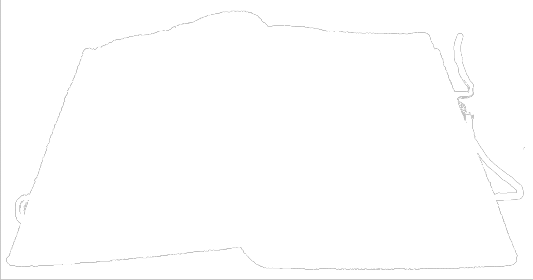
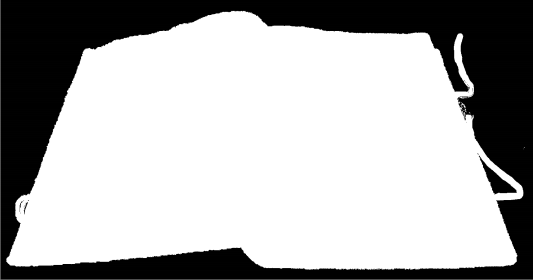
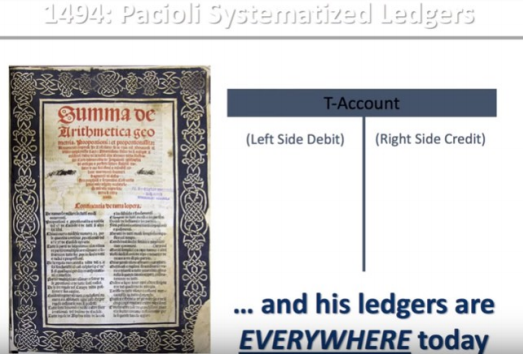
Hyperledger Day -1

31/10/20 3

31/10/20 4

Hash

Blockchain's Birth

Public

Blockchain

● Anyone can read without explicit authorisation

● Anyone can write without explicit permission ● More complex rules for better security ● Complex consensus algorithm

● Computationally expensive to mine & add a Block

● No one owns it

● Computational power is distributed globally ● Example: Bitcoin Blockchain, Ethereum Blockchain etc

8

Private

Blockchain

● Only authorised nodes can read the transaction data ● Only authorised nodes can write the transaction into Blockchain ● Private hence security can be implemented in a straightforward way

● One authorised node can be the arbitrator for any dispute ● Easy or computationally less expensive to add a Block ● One or more private entities own the Blockchain

● Many things can be replaced by legal contract giving more control to the one party

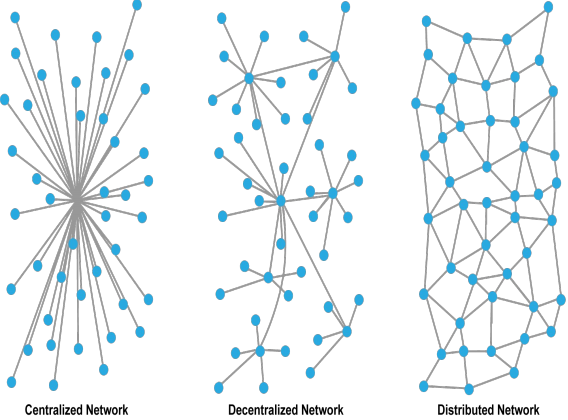
● Examples: Privately installed Ethereum Blockchain, ICICI Bank’s Blockchain etc

9

Why is it called a P2P network? 1

Decentralized 

Network

2

Steps to create your Blockchain Solution?

●**Identify a Suitable Use-case -** Identify a use-case that makes business sense. ●**Identify the Most Suitable Consensus Mechanism -** Depending upon your use case, you need to choose the consensus mechanism that makes the most sense.

●**Identify the Most Suitable Platform -** Depending upon the consensus mechanism you chose the suitable platform

12

What are Smart Contracts?

A *smart contract* is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a *contract*. Smart*contracts* allow the performance of credible transactions without third parties. One of the best things about the blockchain is that, because it is a decentralized system that exists between all permitted parties, there’s no need to pay intermediaries (Middlemen) and it saves you time and conflict.  Blockchains have their problems, but they are rated, undeniably, faster, cheaper, and more secure than traditional systems, which is why banks and governments are turning to them

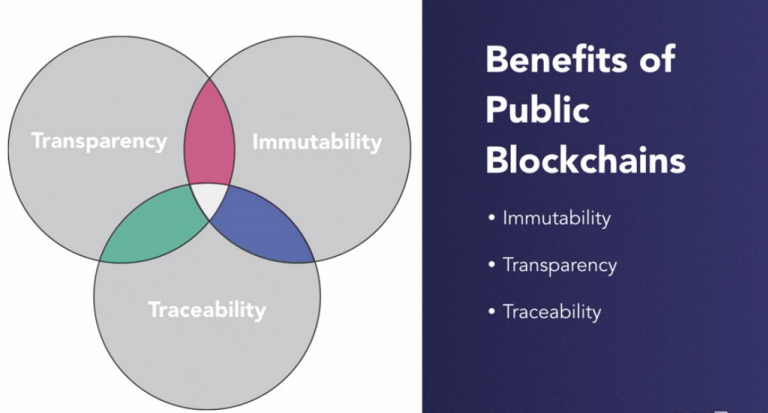
1

What are Smart Contracts?

A *smart contract* is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a *contract*. Smart*contracts* allow the performance of credible transactions without third parties. One of the best things about the blockchain is that, because it is a decentralized system that exists between all permitted parties, there’s no need to pay intermediaries (Middlemen) and it saves you time and conflict.  Blockchains have their problems, but they are rated, undeniably, faster, cheaper, and more secure than traditional systems, which is why banks and governments are turning to them

1

Public Vs Private Ledgers



Public Vs Private Ledgers



Hyperledger

Hyperledger

Participants in Hyper Ledger

Important Elements

Channel

Peers

● Organisations will host at least one peer to a channel and they maintain the copy of log which is called ledger of the channel.

● 3 Diffrent Types of Peers

● Commiting

● Endorsing

● Ordering

● Extra 2 Peers are – anchor peers and leader peers

Consensus Mechanism

Process of coming to an agreement by all parties in Network.

Steps are,

1) Trasaction Endorsment , Security Check and Policy Agreement

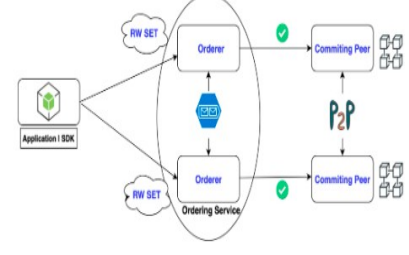
2) Ordering Transactions in to blocks ready to commit by peers

3) Validate the endorsement

HF allows users from organisations to define policies around the lifecycle of chaincode.

Transaction Flow

Transactions rolled our from Client Applications such as Nodejs or from CLI to endorsing peers.



MSP – Membership Service Provider

● Defines the Rules

● Manages trusted identities to authenticate the client.

● MSP depends on CA which is Pluggable Interface

Installation

Requirements

4GB of RAM (more is preferred)

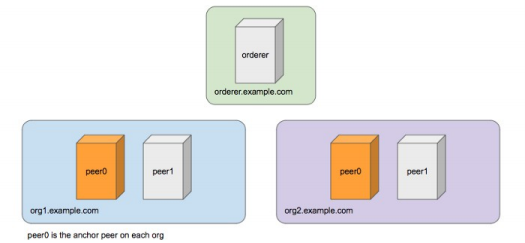
Docker, Docker-Compose, Code editor (e.g. Visual Studio Code), Git

NodeJS version 8.9+ (Preferred is 8.9.4 – change your version with a version manager like ‘n’) / Latest

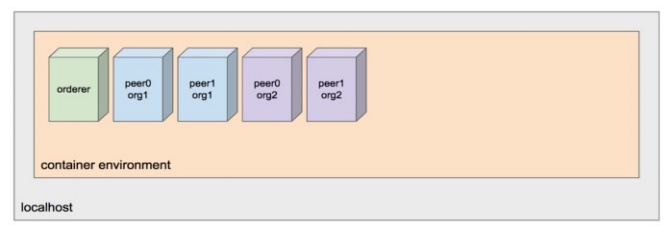
Basic JavaScript knowledge

Hyperledger First Network

● Hyperledger Fabric comes with a lot of examples, and among them, the First Network is always the one we begin with (Building Your First Network)



First Network Deployed



Fabric Samples, Tools and Docker Images

$ curl -sSL http://bit.ly/2ysbOFE | bash -s 1.2.0

● clone the fabric samples (kept in fabric-samples)

● download the binary tools in Hyperledger Fabric (stored inside fabric-sample/bin)

● download the docker images of Hyperledger Fabric

Begin with Predefined Script: ./byfn.sh

● generate: generate the required certificates and genesis block (channel artifacts)

● up: bring up First Network, and execute the First Network chain code

● down: tear down First Network

./byfn.sh generate

Run ./byfn.sh generate to create the required components

● Generating certificates using cryptogen tool ● Generating Orderer Genesis block

● Generating channel configuration transaction 'channel.tx'

● Generating anchor peer update for Org1MSP and Org2MSP

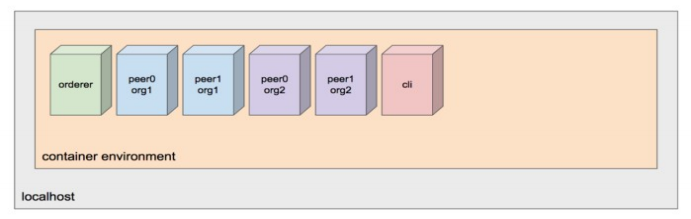
$ docker ps

take a look on containers running in the local host. We should see nothing here

$ docker ps

take a look on containers running in the local host. We should see nothing here

Infrastructure Setup



All you Need to Know as of..

Anchor Peer

This gets used for communications between organisations. It makes peers in different organisations aware of each other.

Blocks

Consist of a header, block data (transactions) and block metadata (information about nodes involved with creating the block).

Certificate Authorities

Everyone who wants to interact with the networks needs an identity. The CA provides the means for each actor to have a verifiable digital identity. Hyperledger Fabric has a built in CA component for use in the blockchain network.

Chaincode

The Hyperledger Fabric term for a smart contract. Note that chaincode does not have to be installed on every peer in a channel.

Channel

A channel allows a group of participants to create a separate ledger of transactions. The transactions are only visible to the members of the channel.

Channel Configuration

Rules that govern the channel, the channel is governed by the channel members. The channel configuration is separate from the network configuration.

Consortium

A group of organisations that share a need to transact.

Committing Peer

Every peer in the channel.

Endorsing Peer

Every peer that has the smart contract installed can be an endorsing peer. Endorsement Policy

The rules for which organisations much approve a transaction before the other organisations will accept a copy. This is specific to the chaincode.

Leader Peer

An organization can have multiple peers in a channel. Only one peer from the organization needs to receive the transactions. The leader distributes transactions from the orderer.

Membership Service Provider

Is a trusted authority.

The MSP identifies which Root Certificate Authorities (CA) and Intermediate CA’s are trusted by the network. The MSP identifies what roles different actors in an organization can play in the network.

Nodes join the network through a Membership Service Provider. Ledger

This is an append only file while can be used to recreate the world state. Ordering Nodes

Is like a network administration point. The ordering nodes support the application channels for ordering transactions into blocks.

Peer Nodes

Each peer maintains a copy of the ledger for each channel it is a member of. Policies

These determine who has control over the network configuration.

Private Data Collection

This is used for keeping the data in a transaction confidential. The data is stored in a private database that is separated from the channel ledger.

Public Key Infrastructure

This provides secure communication in a network. CAs issue digital certificates that get used to authenticate messages in the network. The PKI provides a list of identities and the MSP says which of them are part of an organization.

System Chaincode

Is code that defines operating parameters for the entire channel.

Lifecycle and configuration system chaincode defines the rules for the channel. Endorsement and validation system chaincode defines the requirements for endorsing and validating transactions.

World State

Is a snapshot of the current state of the objects in the network, this is usually a graph database in practise.