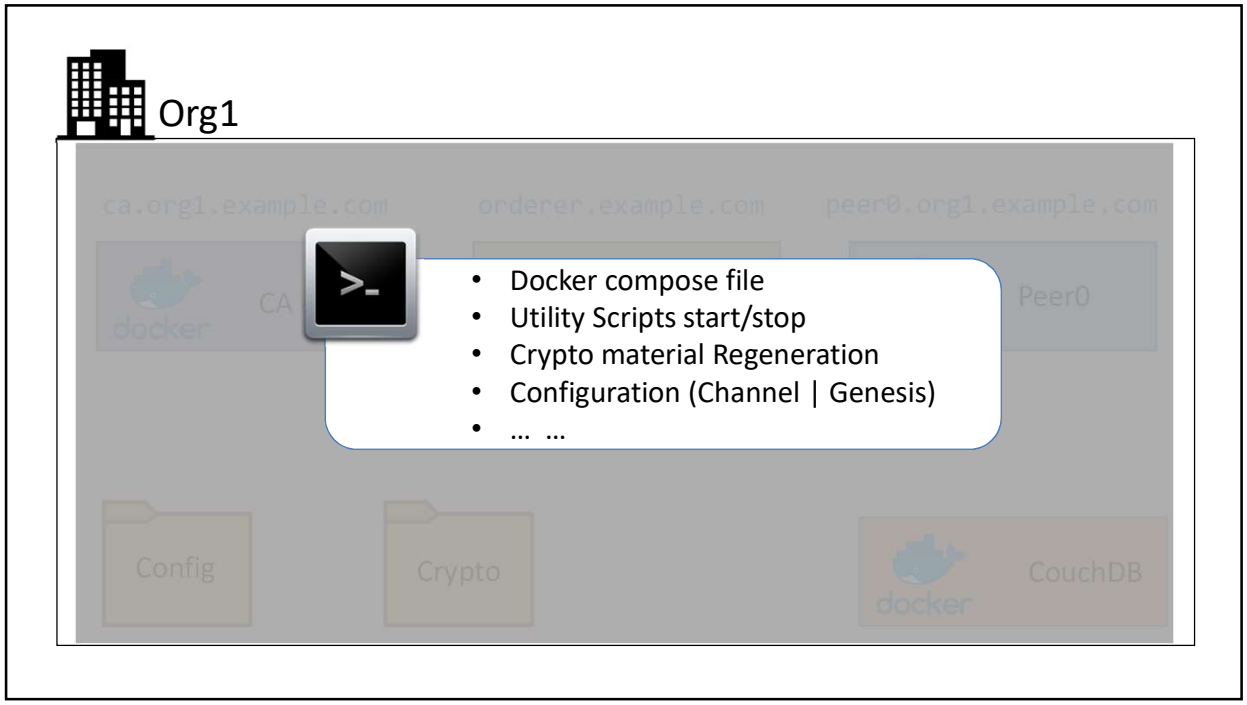
http://ACloudFan.com




Org1
ca.org1.example.com
CA - MSP
orderer.example.com
Orderer
peer0.org1.example.com
Peer0
Config
Crypto
CouchDB
• Certification Authority
• Only 1 in this network


Org1
ca.org1.example.com
CA - MSP
orderer.example.com
Orderer
peer0.org1.example.com
Peer0
ConfigTx
Crypto
CouchDB
• Only 1 in this network
• SOLO Orderer


Org1
ca.org1.example.com
orderer.example.com
peer0.org1.example.com
CA - MSP
Orderer
Peer0
docker
Single Peer
Setup to use CouchDB for state data
Config
Crypto
CouchDB

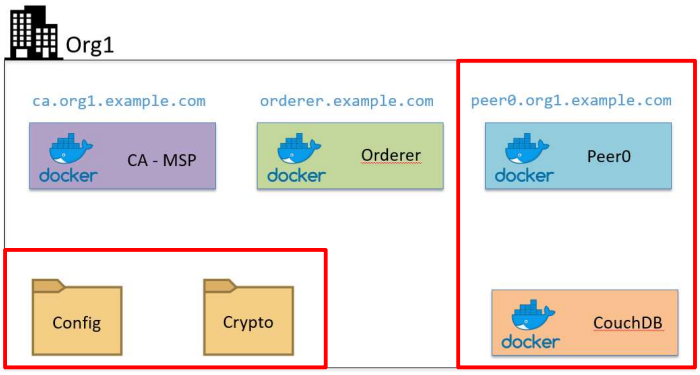

Org1
ca.org1.example.com
orderer.example.com
peer0.org1.example.com
CA
Peer0
Docker compose file
Utility Scripts start/stop
Crypto material Regeneration
Configuration (Channel | Genesis)
… …
Config
Crypto
CouchDB

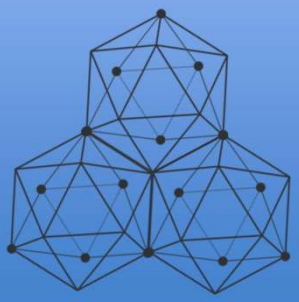
Walkthrough : Dev Setup

raj@acloudfan.com

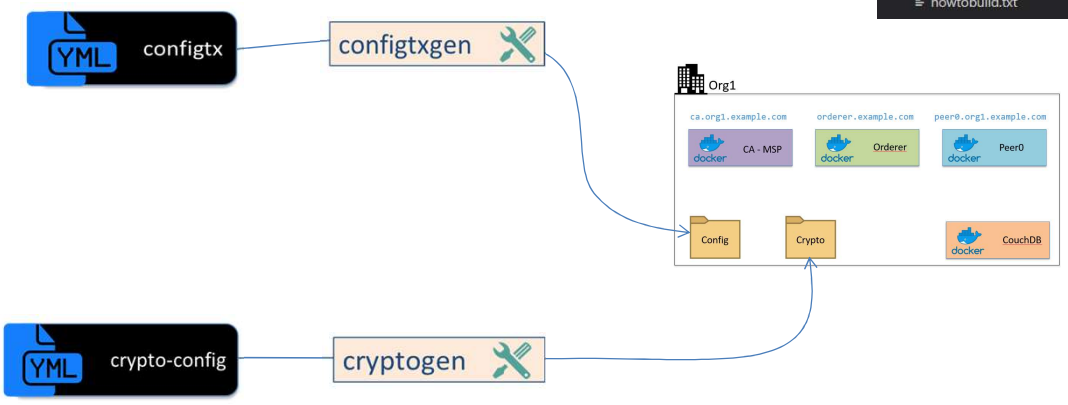
@acloudfan

http://ACloudFan.com

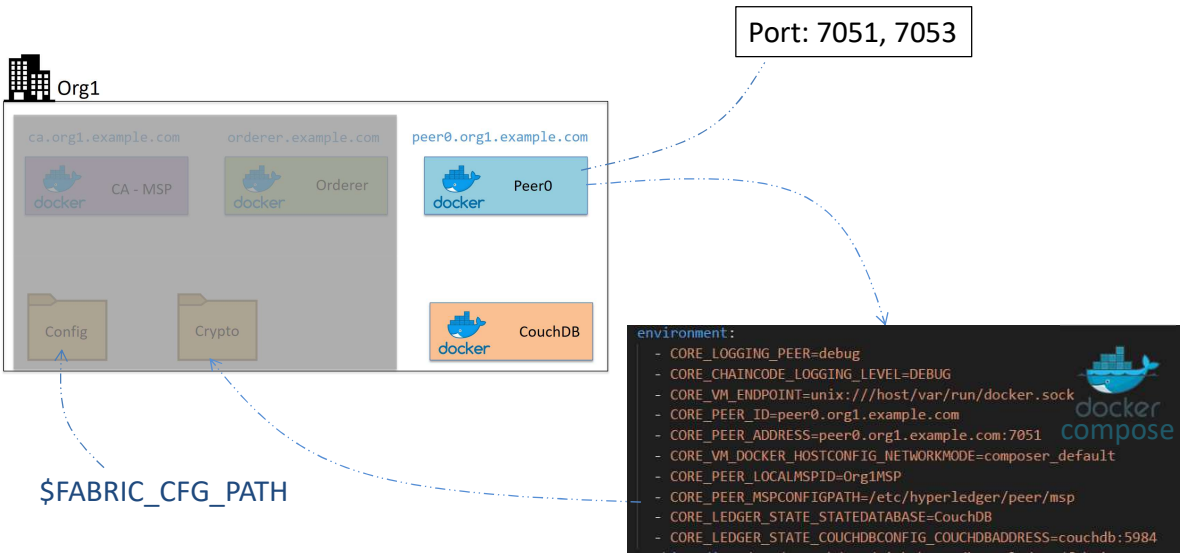




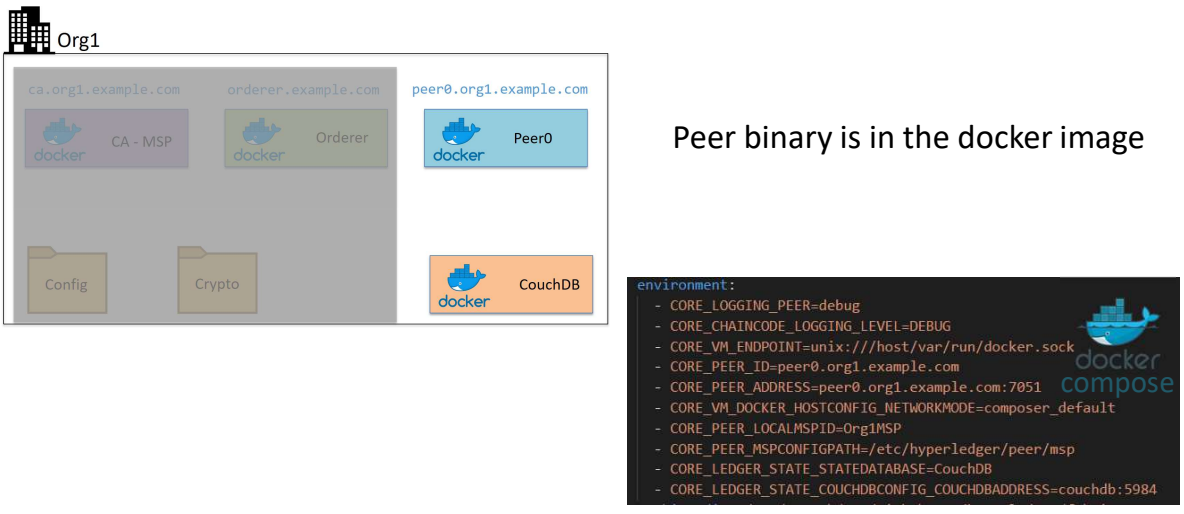
- Setup configured by way of 2 YAML files



{Dev Setup}



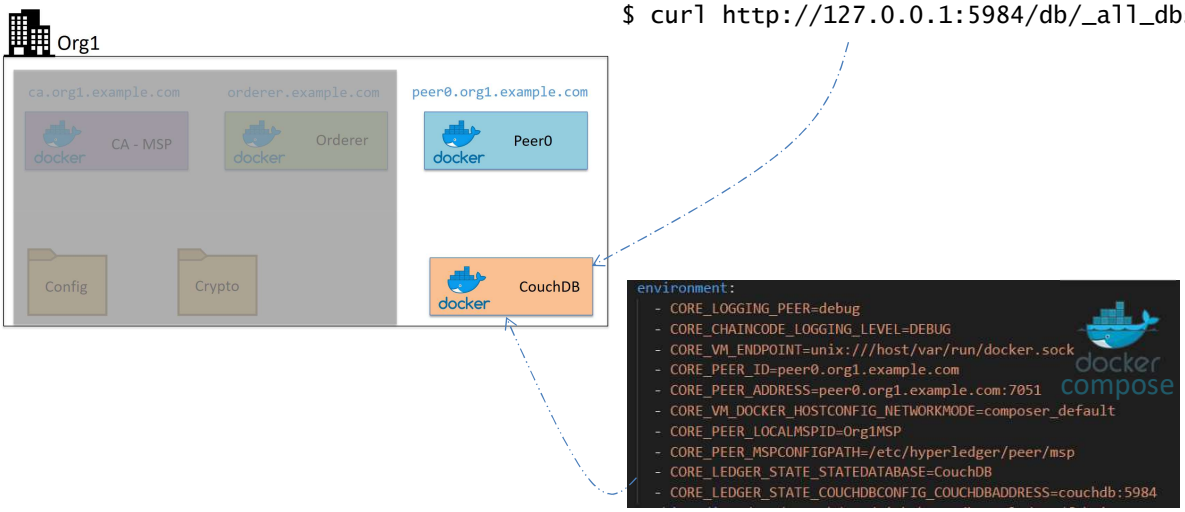
{Dev Setup}



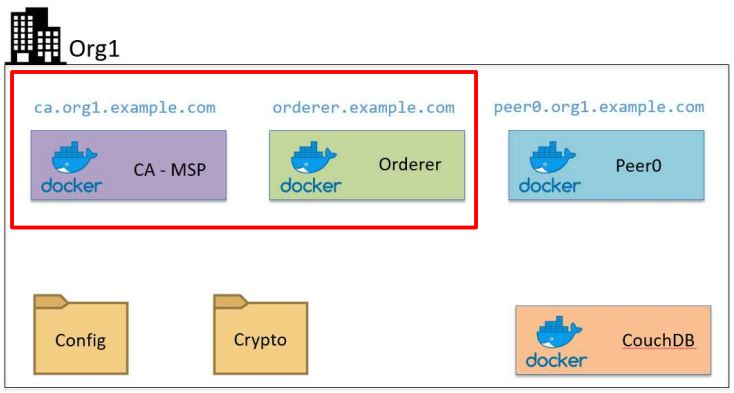
Peer binary is in the docker image

{Dev Setup}

```
$ curl http://127.0.0.1:5984
$ curl http://127.0.0.1:5984/db/_all_dbs
```



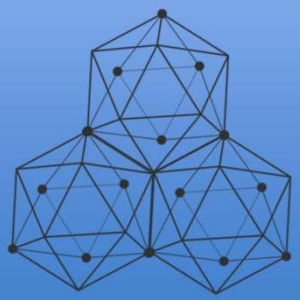
Walkthrough : Dev Setup



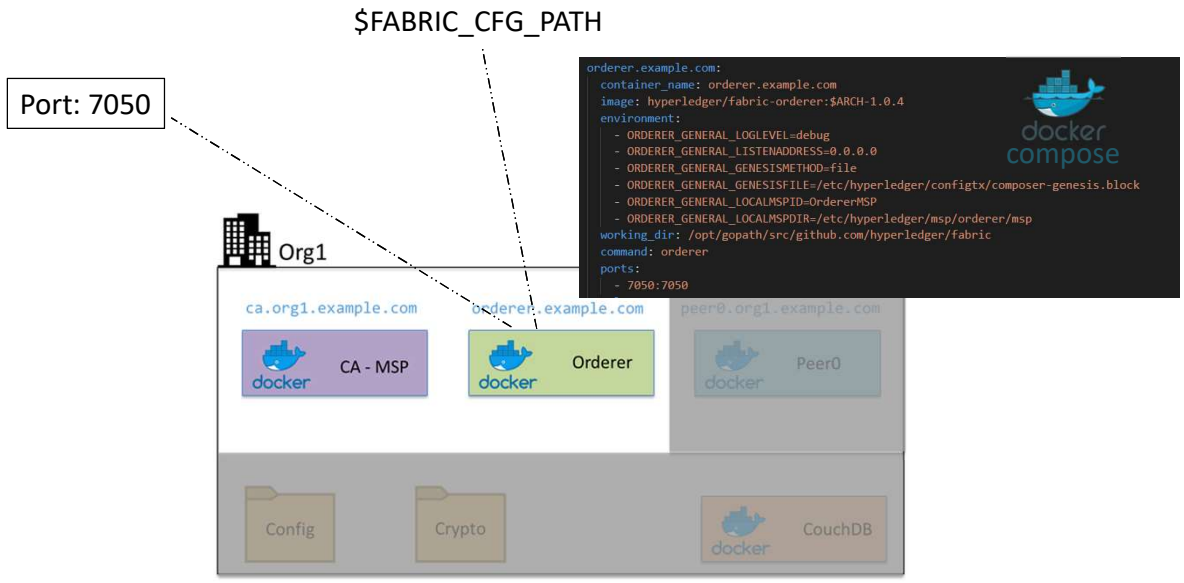
raj@acloudfan.com

@acloudfan

http://ACloudFan.com



{Dev Setup}



{Dev Setup}

fabric-ca-client tool used for managing certificates