Blockchain

Bacem Mbarek, Ph.D.
Masaryk University,
Lasaris Lab (Lab of Software Architectures and Information Systems)

Plan: Brief description

- **Blockchain components**

Learn about Blockchain components and how they work together to create a Blockchain network.

- **Hyperledger Fabric**

Learn the practical implementation of the Hyperledger Fabric blockchain framework.

- **Security and Privacy**

Learn about the Security, Scalability, and Privacy in Blockchain Applications and Smart Contracts.

- **Hyperledger caliper**: Blockchain Simulator

Learn how to design and implement Hyperledger caliper benchmark tool to measure the performance of a Blockchain implementation.

- **Blockchain and Internet of things(IoT)**

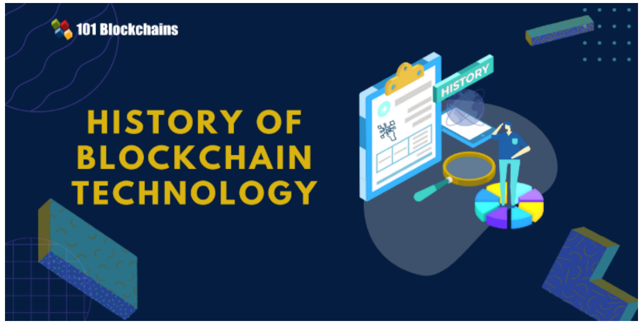
Learn about why Blockchain should be integrated with IoT and how to do this.

- **Student project: Create a real Blockchain platform in real context**

General Introduction

- Blockchain technology distribution was seen in October 2008 under an alias Satoshi Nakamo with the aim of supporting the first Bitcoin cryptocurrency, and it caused result in starting Bitcoin network in January 2009.

- Bitcoin has inchmeal entered the financial industry, and to be recognized as the most influential and important cryptocurrency.

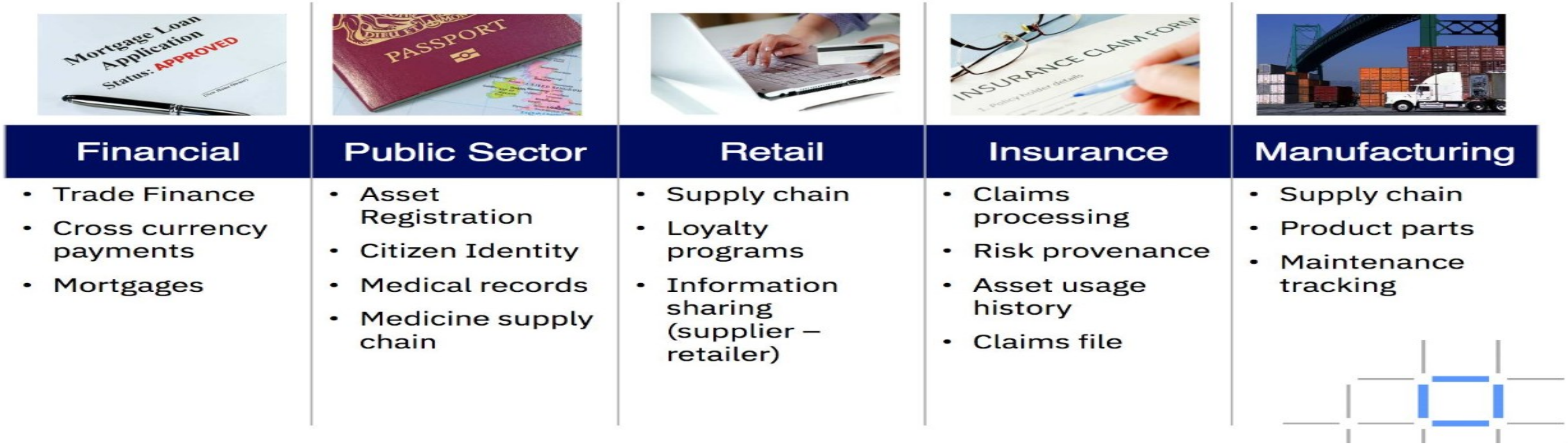


Application domains

- The blockchain technology after Bitcoin has become a game-variable innovation around the world.
- Lots of industries exist which will be interrupted via blockchain, including life sciences, legal industry, health care, financial services, cyber security, cloud storage, supply series management, cloud storage, charity, electing, government, social interests, energy management, private transport and ride sharing, retail, and actual estate between others.
- Blockchain usages in carbon credits, distributes energy resources and renewable and power systems data security versus cyber-attacks are really encouraging,

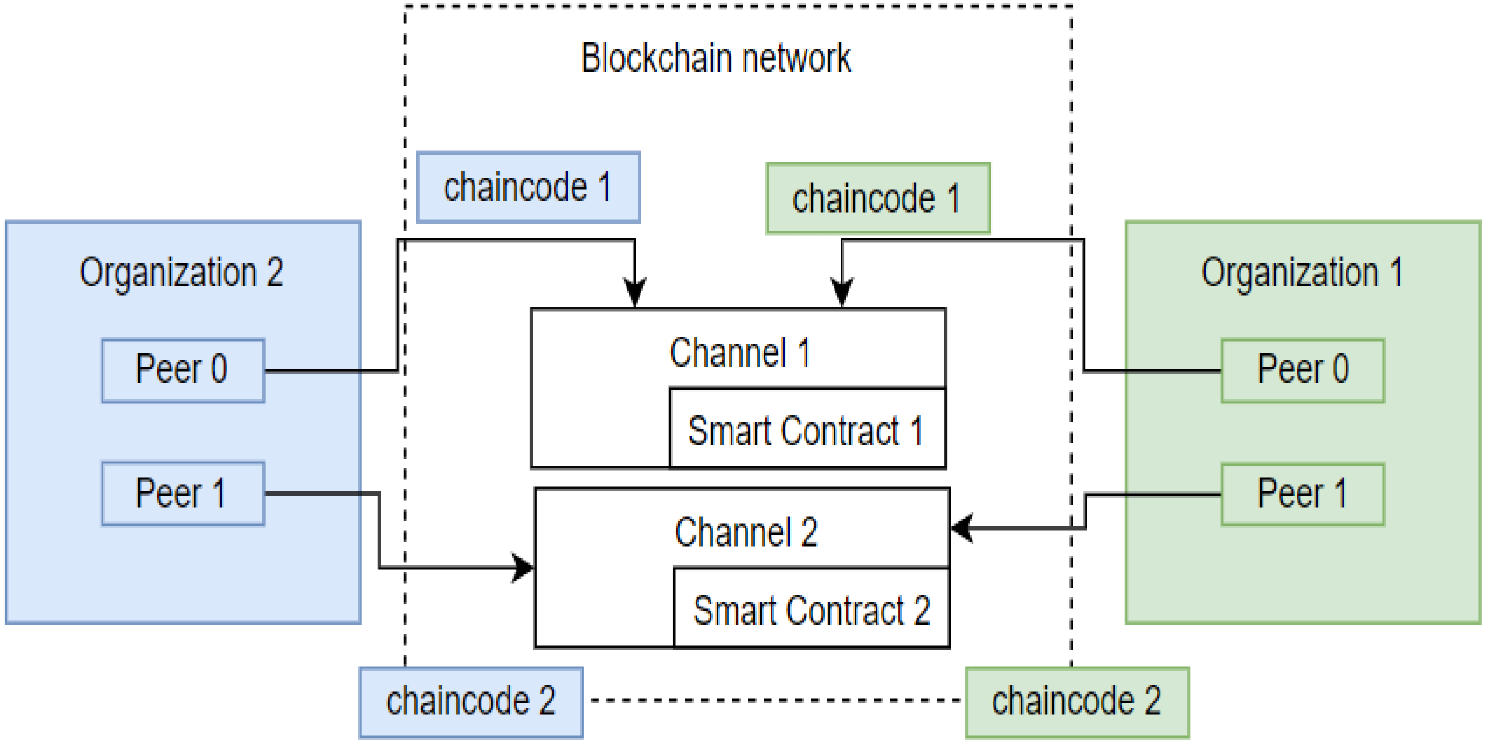
Application domains

Banks, insurance, health and pharmaceutical industry, supply chain of many sectors (food industry, luxury, international trade, distribution, wines, aeronautics, automobile ...), music, industry, energy, real estate, voting ...



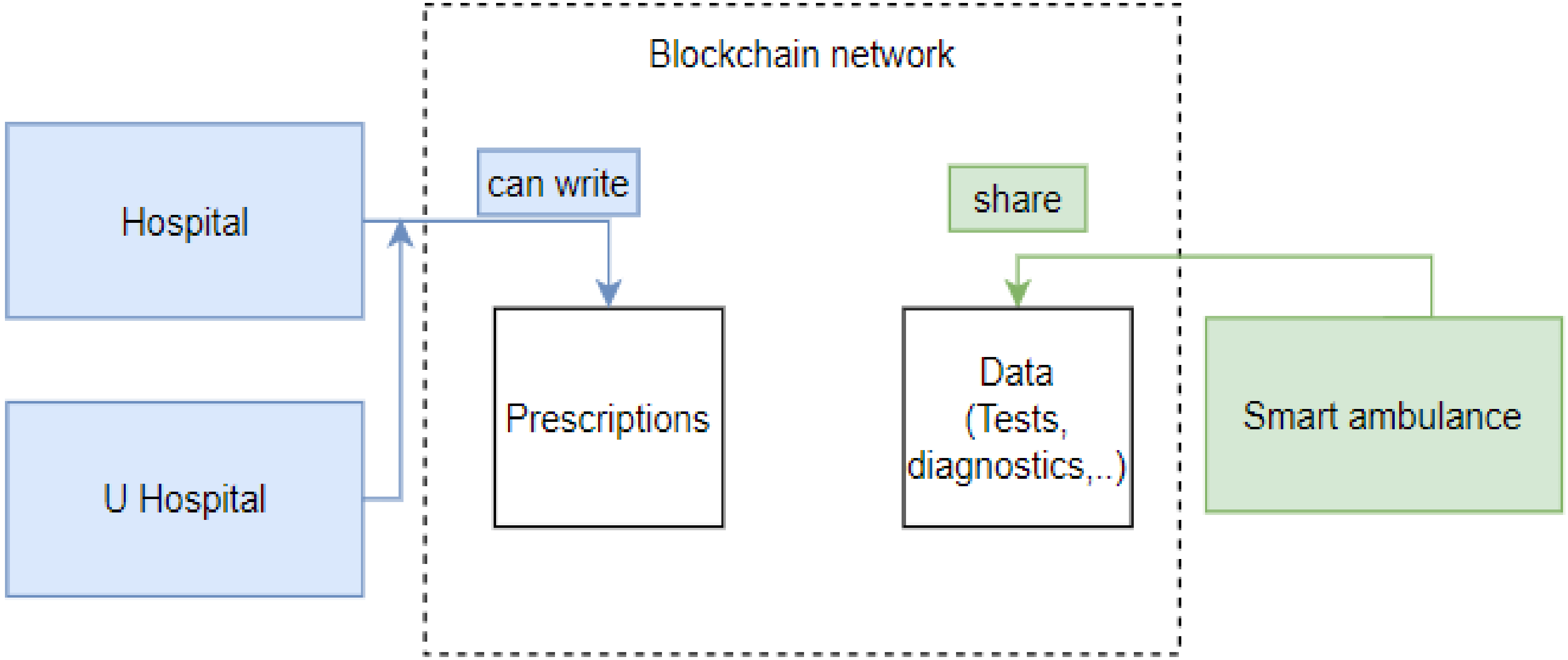
Financial	Public Sector	Retail	Insurance	Manufacturing
• Trade Finance • Cross currency payments • Mortgages	• Asset Registration • Citizen Identity • Medical records • Medicine supply chain	• Supply chain • Loyalty programs • Information sharing (supplier – retailer)	• Claims processing • Risk provenance • Asset usage history • Claims file	• Supply chain • Product parts • Maintenance tracking

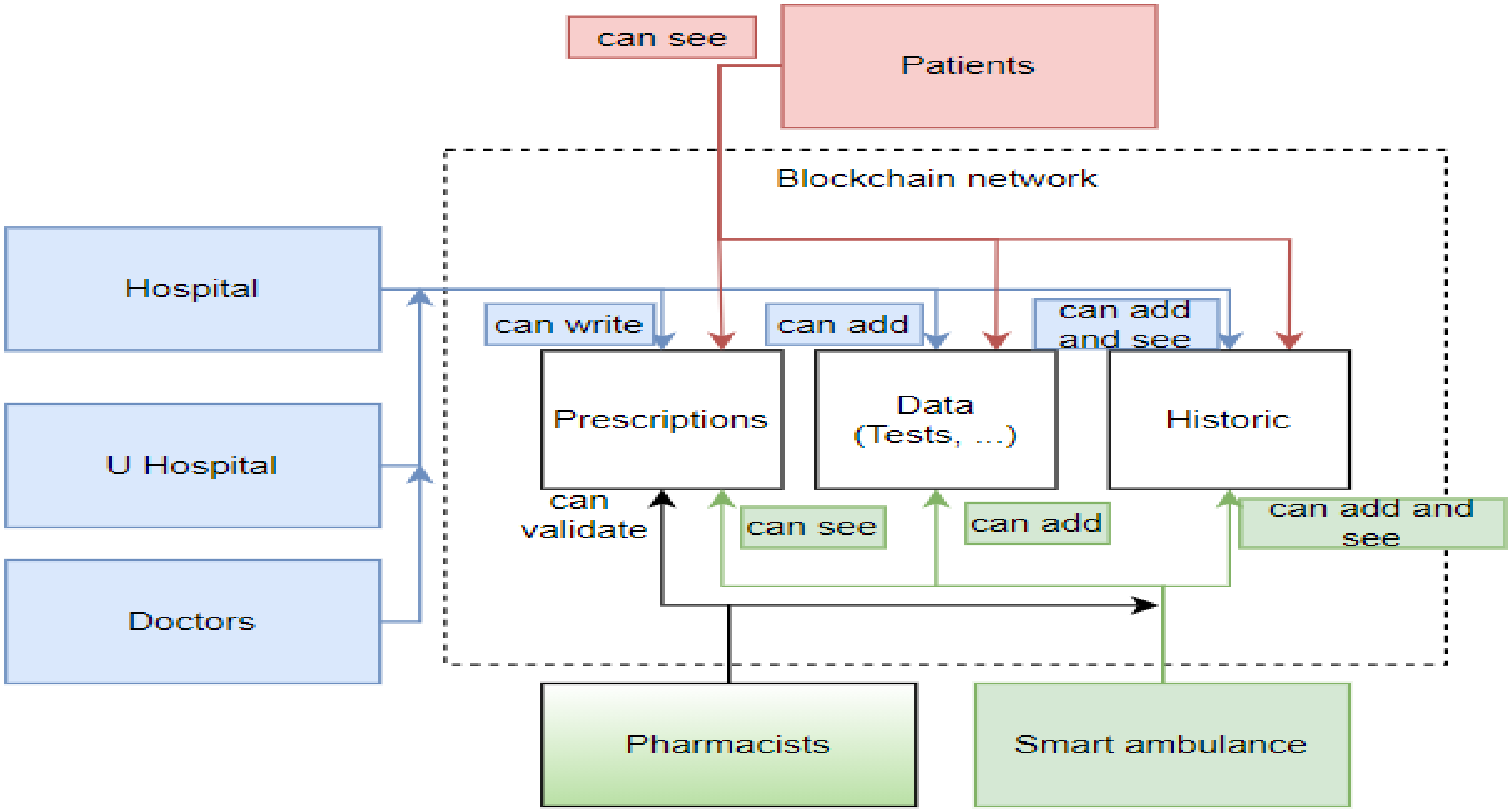
Blockchain Framework



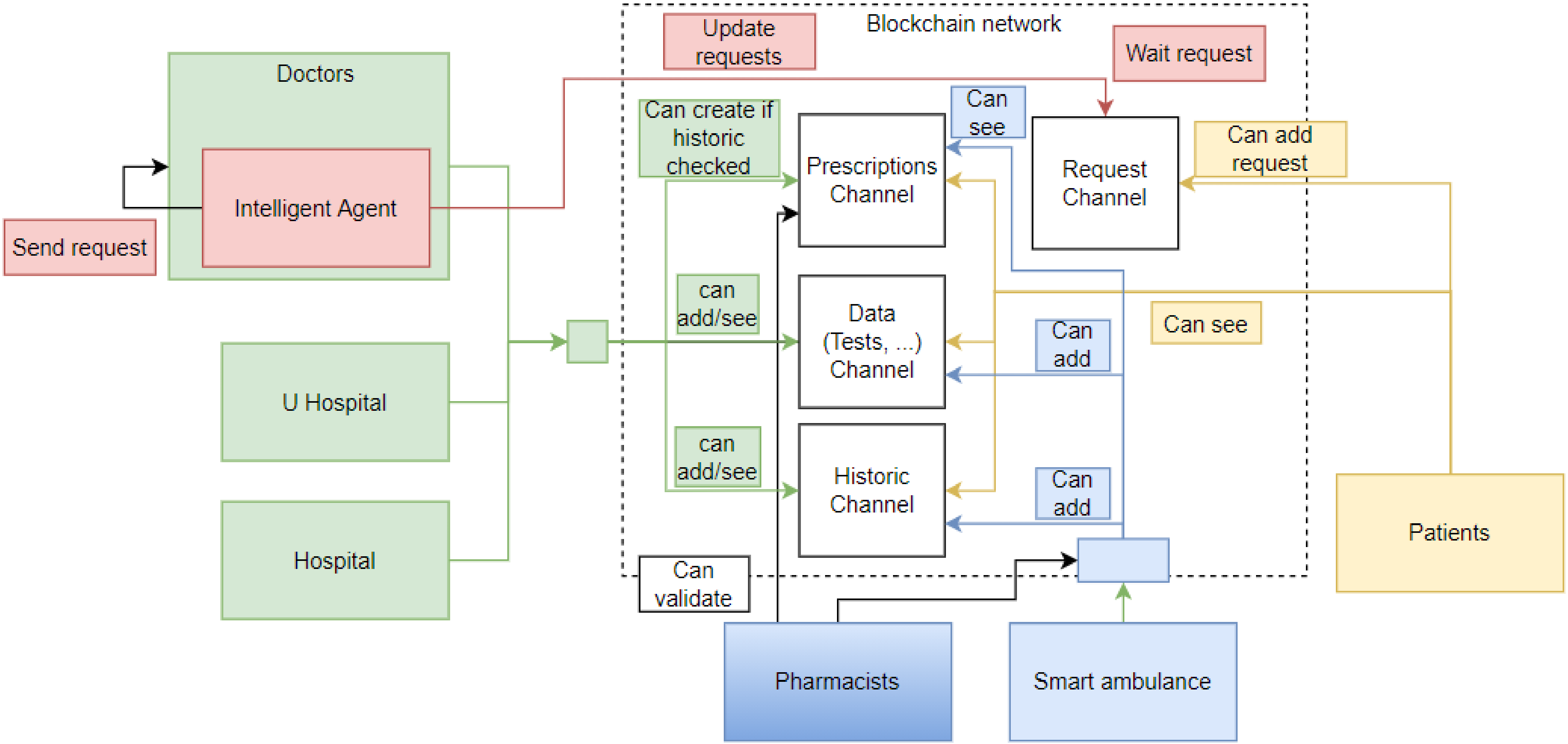
Hyperledger Fabric example network

Blockchain- Healthcare application





Improved use case for the first solution



Blockchain network
Update requests
Wait request
Doctors
Intelligent Agent
Send request
Can create if historic checked
Can see
Prescriptions Channel
Request Channel
Can add request
can add/see
Data (Tests, ...) Channel
Can add
Can see
U Hospital
can add/see
Historic Channel
Can add
Hospital
Can validate
Patients
Pharmacists
Smart ambulance

Why Blockchain

Blockchain helps primarily in three different ways

1. Trust – Blockchain helps in creating applications that are decentralized and collectively owned by multiple people. No body within this group has the power to change or delete previous transactions. Even if someone tries to do so, it will be not be accepted by other stakeholders.

2. Autonomy- There is no single owner for Blockhain based applications. No one controls the Blockchain, but everyone participates into its activities. This helps in creating solutions that cannot be manipulated or induce corruption.

3. Integrity- The state and transactions are secured cryptographically and cannot be modified easily.

Understanding Blockchain (1)

What is Blockchain?

Blockchain is essentially a decentralized distributed database or ledger. There are some very important keywords like decentralized, distributed, database and ledger used in defining Blockchain.

Decentralization in simple term means that the application or service continue to be available and usable even if a server or a group of servers on a network crashes or are not available, The service or application is deployed on a network in a way that no server has absolute control over data and execution rather each server has current copy od data and execution logic with them.

Understanding Blockchain (2)

- Distributed means that any server or node on a network is connected to every other node on the network directly or indirectly. Rather than having one to one or one to many connectivity between servers, servers have many to many connections with other servers.

- Database refers to location for storing durable data that can be accessed at any point in time, Database allows storage and retrieval of data efficiently like export, import, backup and restoration.

Ledger

Ledger is an accounting term and think of it as specialized storage and retrieval of data.

Think of ledgers that are available with banks. When a transaction is executed with a Bank say Tom deposits 100 dollars in his account, the bank enters this information in ledger as a credit.

At some point in time in future Tom withdraws 25 dollars, The bank does not modify the existing entry and sored data from 100 to 75.

Instead, it adds another entry in the same ledger as a debit of 25 dollars. It means a ledger is a specialized database that do not allow modification of existing data. It allows creation and appending of new transaction to modify the current balance in the ledger.

Blockchain ledger (1)

Blockchain is a database that has the same characteristics of a ledger. It allows newer transaction to be stored in append only pattern without any scope to modify past transaction, It is important here to understand that existing data can be modified by using a new transaction, but past transactions cannot be modified.

A balance of 100 dollar can be modified anytime by executing a new debit or credit transaction but previous transaction cannot be modified.

Blockchain ledger (2)

- ✓ Blockchain is a **distributed ledger** that records all the transactions that take place on the network.

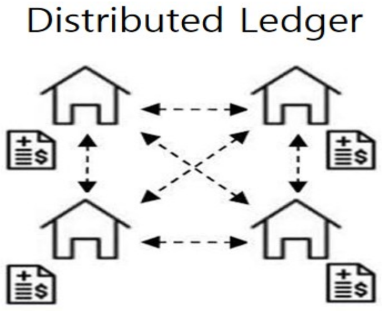
- ✓ **A distributed ledger** is a database that is consensually shared and synchronized across multiple sites, institutions or geographies.

- ✓ The participant at each node of the network can access the recordings shared across the network and can own an identical copy of it.

Distinction between centralized, decentralized and distributed

A **blockchain can** be either **centralized** or decentralized. It is important, however, that decentralized not be confused with **distributed**. While a **blockchain** is inherently **distributed** (meaning that many parties hold copies of the ledger), it is not inherently decentralized.

Consensus:
The process of keeping the ledger transactions synchronized across the network –to ensure that ledgers update only when transactions are approved by the appropriate participants, and that when ledgers do update, the update with the same transactions in the same order – is called consensus.



- Each node has an identical ledger that contains transaction after "**consensus**"
- Network effect holds transaction immutability

A blockchain database

❑ A blockchain is a way to implement a distributed ledger, but not all distributed ledgers necessarily employ blockchains.

❑ In a distributed ledger, it is not necessarily the case that all nodes either receive all the information.

❑ By extension, a blockchain constitutes a database that contains the history of all the exchanges made between its users since its creation.

❑ This database is secure and distributed: it is shared by its different users, without intermediaries, which allows everyone to check the validity of the chain.

How it works?

Channel

- A channel is a private blockchain overlay which allows for data isolation and confidentiality. A channel-specific ledger is shared across the peers in the channel, and transacting parties must be properly authenticated to a channel in order to interact with it.

- A channel can be defined as a sub-network for peers communication, if it is necessary to divide transactions according to different boundaries according to some service logic.

Blockchain as the word refers means a chain of Blocks. Blockchain means having multiple blocks chained together and each block stores transactions in a way that it is not possible to modify these transactions. We will discuss in later section about storage of transactions and how immutability is achived in blockchain.

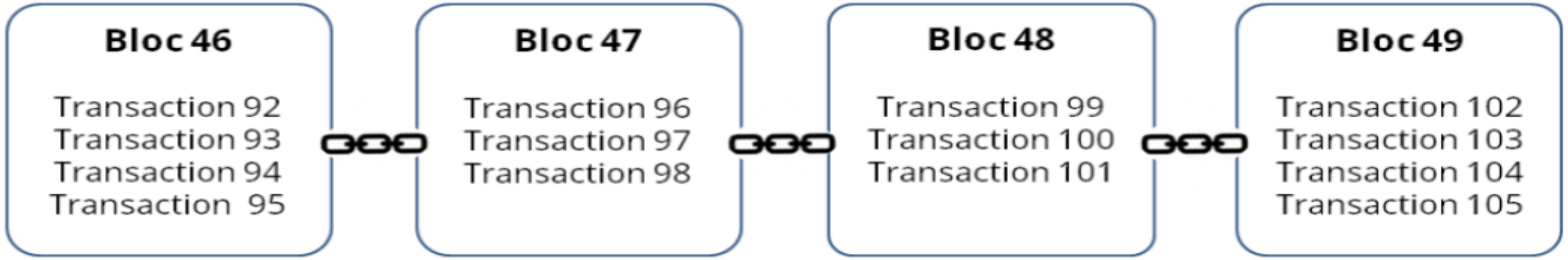
Not being able to change and modify past transactions makes Blockchain solution highly trustworthy, transparent and incorruptible.

It is important to understand that blocks and its chain is just one of the facts of blockchain. There are other important like mining, miners, consensus and protocol that works along with chain of blocks to make blockchain work flawlessly.

Blocks

“Blocks” on the blockchain are made up of digital pieces of information. Specifically, they have three parts:

- Blocks store information about transactions like the date, time, and price, etc.
- Blocks store information about who is participating in transactions.
- Blocks store information that distinguishes them from other blocks. Each block stores a unique code called a “hash” that allows us to tell it apart from every other block.



Bloc 46
Transaction 92
Transaction 93
Transaction 94
Transaction 95

Bloc 47
Transaction 96
Transaction 97
Transaction 98

Bloc 48
Transaction 99
Transaction 100
Transaction 101

Bloc 49
Transaction 102
Transaction 103
Transaction 104
Transaction 105

Transaction

- ❑ A **Blockchain transaction** can be **defined** as a small unit of task that is stored in public records.

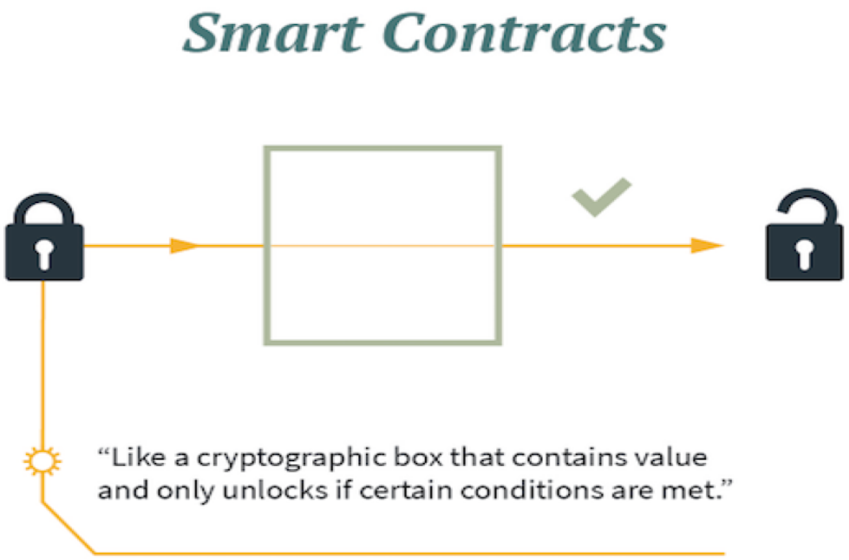
- ❑ These records also know as blocks.

- ❑ These blocks are executed, implemented and stored in **blockchain** only after the validation by all persons involved in the **blockchain** network.

- ❑ So, when a blockchain transaction happens all the nodes in the network will have to say it’s valid or it won’t get added to the ledger.

Smart contract (1)

In blockchain, the smart contract is a code fragment that executes the terms of a contract. The code behind a smart contract contains specific terms that are executed when triggered by specific agreed events. A blockchain network uses smart contracts to provide controlled access to the ledger.

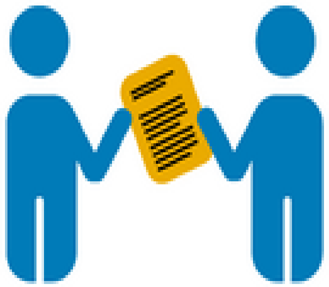

Smart Contracts
"Like a cryptographic box that contains value
and only unlocks if certain conditions are met."

Smart contract (2)

Smart contracts are designed and implemented within blockchains, and therefore they inherit some of the blockchain's properties:

✓ **They're immutable**, which means a smart contract can never be changed and no one can tamper with or break a contract.

✓ **They're distributed**, which means that the outcome of the contract is validated by everyone in the network, just like any transaction on a blockchain. Distribution makes it impossible for an attacker to force control to release funds, as all other participants would detect such an attempt and mark it as invalid.



An option contract between parties is written as code into the blockchain. The individuals involved are anonymous, but the contract is the public ledger.

Application domains

We can classify the use of blockchain in three categories:

- Applications for the transfer of assets (monetary use, but not only: securities, votes, stocks, bonds, etc.).

- Blockchain applications as a registry: it thus ensures better traceability of products and assets.

- Smart contracts: these are stand-alone programs that automatically execute the terms and conditions of a contract, without requiring human intervention once started.

Blockchain platforms

Many Blockchain platformscan be considered like Ethereum, Hyperledger, Multichain,Open Ledger, Chain, Bitcoin Blockchain, and Corda.

Hyperledger Fabric (1)

What is Hyperledger Fabric ?

Hyperledger Fabric is one of the blockchain projects within Hyperledger. Like other blockchain technologies, it has a ledger, uses smart contracts, and is a system by which participants manage their transactions.

Hyperledger Fabric — hosted under Linux Foundation — is a private, permissioned and open source blockchain solution.

Private means that blockchain networks are not publicly accessible and only invited parties can join the network. Permissioned means each party is clearly identified and every transaction is authenticated, authorized, validated and tracked.

Hyperledger Fabric (2)

Organization

- An organization in Hyperledger Fabric corresponds to a real organization, company, political party, etc.

- Each organization in Fabric has to dispose of a Public Key Infrastructure (PKI) which has to be comprised of a Certificate Authority (CA) and possibly even an Intermediate Certificate Authority (ICA) that will issue digital certificates for the organizations identities (e.g. users, client applications, peers, orderers). Those then use them to authenticate themselves in the messages they exchange within the networks.

- Hyperledger Fabric comes with a default CA service but it is not necessary to use the default service for your PKI management.

Hyperledger Fabric (3)

Membership Service Provider (MSP)

- ❑ **Membership Service Provider** (**MSP**) is a component that aims to offer an abstraction of a **membership** operation architecture.

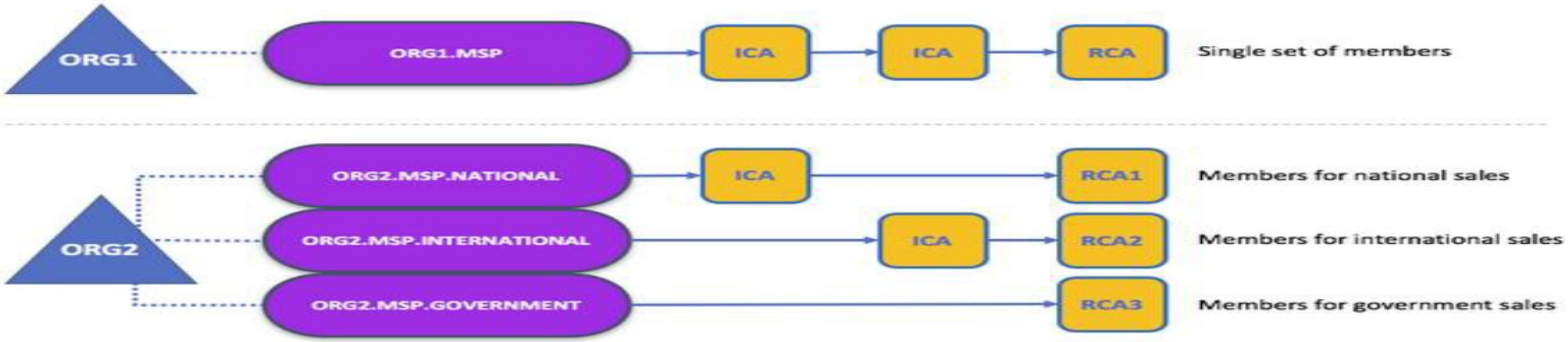
- ❑ In particular, **MSP** abstracts away all cryptographic mechanisms and protocols behind issuing and validating certificates, and user authentication.

- ❑ As mentioned in MSP description, MSPs may be configured with a set of root certificate authorities (rCAs), and optionally a set of intermediate certificate authorities (iCAs).

Hyperledger Fabric (4)

In Fabric, an organization is identified by its MSP. In Hyperledger Fabric Network each organization is identified by its Membership Service Provider identification (MSP ID).

To be accurate, an organization can be comprised of one or multiple MSPs but for most cases, and for the sake of simplicity, you will probably use a single MSP to represent an organization. An MSP is formed by **an instance of a PKI infrastructure** which is then able to issue certificates for the MSP.



Hyperledger Fabric Membership Service Provider (MSP) hierarchy diagram (image source)

Peers

A peer is a node running on the Hyperledger Fabric peer binary. Each organization is supposed to have peers to host ledgers and smart contracts.

Every channel (network) has its own data in a separate ledger stored on peers. And every channel is supposed to have one or more smart contracts (chaincodes). Multiple versions of a chaincode can be installed and stored on organizational peers and can be instantiated into one or multiple channels.

There are different types of peer nodes with different roles in the network:

- ✓ Endorser peer
- ✓ Anchor peer
- ✓ Orderer peer
- ✓ Committing peer

Endorser peer

Peers can be marked as Endorser peer (ie Endorsing peer). Upon receiving the "transaction invocation request" from the Client application the Endorser peer

- Validates the transaction. ie Check certificate details and roles of the requester.
- Executes the Chaincode(ie Smart Contract) and simulates the outcome of the transaction. But it does not update the ledger. At the end of the above two tasks, the Endorser may approve or disapprove the transaction.

As only the Endorser node executes the Chaincode (Smart Contract) so there is no necessity to install Chaincode in each and every node of the network which increases the scalability of the network.

Anchor Peer

- ❑ Anchor peer or cluster of Anchor peers is configured at the time of Channel configuration. Just to remind you, in Hyperledger Fabric you can configure secret channels among the peers and transactions among the peers of that channel are visible only to them.

- ❑ Anchor peer receives updates and broadcasts the updates to the other peers in the organization. Anchor peers are discoverable. So any peer marked as Anchor peer can be discovered by the Orderer peer or any other peer.

Orderer peer

- ❑ Creates the block of transactions, and sends it to all the peers. The ordering service collects transactions for a channel into proposed blocks for distribution to peers.

- ❑ Blocks are delivred on a channel basis. The ordering service accepts endorsed transactions, orders them into a block, and delivers the blocks to the committing peers.

- ❑ The main responsibility of ordering service is to receive transactions from the Blockchain devices and fit into a Block.

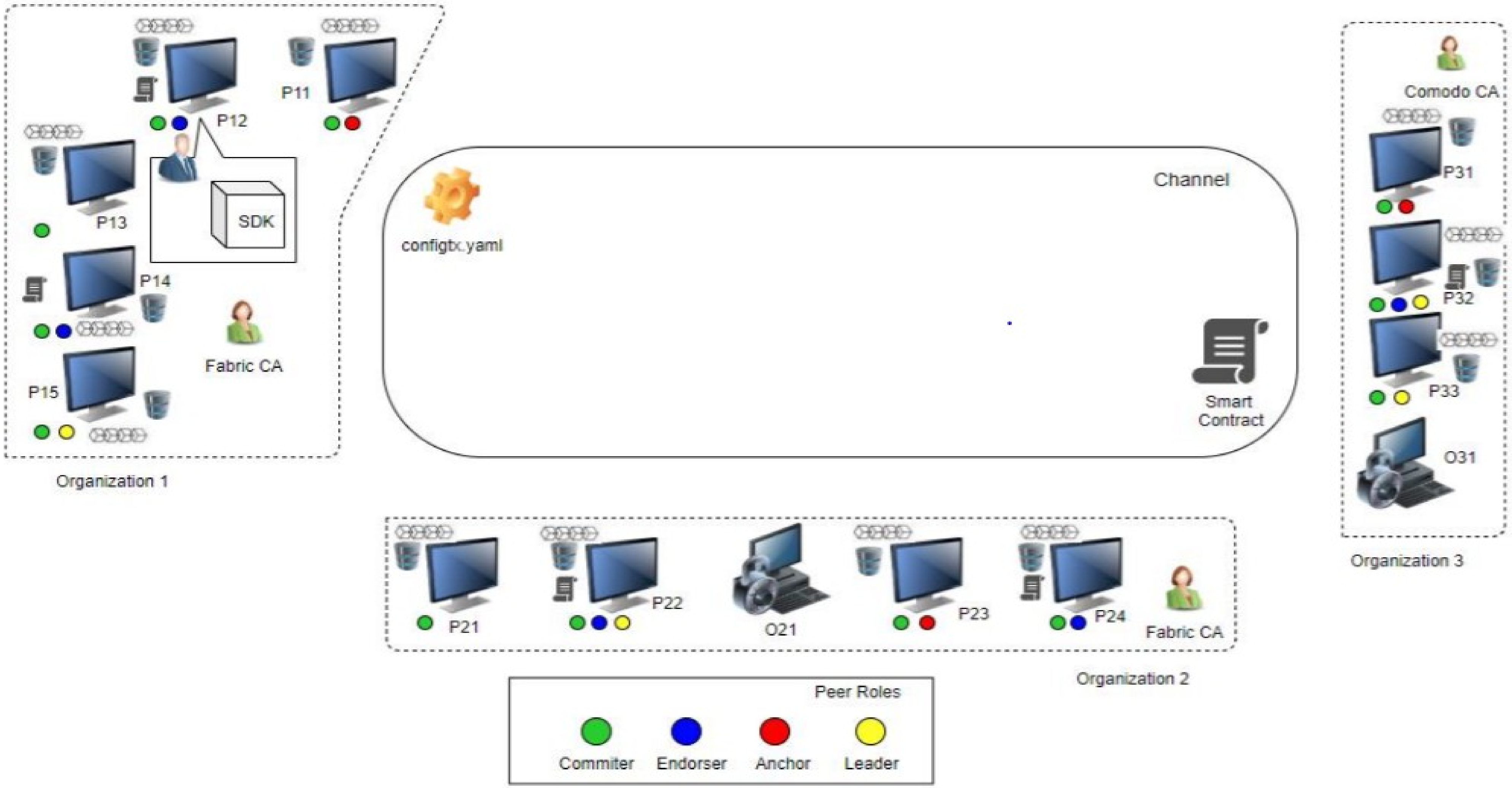
Committing peers

A committing peers are a predefined number of peers.

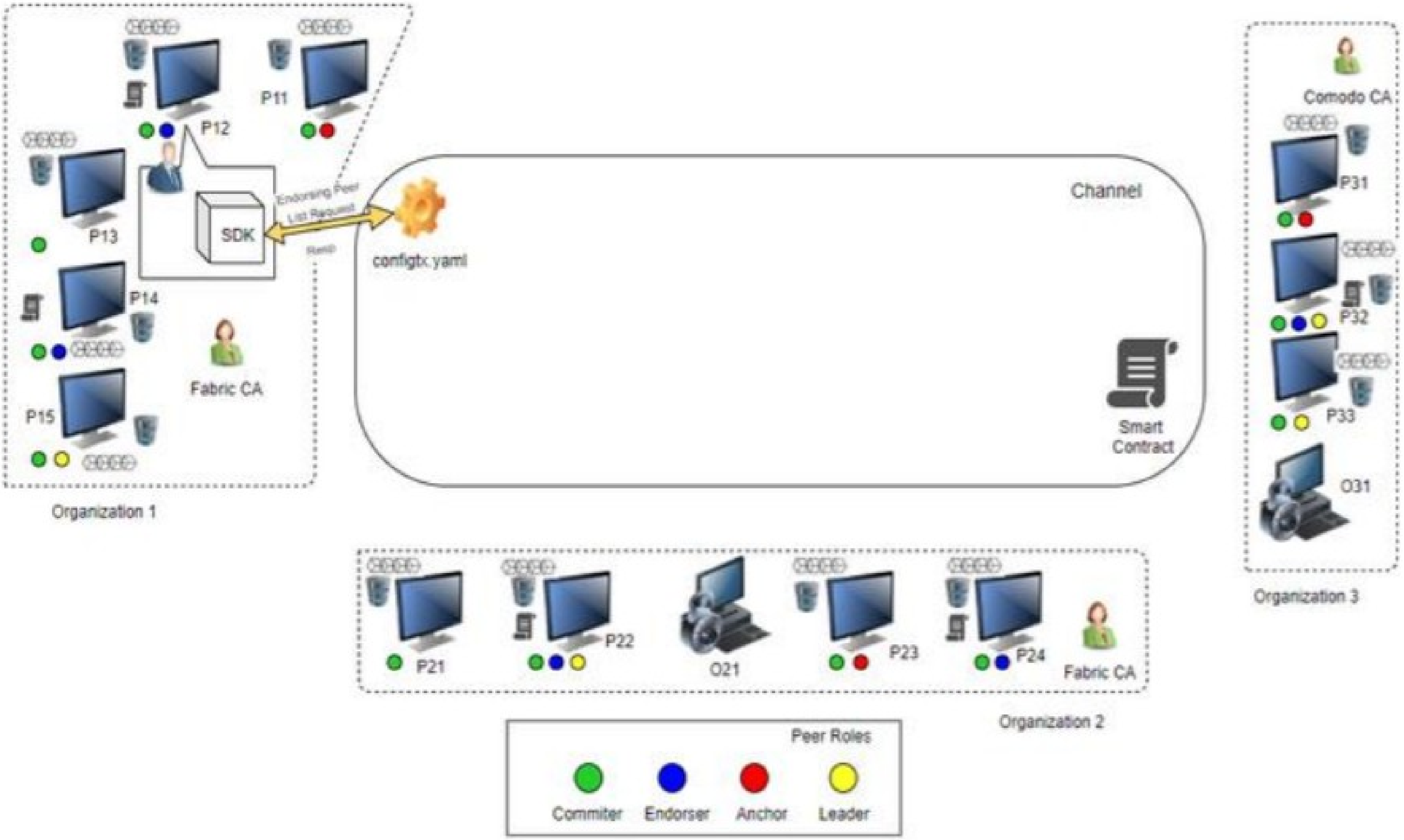
Usually endorsing peers are also committing, but a peer can be only committing and not endorsing.

Committing peers (including endorsing peers) run validation and update their copy of the Blockchain and world state.

Network Setup

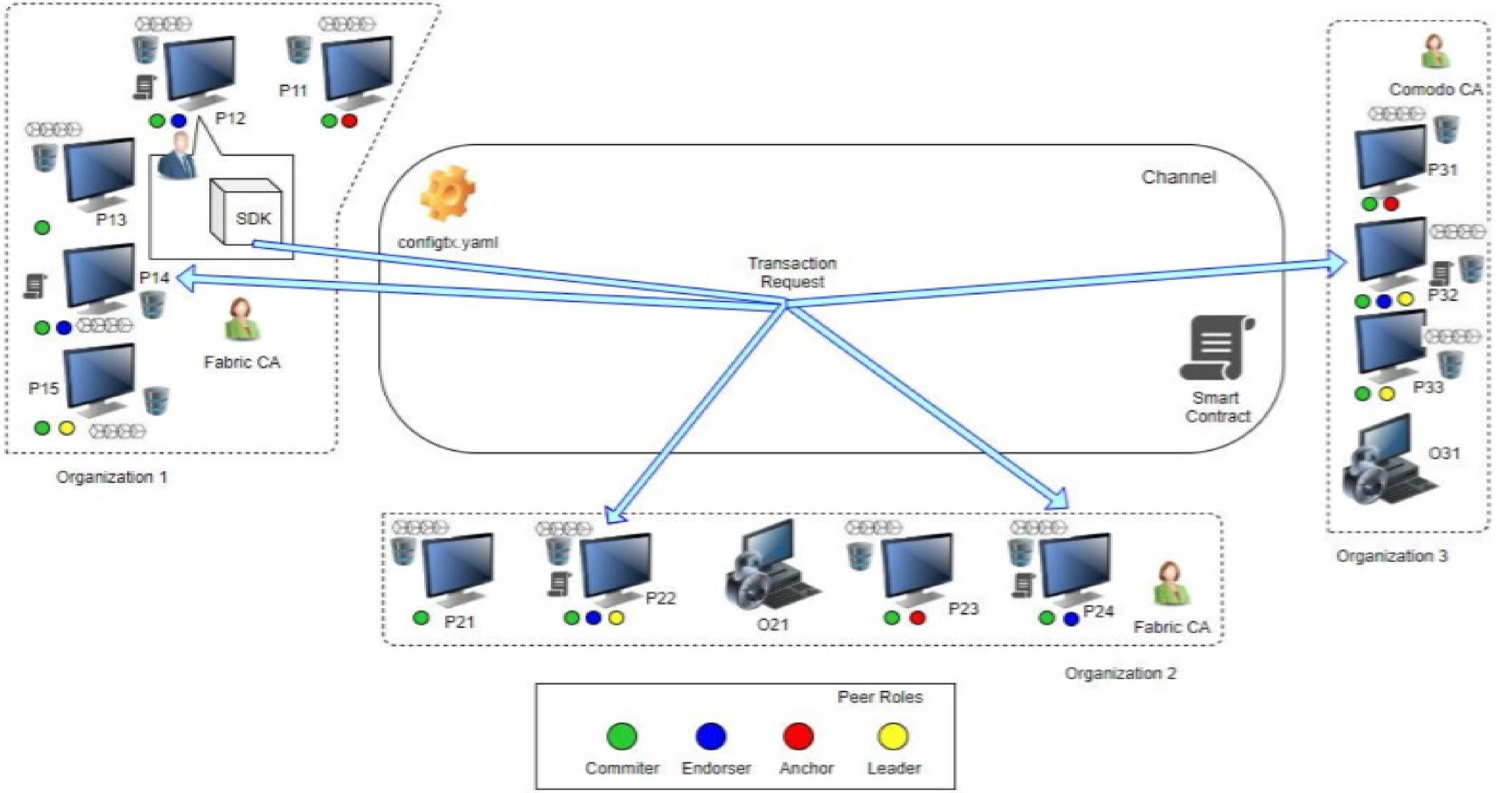


Client Initiates the transaction

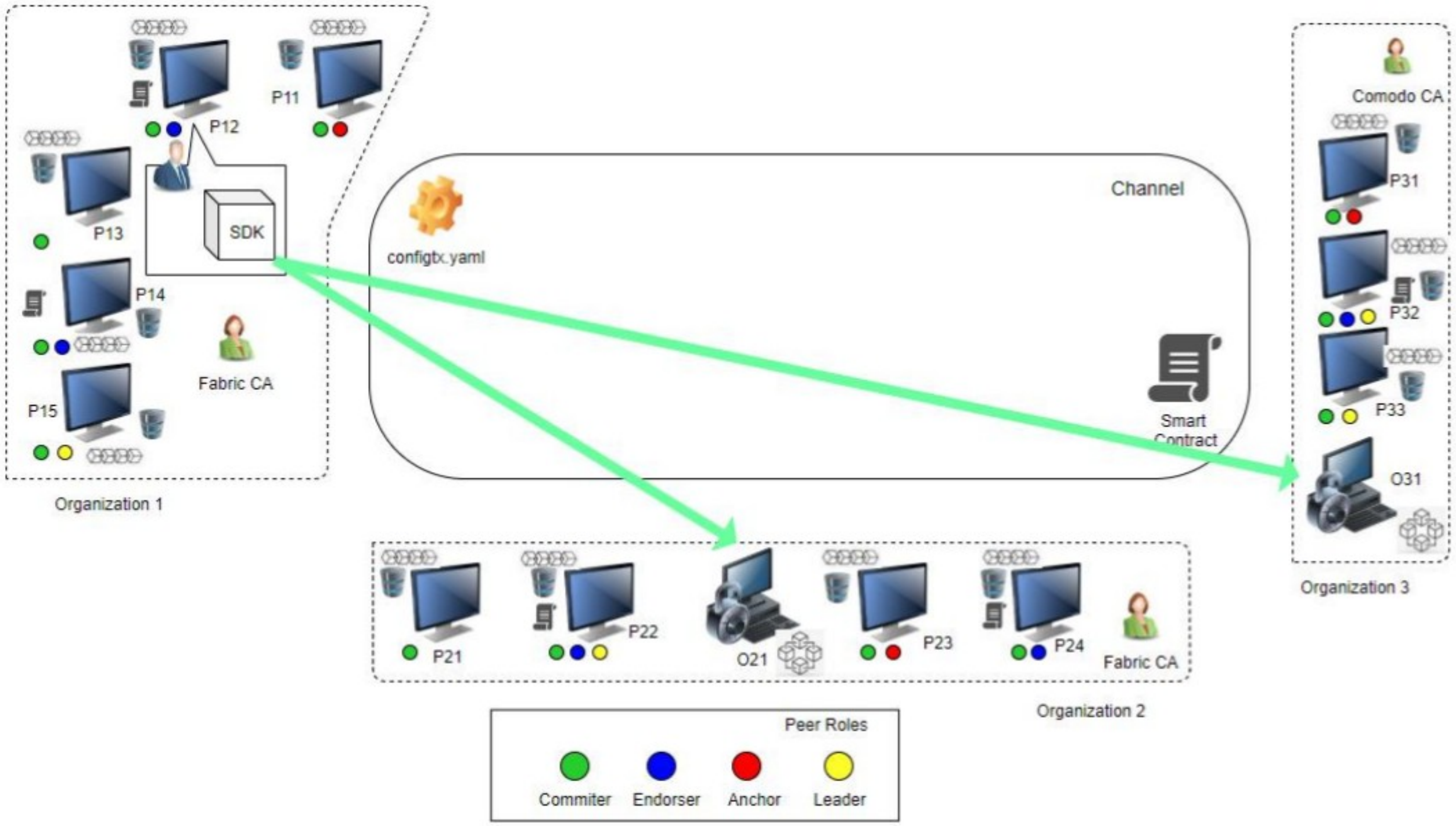


Client requests for Endorsement lists

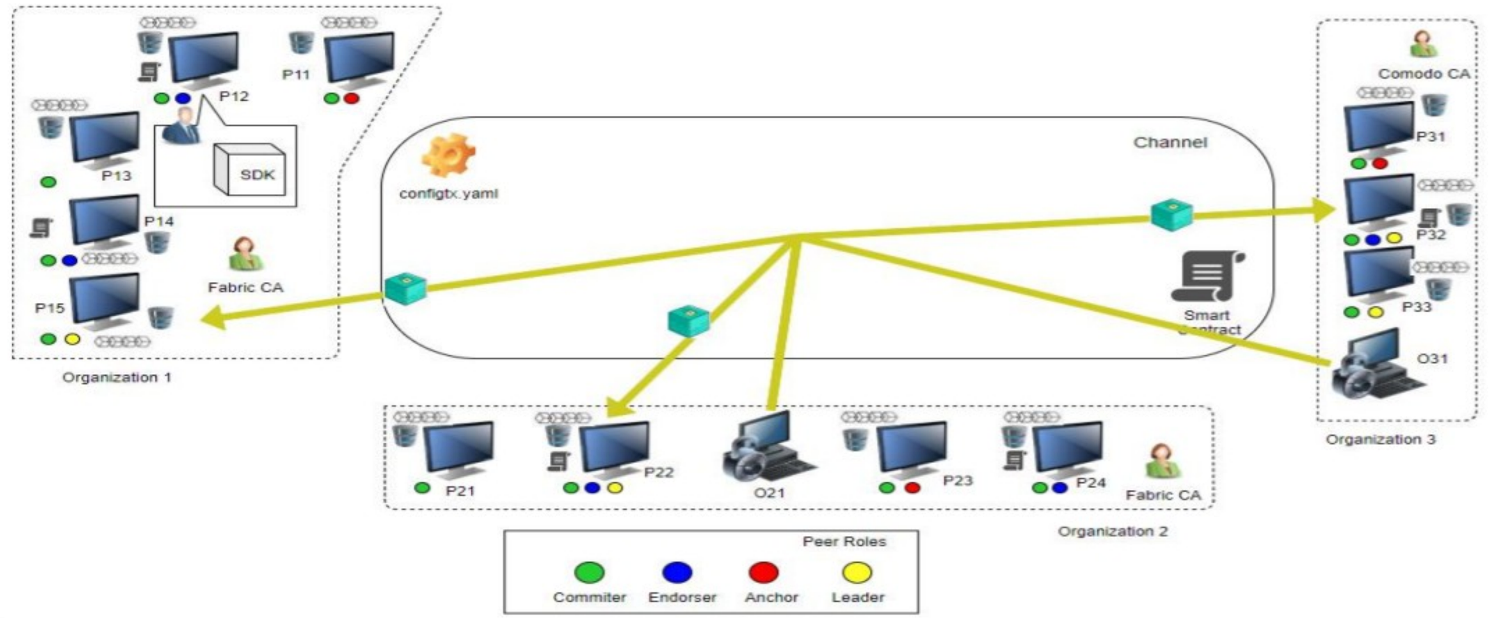
Endorsing peers verify signature & execute the transaction



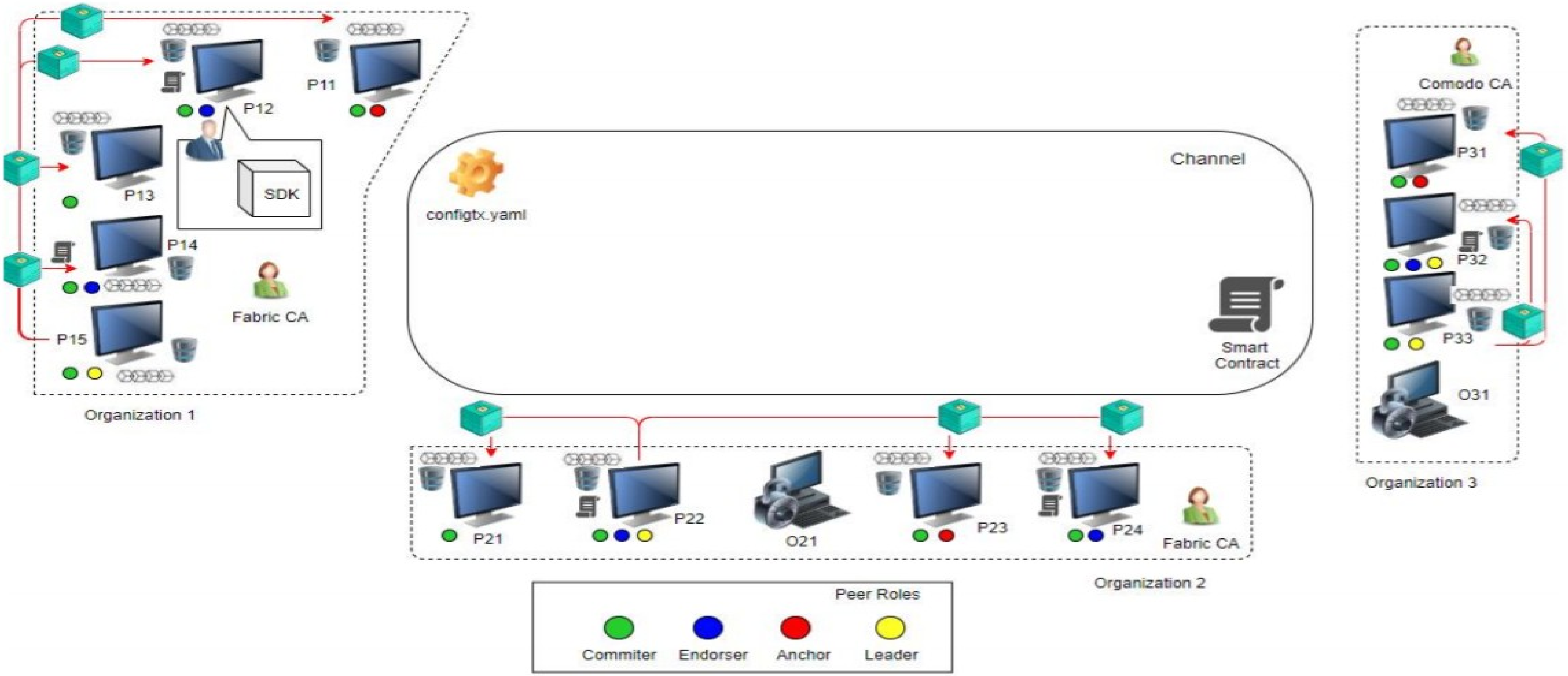
Client assembles endorsements into a transaction



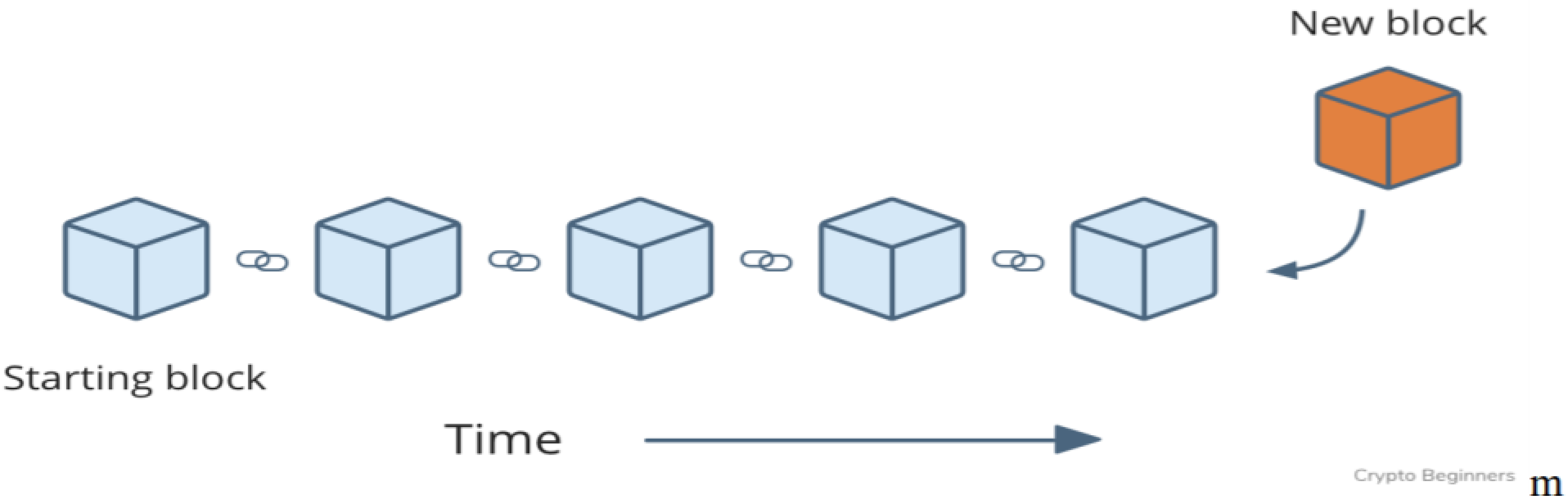
Disseminate the block to leader peers



Transaction is validated and committed



Ledger update



Client notification