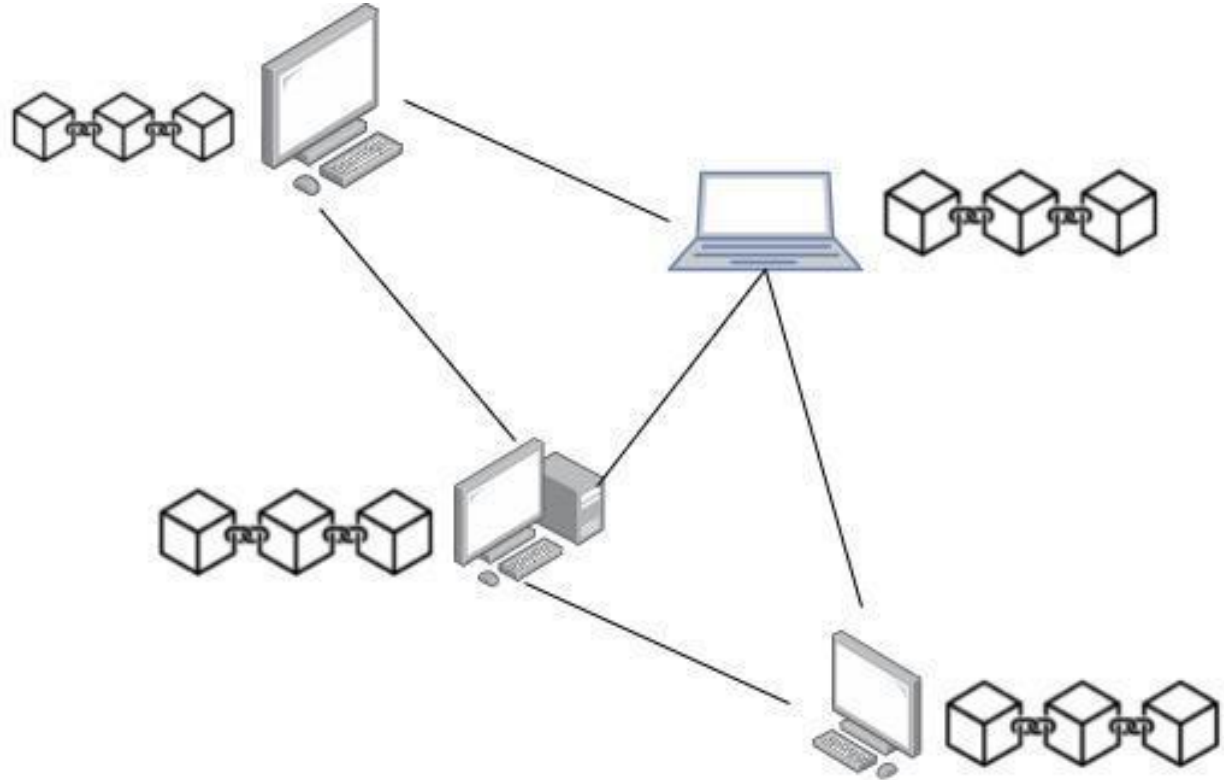


Agenda

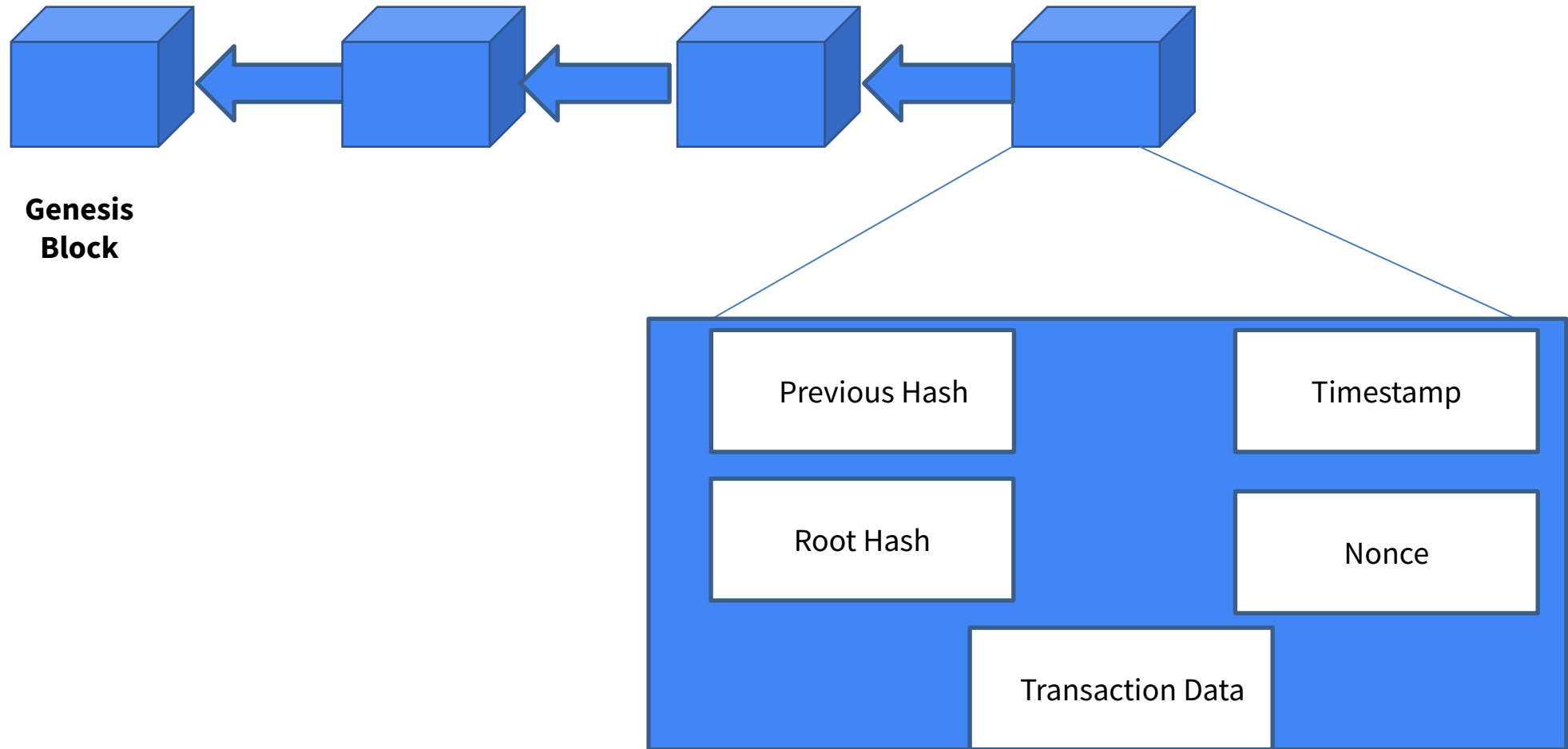
- Blockchain Overview
- Public Blockchain Vs Private Blockchain
- Features of Private Blockchain
- Hyperledger Foundation
- Hyperledger Umbrella projects
 - Hyperledger Fabric

What is a Blockchain?

Blockchain technology is a **Distributed Ledger Technology**.



Blockchain



BITCOIN



The Bitcoin Whitepaper

- The idea was published in 2009 by an pseudonymous person/group of people, named **Satoshi Nakamoto**.

Goal with Bitcoin was:

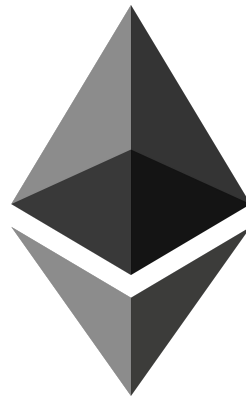
- To create a **trustless** system, using cryptography
- Solve double-spending problem of previous digital currencies
- Create digital assets that can be owned, with proof of ownership

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

OTHER PUBLIC BLOCKCHAINS



Public Blockchain	Private Blockchain
It is open and anyone will be able to access it.	Restrictions and permission mechanisms will be in place. Anyone who wants to join the network needs to get authorized
Each node will have equal privileges for a transaction and data	Only limited nodes or certain types of nodes can perform a transaction
Transaction-per-second (tps) is low	Will have very high Tps
Transaction cost is high	Transaction cost is comparatively very low
Uses consensus protocols like proof-of-work, proof-of-stake.	Uses consensus algorithms like pBFT, PoET, Raft etc..
Requires no trust among members inside the network	Members inside the network need to trust each other.
Energy Consumption is very high	Energy consumption is too low.



DIGITAL IDENTITY

A SELF SOVEREIGN ID CAN BE USED TO VERIFY IDENTITY WITHOUT NEEDING AN INDIVIDUAL TO PRODUCE NUMEROUS DOCUMENTS



SUPPLY CHAIN MANAGEMENT

BLOCKCHAINS ALLOW MULTIPLE PARTIES TO ACCESS A DATABASE TO ACT AS THE SINGLE SOURCE OF TRUTH. RECORDED TRANSACTIONS ARE IMMUTABLE, ARE APPEND ONLY AND PROVIDE A TIME STAMPED AUDIT TRAIL .



HEALTHCARE

USING BLOCKCHAIN TECHNOLOGY TO RECORD PATIENT INFORMATION ON A DISTRIBUTED LEDGER CAN ALLOW DIFFERENT STAKEHOLDERS CONDITIONAL ACCESS TO A SINGLE SOURCE OF TRUTH



REAL ESTATE

BLOCKCHAIN ALLOWS PEOPLE TO TRANSFER FUNDS, PROPERTY TITLES AND DATA IN A MORE PEER-TO-PEER MANNER THAT IS DIGITAL AND OPEN SOURCE

Features of Private Blockchain

- Enhanced Scalability
- Ability to Prevent Unauthorized Access
- Cost-Efficiency
- Enterprise Customizability

What is Hyperledger Foundation ?

- An open source initiative led by the **Linux Foundation**
- Cross-industry collaborative effort to support blockchain-based distributed ledgers



Hyperledger Projects



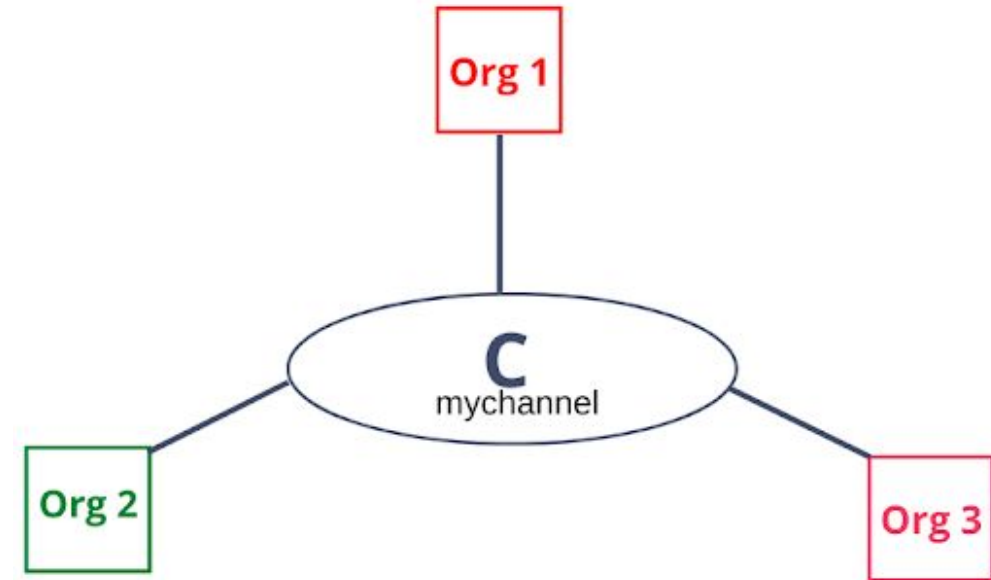


Salient Features of Hyperledger Fabric

- Permissioned blockchain network
- Smart contract can be written in standard programming languages(Go, NodeJS, Java)
- No cryptocurrency and No mining
- Pluggable Architecture
- Privacy and confidentiality of transactions - Channels and PDC

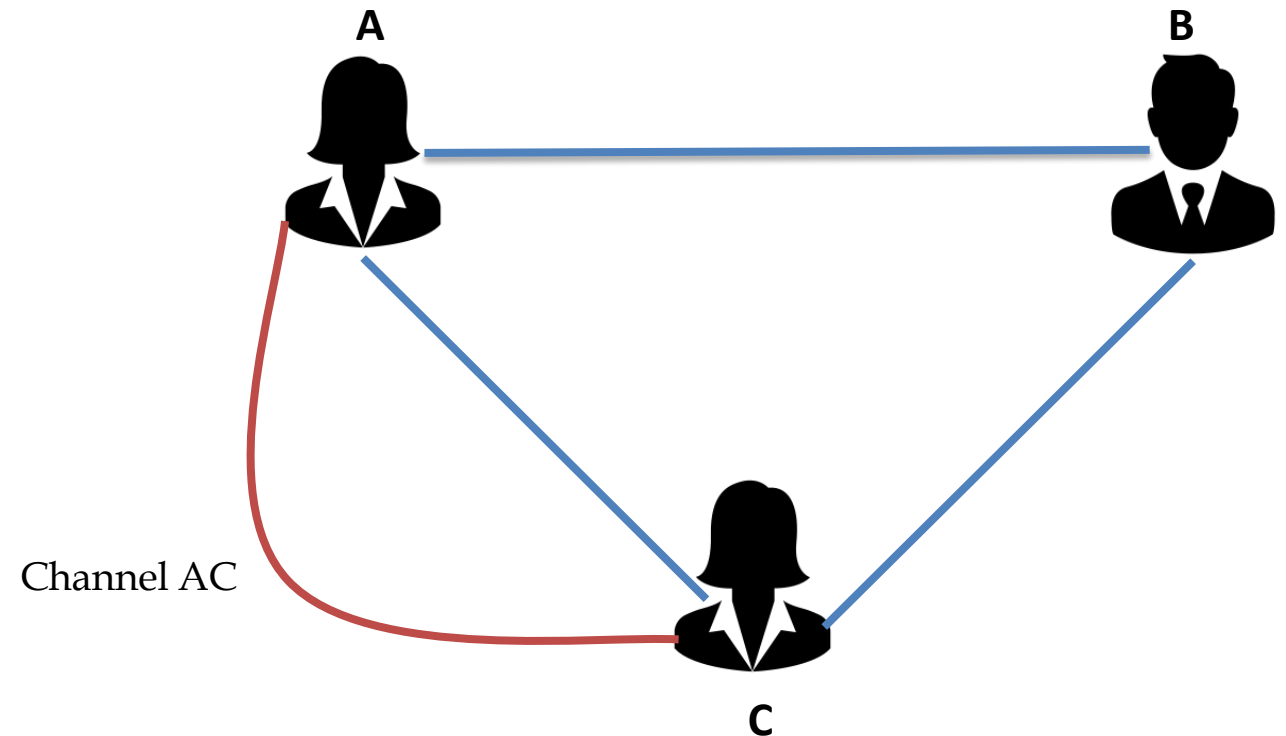
Channel

- A communication pathway between members of a Hyperledger Fabric network .
- Transaction on a Hyperledger Fabric network occurs on a channel.
- Channel enables the communication between all the peers, orderer and applications.
- Multiple channels can be created in a network with the same or different participants.
- Each channel will have its own rules and help the participants to transact privately.



Multiple Channel

- Hyperledger Fabric can create multiple channels
- Let A, B, and C be participants in a DLT based business network application
- A and C can conduct a confidential transaction by creating a separate channel between them



Components of Hyperledger Fabric

- Certificate Authority
- Peers
- Ledger
- Smart contract
- Orderer

Certificate Authority

- Certificate Authority, is a service needed for issuing the (*enrollment*) certificates to authenticated participants
- Issues certificates to network member organizations and their users
- The CA issues digital certificates that comply with **X.509** standard
- Generate certificates using **Fabric CA** and **Cryptogen**
- **Membership Service Provider (MSP)** - set of folders that are added to the configuration of the network and is used to define an organization

Peer

- A network entity(node) that maintains a ledger and runs chaincode containers in order to perform read/write operations to the ledger.
- Peer manages the Ledger which consists of the Transaction Log (Blockchain) and World State
 - **World State:** holds **current values**
 - **Blockchain:** records all the changes that have resulted in the current the world state
- Peer has two roles Endorser and Committer

Types of Peers

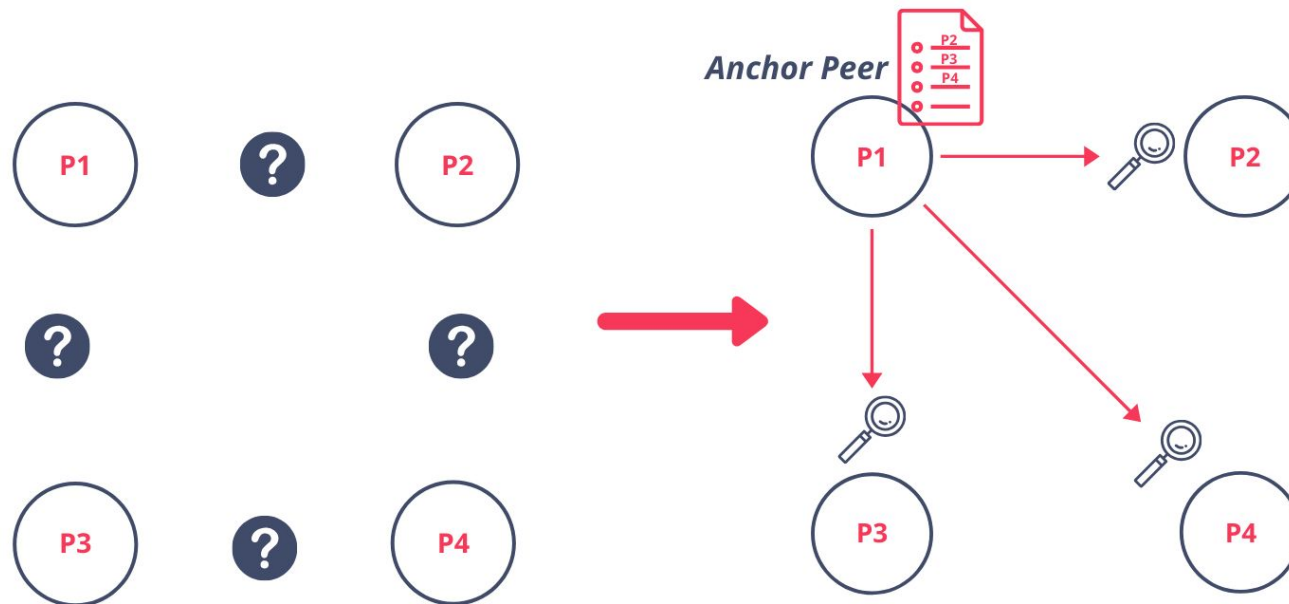
Committing Peer: Maintains ledger and state. Commits transactions. May hold smart contract(Chaincode)

Endorsing Peer: Specialised peers also endorses transactions by receiving a transaction proposal and respond by granting or denying endorsement. Must hold contract

Other peers....

Anchor peer:

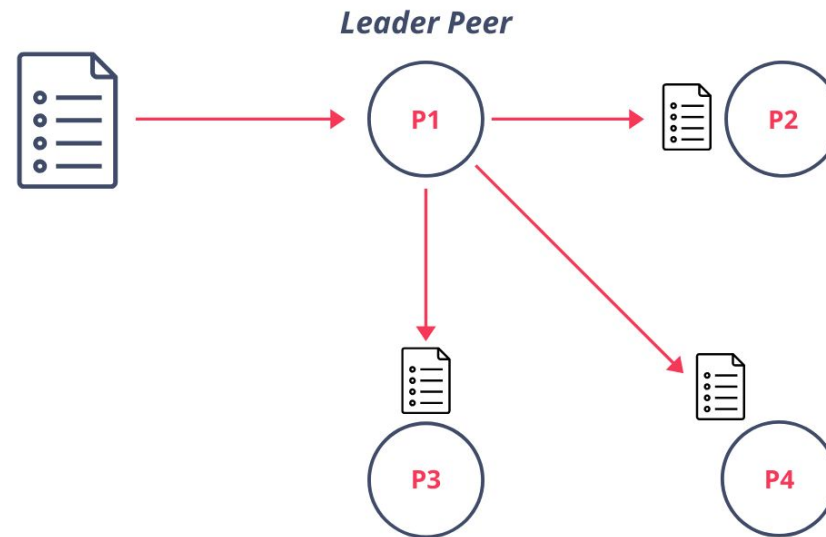
- perform cross-organisation communication scenarios and it is defined in the channel configuration.



Other peers conti....

Leader Peer:

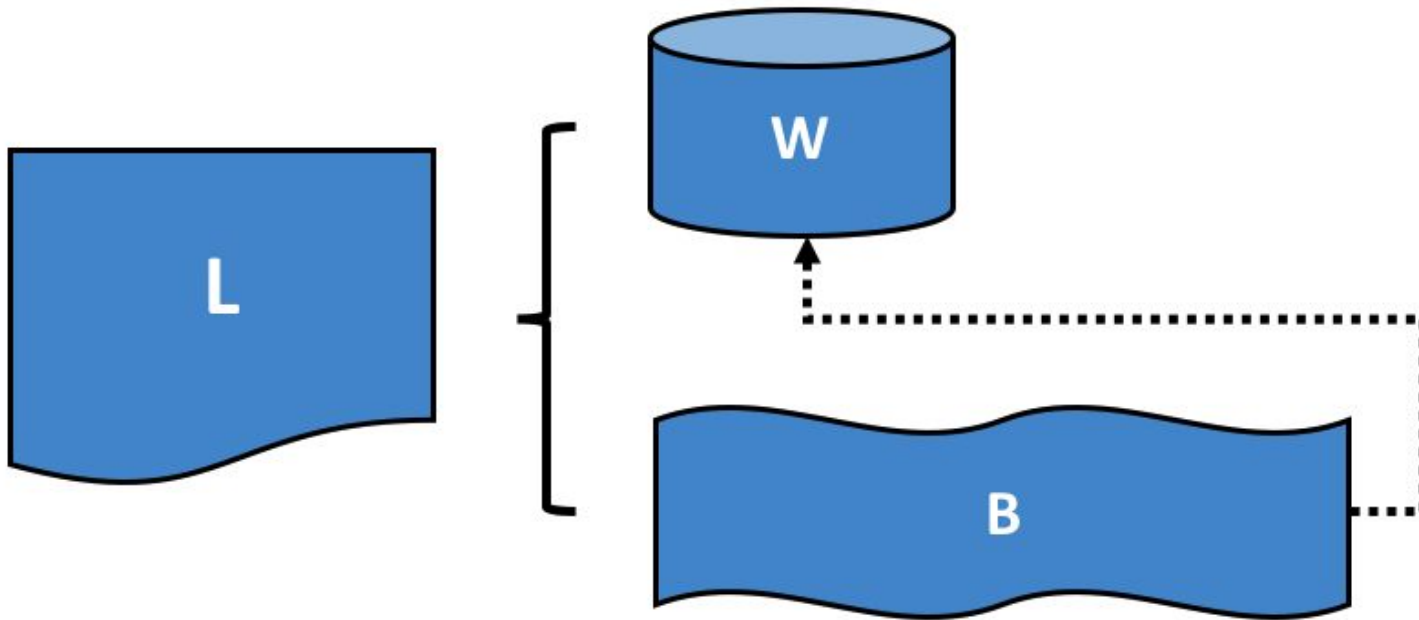
- sends the transactions received from the **orderer** to other **committing peers** in the channel.




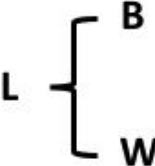
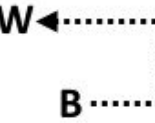


Fabric Ledger

- A ledger is a sequenced, tamper-resistant record of all state transitions.
- The Fabric ledger is maintained by each peer and includes the **blockchain** and **worldstate**
- A separate ledger is maintained for each channel the peer joins.
- Channel configurations, Transaction etc are written to the blockchain
- The worldstate can be either LevelDB (default) or CouchDB
 - LevelDB** is a simple key/value store
 - CouchDB** is a document store that allows complex queries
- The smart contract decides what is written to the worldstate

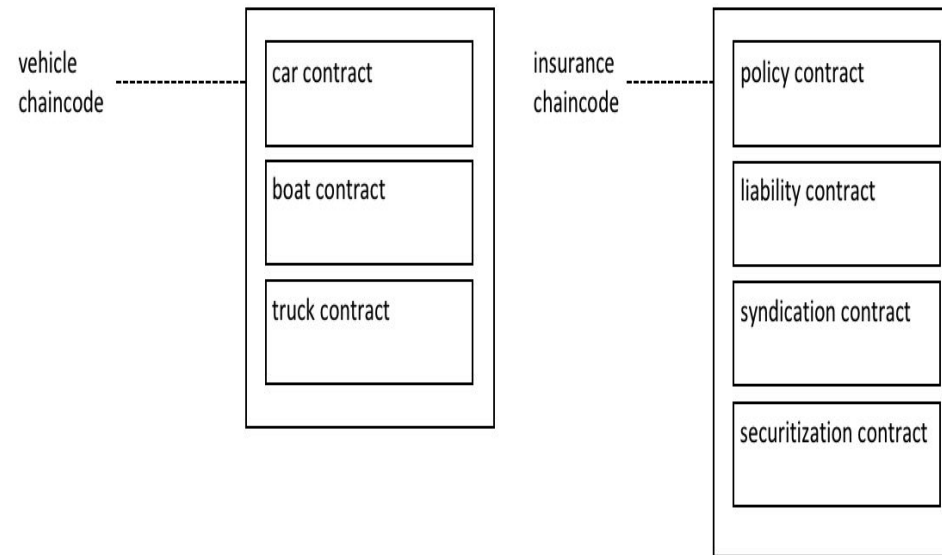
Ledger : World State and Blockchain



	Ledger
	World State
	Blockchain
	L comprises B and W
	B determines W

Smart Contract

- A smart contract defines the **transaction logic**.
- A smart contract is defined within a **chaincode**.
- Multiple smart contracts can be defined within the same chaincode.
- When a chaincode is deployed, all smart contracts within it are made available to applications.



Ordering Nodes

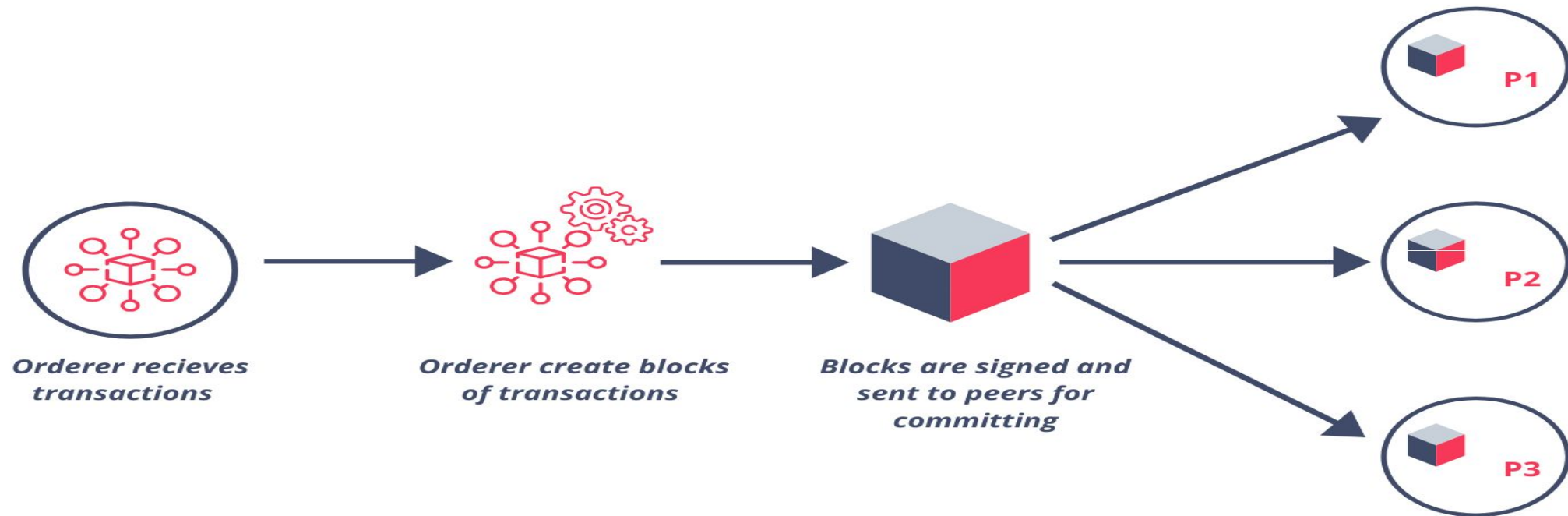
- Approves the inclusion of transaction blocks into the ledger and communicate with committing and endorsing peer nodes.
- Orderer Node also holds the ledger.

Ordering Services

The ordering service packages transactions into blocks to be delivered to peers. Communication with the service is via channels.

- Nodes receive transactions from many different application clients concurrently.
- Arrange batches of submitted transactions into a well-defined sequence and package them into *blocks*.
- These blocks will become the *blocks* of the blockchain.

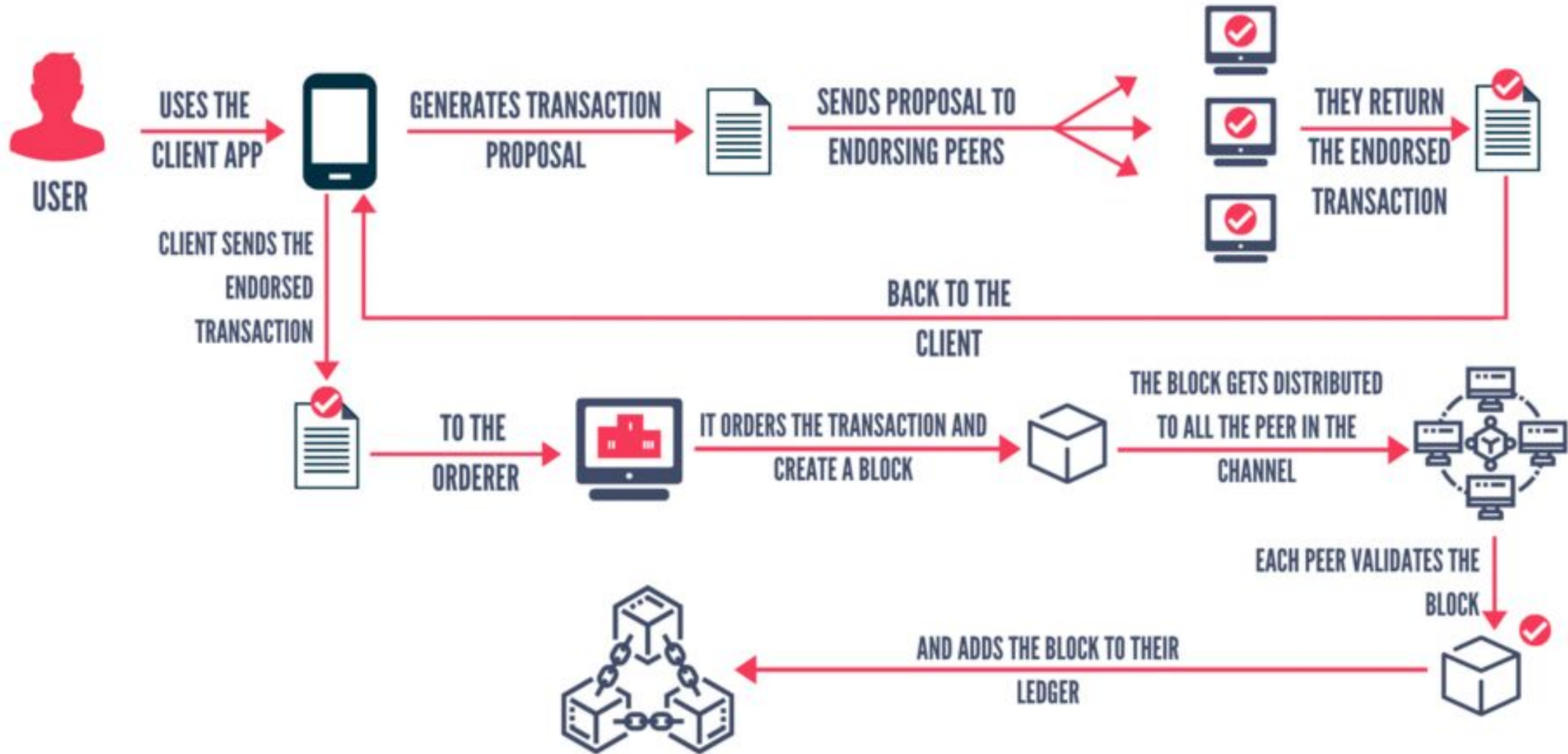
Working of Orderer



Endorsement Policy

- Every chaincode has an endorsement policy.
- Endorsement policies define the smallest set of organizations that are required to endorse(approve) a transaction in order for it to be valid.
- To endorse, an organization's endorsing peer needs to run the smart contract associated with the transaction and sign its outcome.
- When the ordering service sends the transaction to the committing peers, they will each individually check whether the endorsements in the transaction fulfill the endorsement policy.

Transaction Flow



Steps in Transaction Flow

1. Client generates Transaction Proposal.
2. Submit Transaction Proposal.
3. Endorsing.
4. Sending to Orderer.
5. Ordering and Block Distribution.
6. Updating the Ledger.
7. Notify the client.

Client generates Transaction Proposal

The client generates a transaction proposal message.

The proposal has the following attributes:

1. **ClientID** - Identifies the client
2. **ChaincodeID** - Identifies the Chaincode to be invoked
3. **Transaction Payload** - It contains the functions to be invoked and the arguments

The client then **signs** the proposal message with the private key.



Submits Transaction Proposal

Client Submits the Transaction Proposal

- The Client Node / Application Node submits the transaction proposal to the Endorsing peer for approval.
- The Endorsement is done based on how the Endorsing policy defined. Based on the policy, the proposal is submitted to Endorsing peers



Endorsing

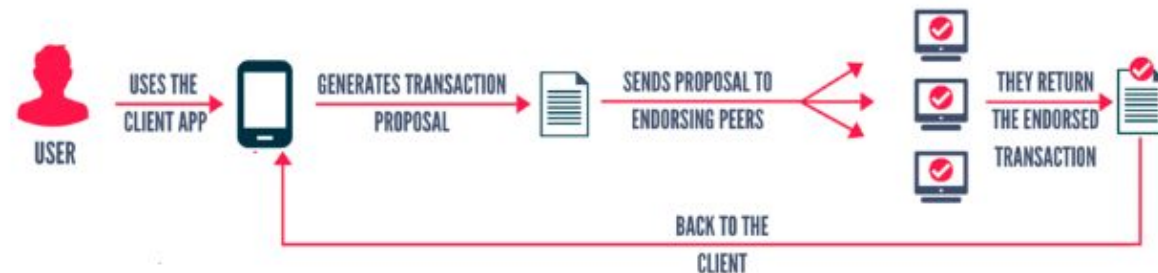
Once the **Endorsing peers(EP)** receive the proposal, they start performing the endorsing process.

If the signature is valid, then the EP will simulate the transaction execution. Simulation results in the creation of the **Read/Write set**.

The signing of the proposal results in the creation of **Transaction Proposal Response - Endorsed** message.

The response has the following attributes:

1. **Endorsing peer's signature**
2. **Read Set** - State value of the key used for the simulation.
3. **Write Set** - State value of the key after executing the logic



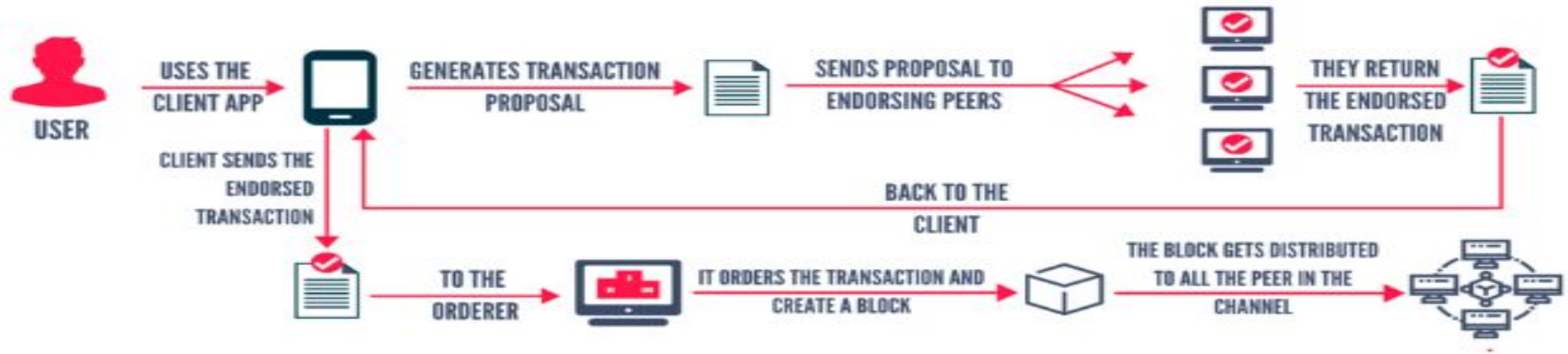
Sending to orderer

- Client verifies the signature of the endorsing peers by comparing the transaction proposal response with the signature of the endorsing peer.
- The transaction may get rejected if the EP signature is not valid or there is a mismatch in proposal responses.
- If everything is fine, then the client sends the transaction to the orderer.



Ordering and Block Distribution

- The Orderer receives the transactions in a group and orders them according to the sequence it received.
- It then creates a block of transactions based on parameters like block size or block timeout which ever is earlier.
- Created blocks are broadcasted to all the peers in the channel.



Updating Ledger

Peer performs its own validation on the blocks received from the orderer.

The process involves:

1. Validating the Endorser and client signature in the transaction done in endorsing step.
2. Validating the Endorsement policy

If the validation is successful, then the data in the block is added to the ledger marked as "**Valid**". If unsuccessful, it is marked as "**Invalid**" and added to the transaction log.

Notify the client

- The client will be notified that the transaction is completed by using events.
- The client records it as a successful or unsuccessful transaction.

Consensus

- A way of coming to an agreement
- Integral to a decentralized system
- Participants may or may not trust each other
- Agreement on common principles of functioning

- In Hyperledger Fabric:
 - Raft
 - SmartBFT
 - Solo and Kafka (deprecated)

THANK YOU