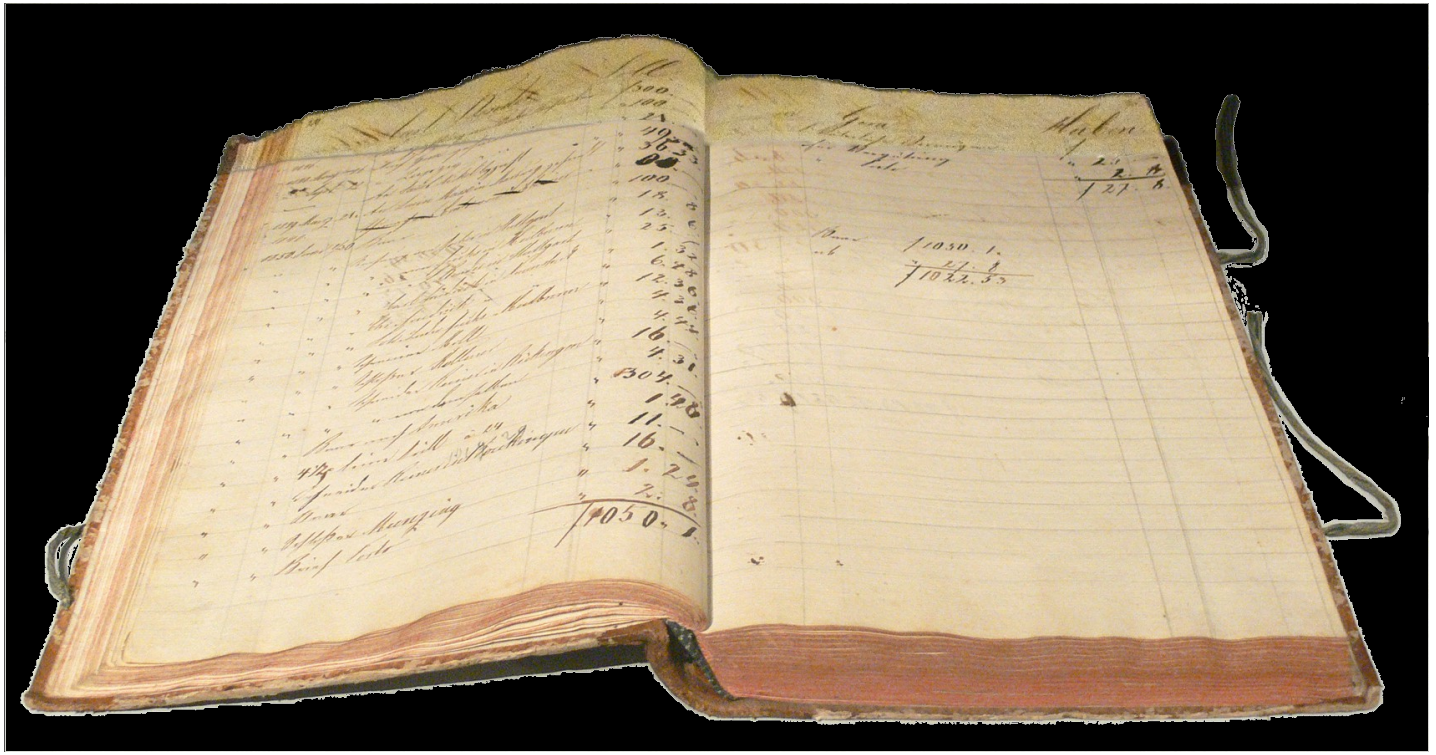
Hyperledger Day -1



1494: Pacioli Systematized Ledgers

T-Account	
(Left Side Debit)	(Right Side Credit)

… and his ledgers are *EVERYWHERE* today

Hash

Blockchain's Birth

Public Blockchain

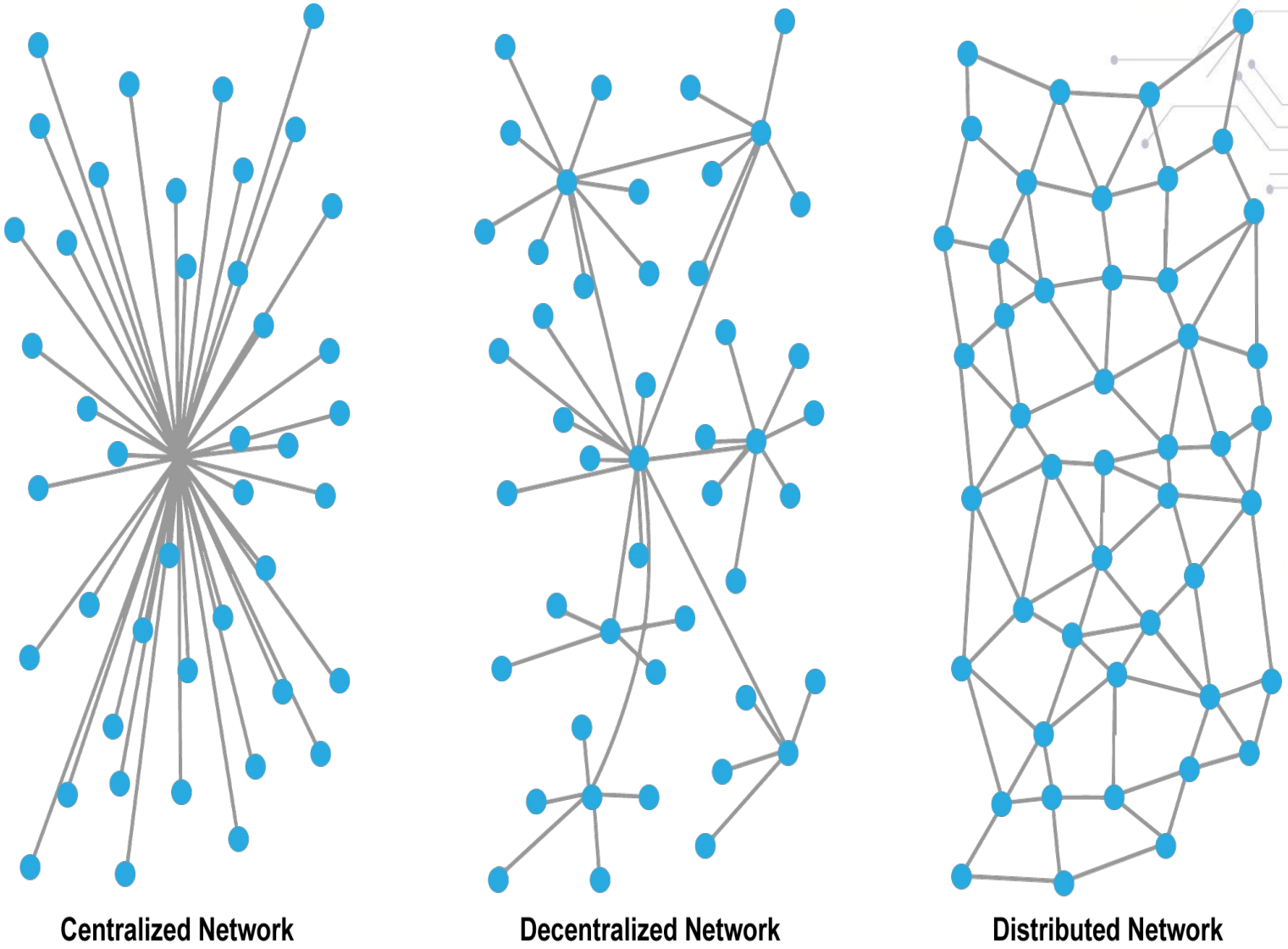
- Anyone can read without explicit authorisation
- Anyone can write without explicit permission
- More complex rules for better security
- Complex consensus algorithm
- Computationally expensive to mine & add a Block
- No one owns it
- Computational power is distributed globally
- Example: Bitcoin Blockchain, Ethereum Blockchain etc

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

Why is it called a P2P network?

Decentralized Network



Centralized Network

Decentralized Network

Distributed Network

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

Primary Purpose	Type of Blockchain
Move value between untrusted parties	Public
Move value between trusted parties	Private
Trade value between unlike things	Permissioned
Trade value of the same thing	Public
Create decentralized organization	Public or permissioned
Create decentralized contract	Public or permissioned
Trade securitized assets	Public or permissioned
Build identity for people or things	Public
Publish for public recordkeeping	Public
Publish for private recordkeeping	Public or permissioned
Preform auditing of records or systems	Public or permissioned
Publish land title data	Public
Trade digital money or assets	Public or permissioned
Create systems for Internet of Things (IoT) security	Public
Build systems security	Public

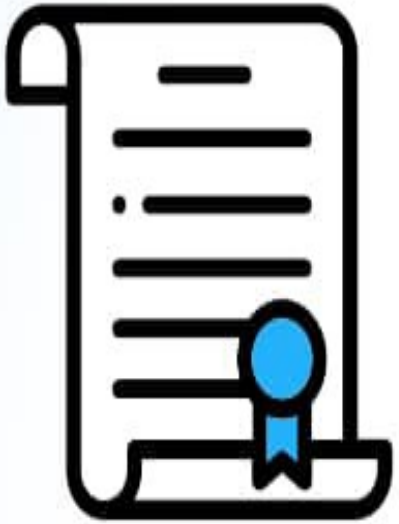
What are Smart Contracts?

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

What are Smart Contracts?

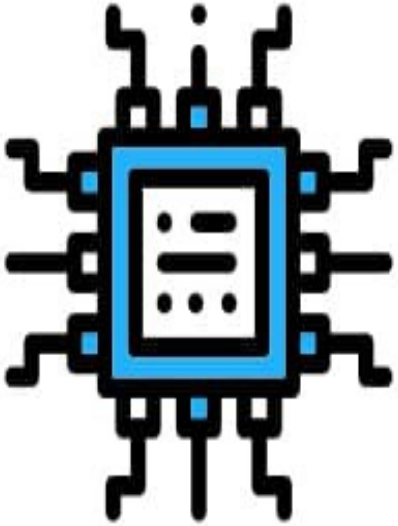
A *smart contract* is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a *contract*. Smart *contracts* allow the performance of credible transactions without third parties. One of the best things about the blockchain is that, because it is a decentralized 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



Smart Contracts are **written as code** and committed to the blockchain. The code and conditions in the contract are **publicly available** on the ledger.

2

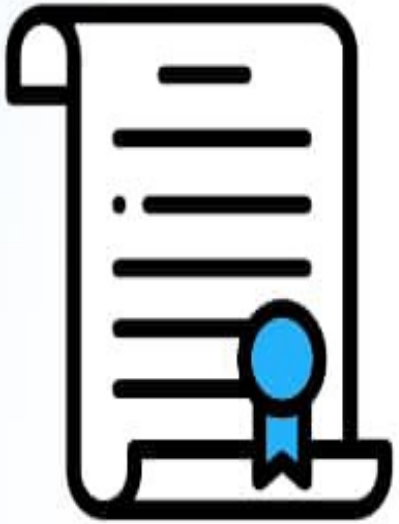


When an event outlined in the contract is triggered, like an expiration date or an asset's target price is reached-- the **code executes**.

3

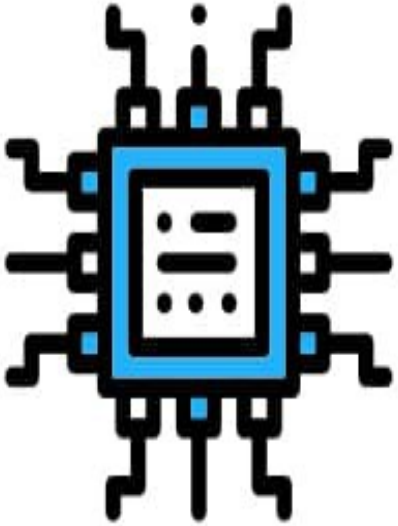
Regulators can watch contract activity on the blockchain to **understand the market** while still **maintaining the privacy** of individual actors.

1



Smart Contracts are **written as code** and committed to the blockchain. The code and conditions in the contract are **publicly available** on the ledger.

2

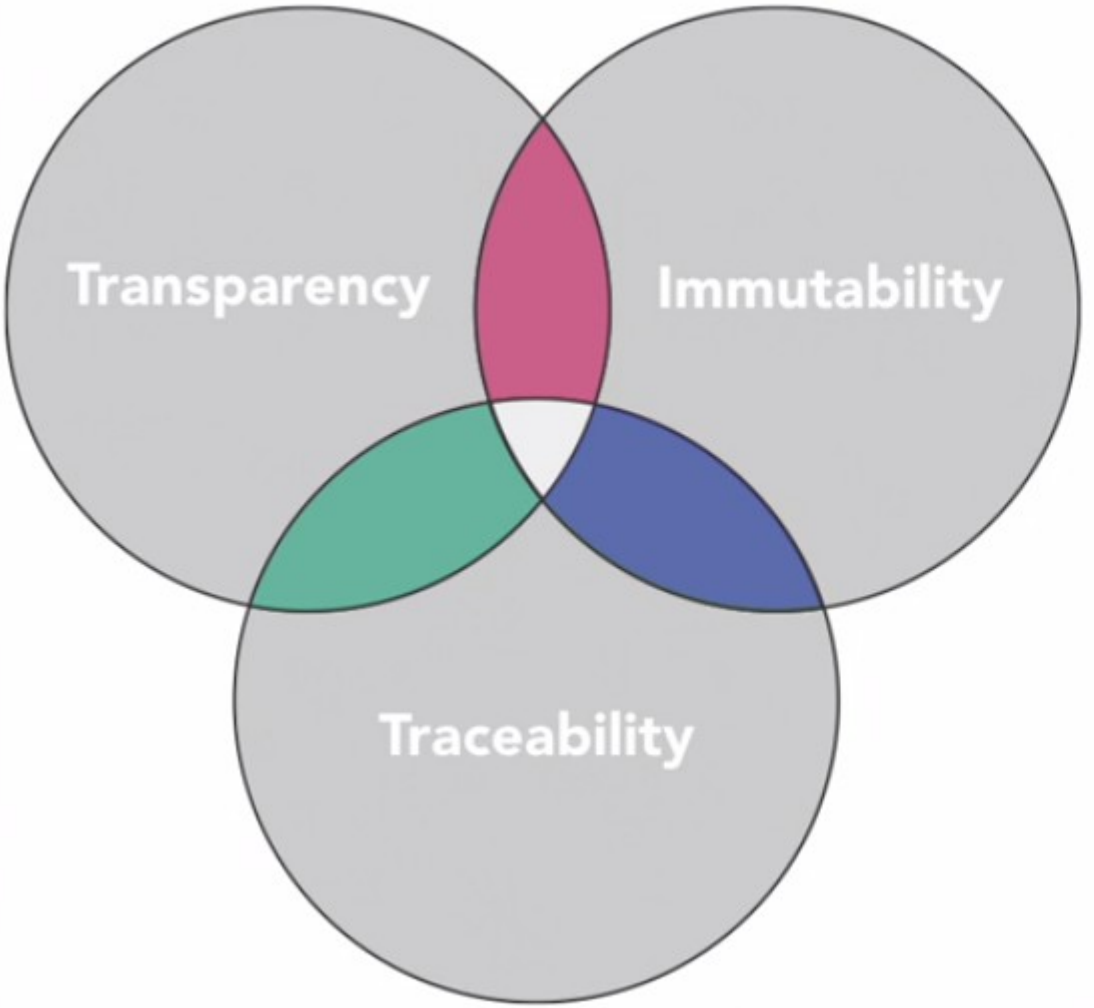


When an event outlined in the contract is triggered, like an expiration date or an asset's target price is reached-- the **code executes**.

3

Regulators can watch contract activity on the blockchain to **understand the market** while still **maintaining the privacy** of individual actors.

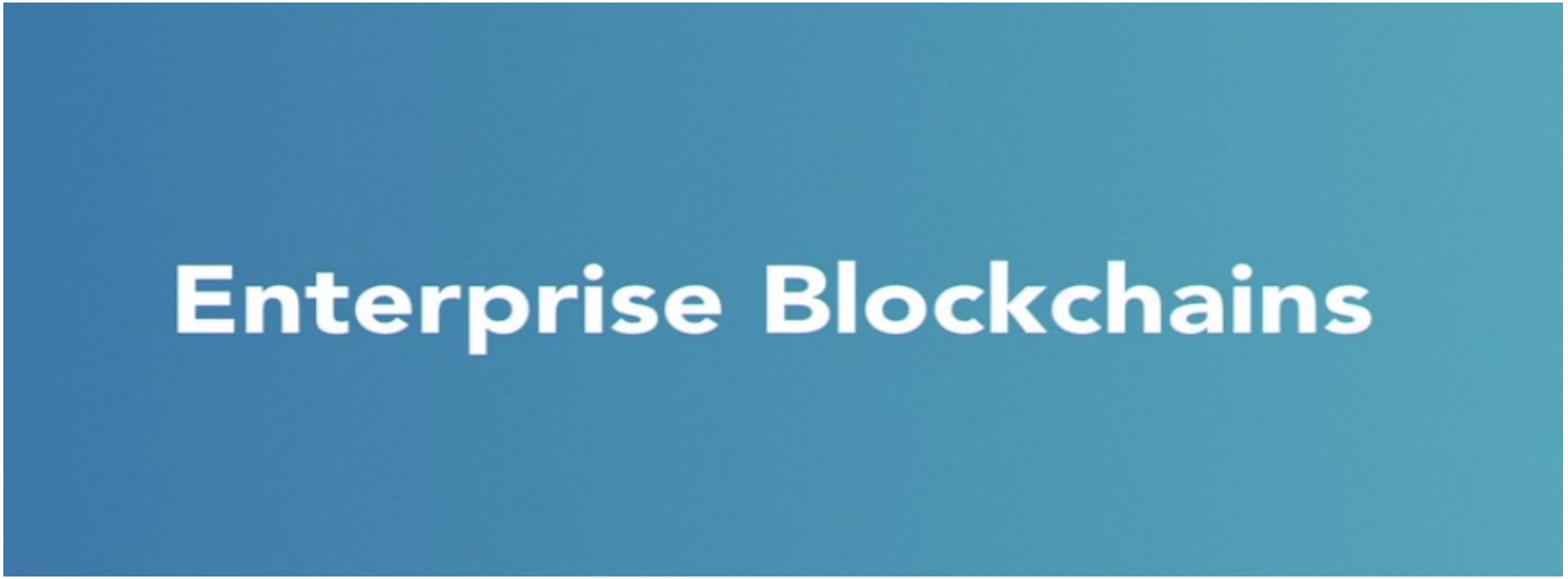
Public Vs Private Ledgers



Benefits of Public Blockchains

- Immutability
- Transparency
- Traceability

Public Vs Private Ledgers



Permissioned Blockchains

- Known participants and peers

Performance

- High performance and low latency

Performance

- High performance and low latency
- No wasted compute resources

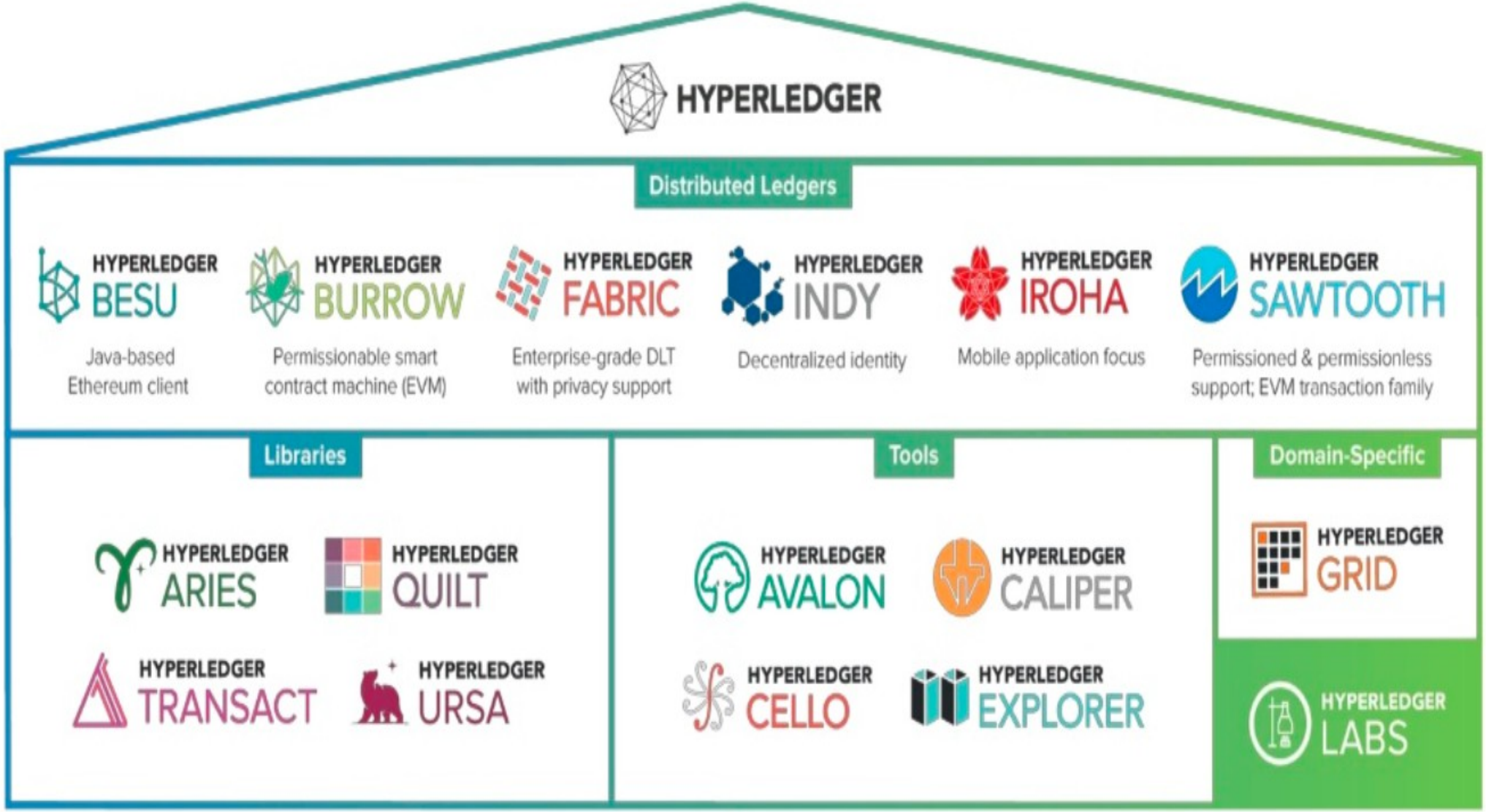
Privacy

- Secure data
- Various access levels and roles

Hyperledger

Hyperledger

Hyperledger Modular Umbrella Approach



HYPERLEDGER

WHAT IS HYPERLEDGER?

Hyperledger is an open-source umbrella project of Linux Foundation, which offers a wide range of frameworks and toolset for developers and businesses. The Hyperledger community helps enterprises to experiment with blockchain networks at ease.

WHY WAS IT CREATED?

Hyperledger was created back in 2015 to help the advancement of blockchain for enterprises by forming a consortium of far-sighted companies. At present, over 260 organizations are working with it to make sure blockchain becomes industry-grade technology.

IS HYPERLEDGER OPEN SOURCE? BUT WHY?

HYPERLEDGER IS AN OPEN-SOURCE PLATFORM.

- More competitive capabilities and features
- There isn't any vendor lock-in, helping customers to switch easily

THEY CHOOSE TO MAKE IT OPEN-SOURCE FOR FIVE KEY REASONS -

- High-end solutions
- Quick bug fixes and customization for the betterment
- The total cost of ownership is much lower

BENEFITS OF HYPERLEDGER

Keep Up With Developments

Using a collaborative environment Hyperledger makes sure the newer participants quickly catch up with previous developments and joins it for the betterment.

Enhanced Productivity Using Specialism

By encouraging specialization, every participant is gaining more expertise, more value, and efficient productivity.

Collaborative Approach

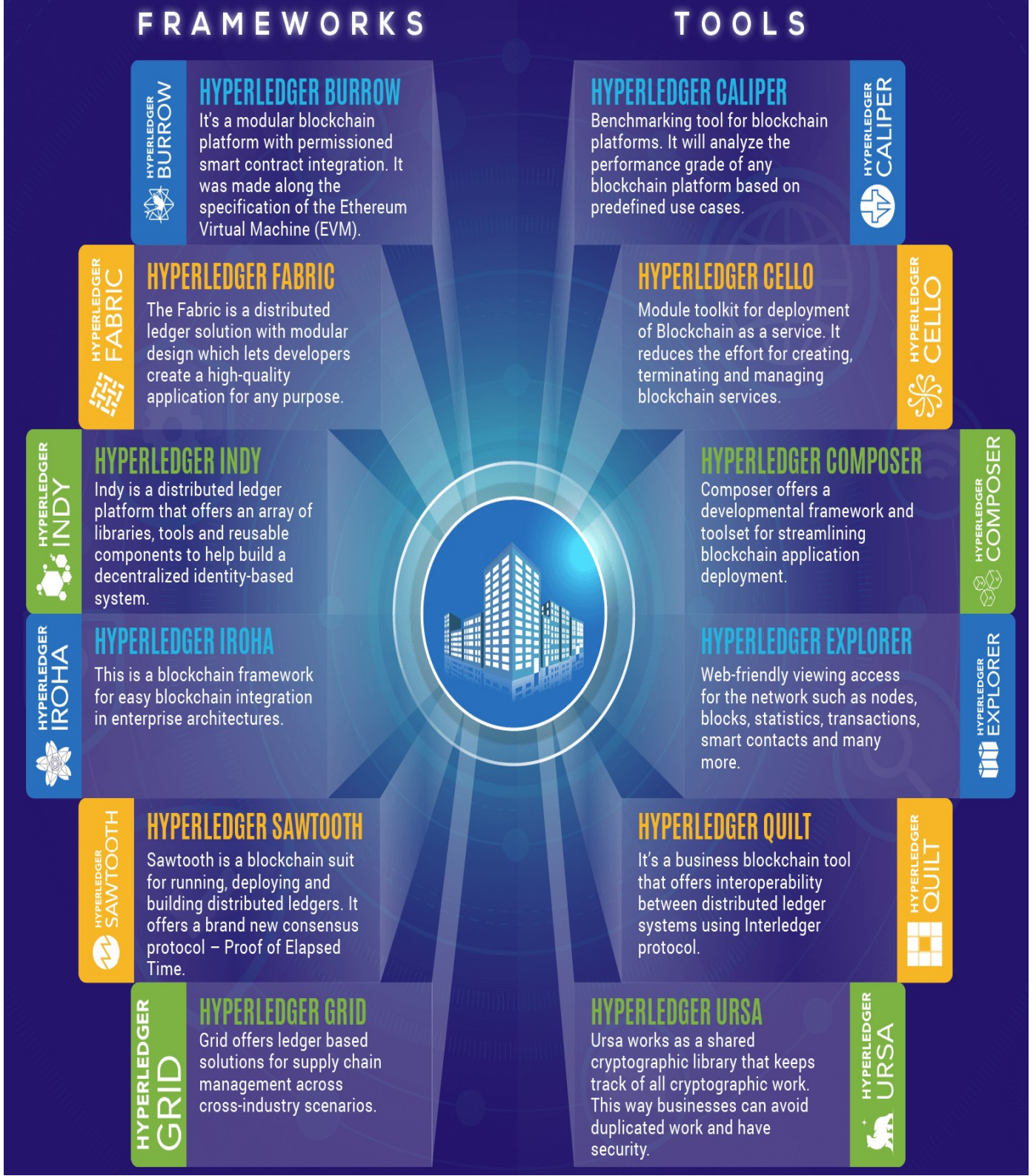
Hyperledger promotes collaboration to streamline new projects. Instead of competing, companies are joining forces to nurture their skills.

Superior Value Control of Coding

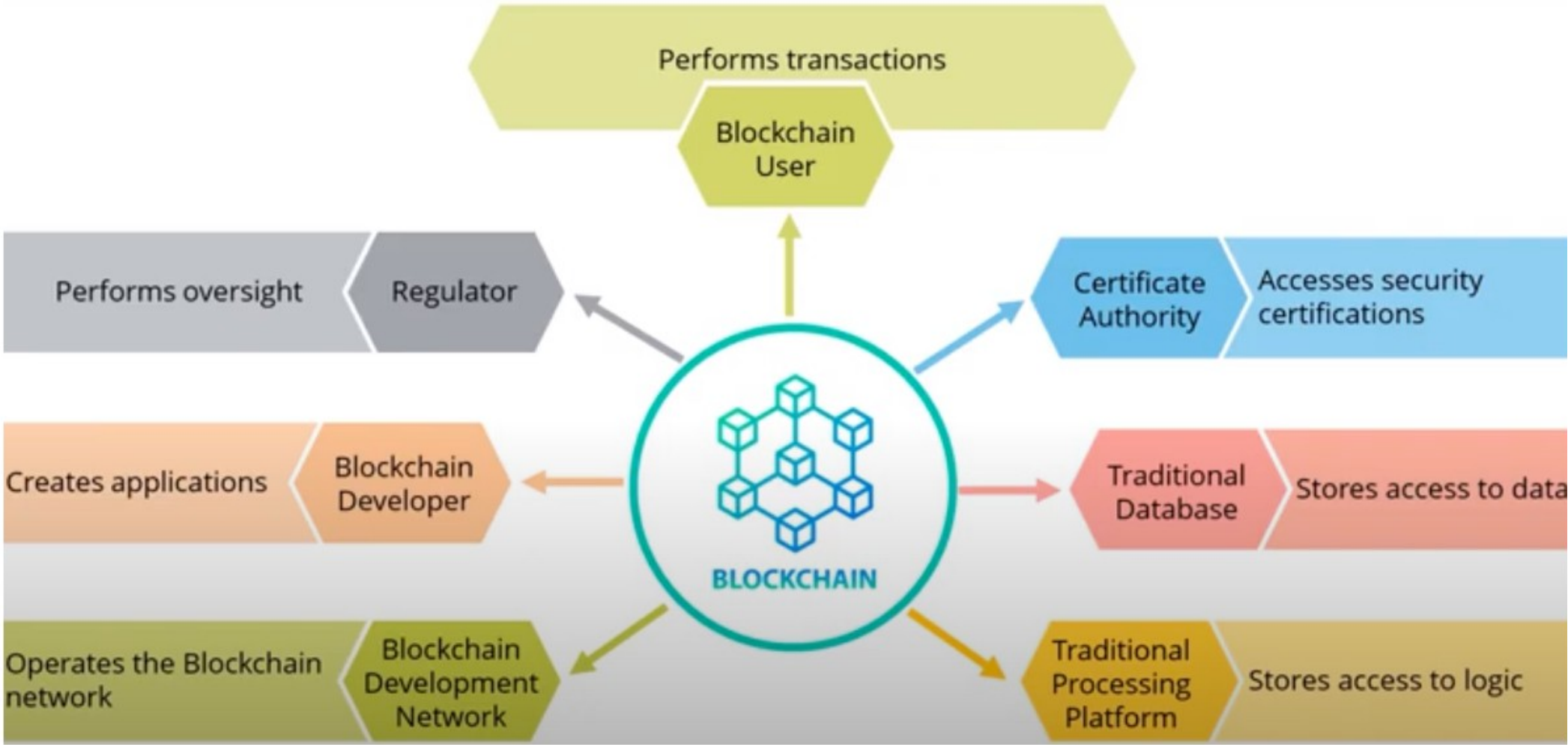
As the platform is open-sourced, developers are free to overview the code and criticize. This ensures a better quality output without any bug in the coding.

Handling Intellectual Property

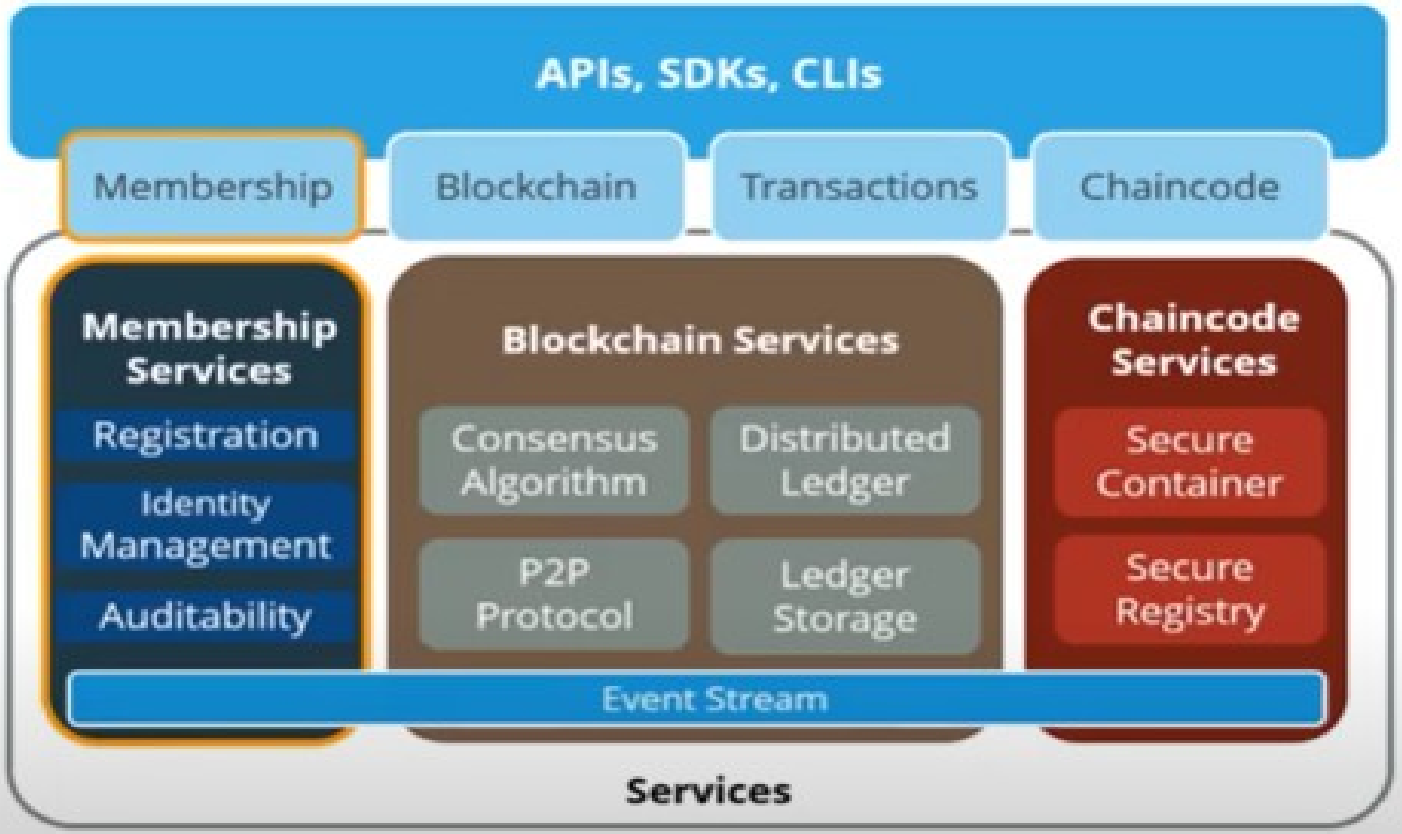
As all the organizations are working with Hyperledger, the company makes sure that no one faces any legal issues regarding intellectual properties.

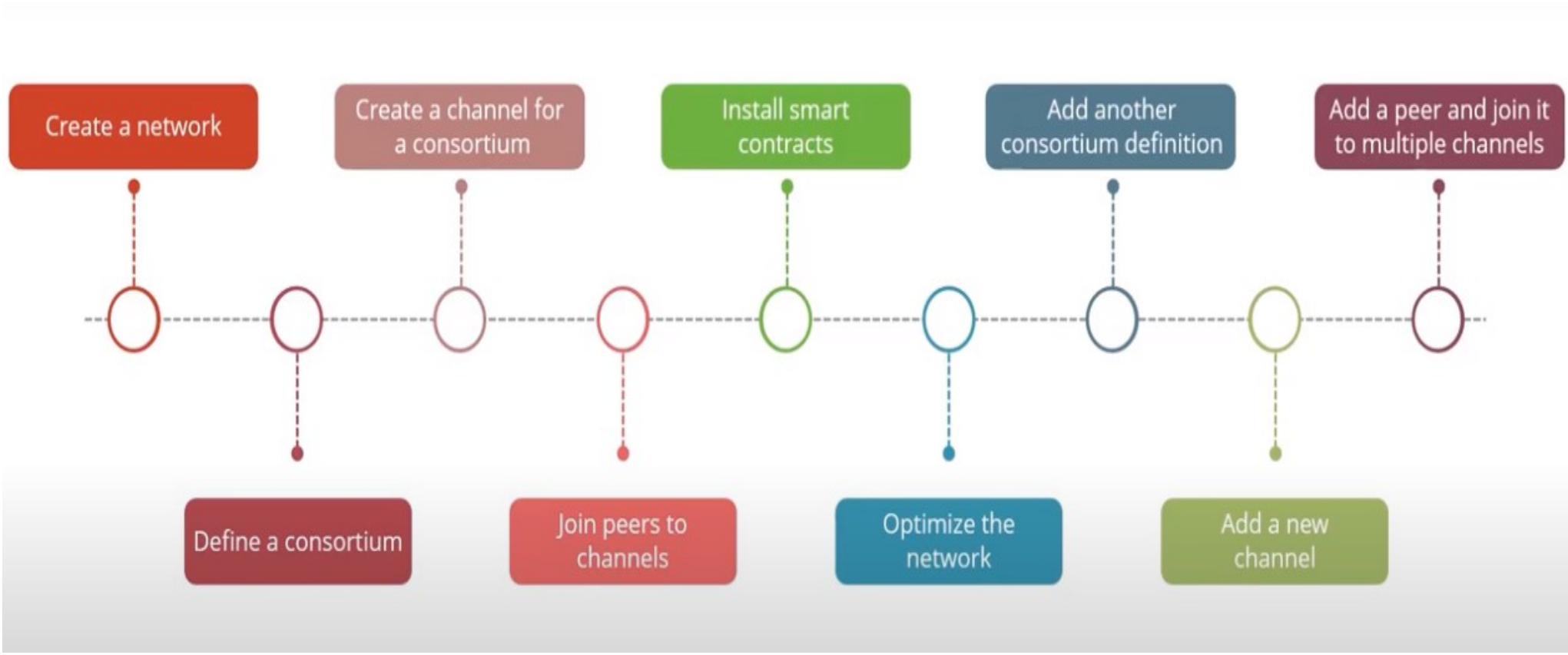

FRAMEWORKS
TOOLS
HYPERLEDGER BURROW
HYPERLEDGER BURROW
It's a modular blockchain platform with permissioned smart contract integration. It was made along the specification of the Ethereum Virtual Machine (EVM).
HYPERLEDGER CALIPER
Benchmarking tool for blockchain platforms. It will analyze the performance grade of any blockchain platform based on predefined use cases.
HYPERLEDGER CALIPER
HYPERLEDGER FABRIC
HYPERLEDGER FABRIC
The Fabric is a distributed ledger solution with modular design which lets developers create a high-quality application for any purpose.
HYPERLEDGER CELLO
Module toolkit for deployment of Blockchain as a service. It reduces the effort for creating, terminating and managing blockchain services.
HYPERLEDGER CELLO
HYPERLEDGER INDY
HYPERLEDGER INDY
Indy is a distributed ledger platform that offers an array of libraries, tools and reusable components to help build a decentralized identity-based system.
HYPERLEDGER COMPOSER
Composer offers a developmental framework and toolset for streamlining blockchain application deployment.
HYPERLEDGER COMPOSER
HYPERLEDGER IROHA
HYPERLEDGER IROHA
This is a blockchain framework for easy blockchain integration in enterprise architectures.
HYPERLEDGER EXPLORER
Web-friendly viewing access for the network such as nodes, blocks, statistics, transactions, smart contacts and many more.
HYPERLEDGER EXPLORER
HYPERLEDGER SAWTOOTH
HYPERLEDGER SAWTOOTH
Sawtooth is a blockchain suit for running, deploying and building distributed ledgers. It offers a brand new consensus protocol – Proof of Elapsed Time.
HYPERLEDGER QUILT
It's a business blockchain tool that offers interoperability between distributed ledger systems using Interledger protocol.
HYPERLEDGER QUILT
HYPERLEDGER GRID
HYPERLEDGER GRID
Grid offers ledger based solutions for supply chain management across cross-industry scenarios.
HYPERLEDGER URSA
Ursa works as a shared cryptographic library that keeps track of all cryptographic work. This way businesses can avoid duplicated work and have security.
HYPERLEDGER URSA

Participants in Hyper Ledger



Hyperledger Architecture




Create a network
Create a channel for a consortium
Install smart contracts
Add another consortium definition
Add a peer and join it to multiple channels
Define a consortium
Join peers to channels
Optimize the network
Add a new channel

Shortcomings of Existing Blockchains

Shared Ledger Database

Blockchain allows multiple different parties to securely interact with the same universal source of truth

Finance

Streamline settlement, improve liquidity, increase transparency, and new products/markets

Healthcare

Use disparate processes, increase data flow & liquidity, reduce costs, and improve patient experience & outcomes

Supply Chain

Track parts & service provenance, ensure authenticity of goods, block counterfeits, reduce conflicts

Hyperledger Goals

Create enterprise grade software
open source, distributed ledger frameworks & code bases to support business transactions

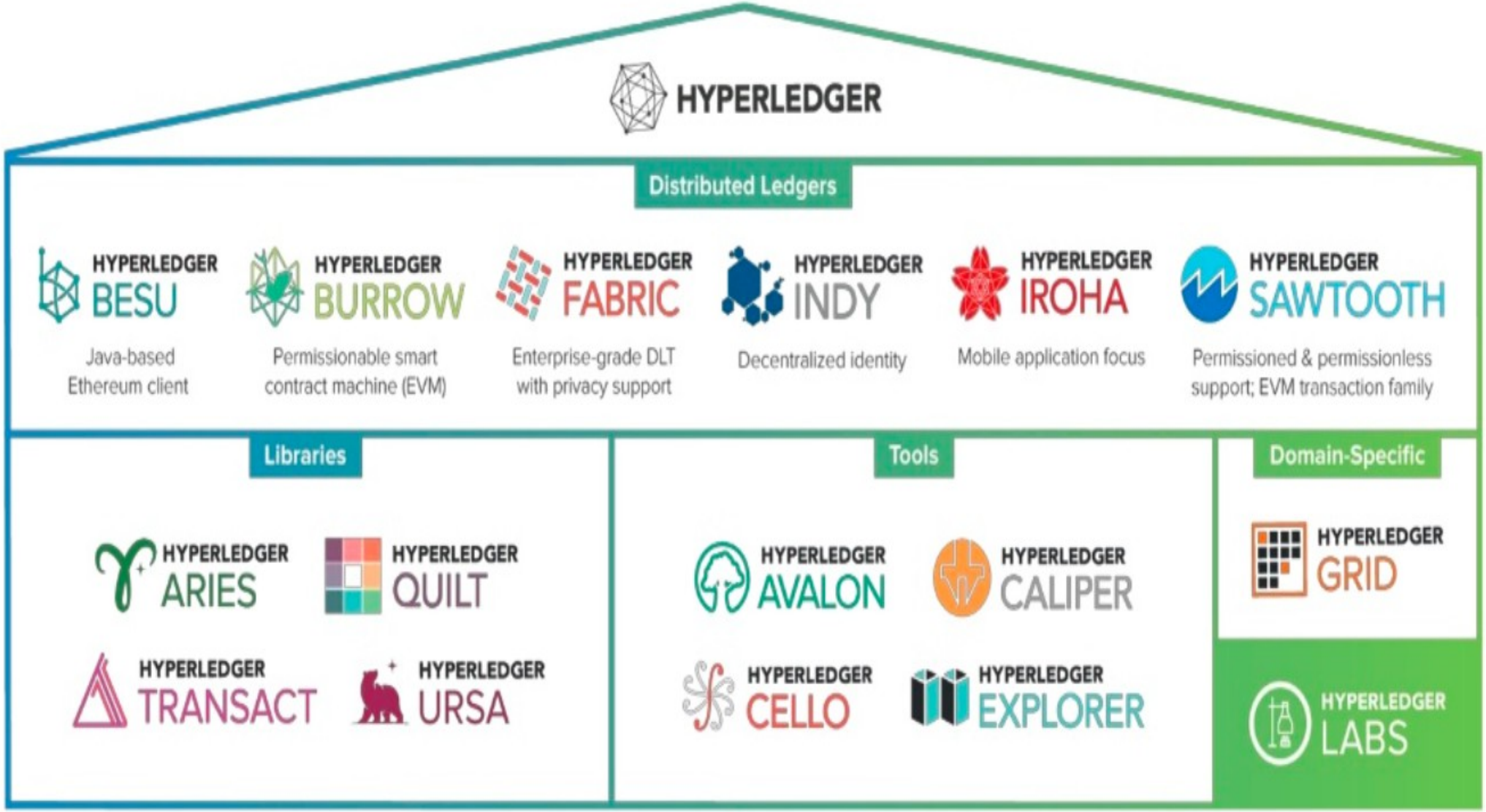
Provide community-driven infrastructures
that are open, neutral and supported by technical and business governance

Build technical communities
to develop blockchain and shared ledger POCs, use cases, field trials and deployments

Educate the public
about the market opportunity for blockchain technology

Promote our communities
taking a toolkit approach with many platforms and frameworks

Hyperledger Modular Umbrella Approach



Benefits

Flexible Modification of Any Component

Common Functional Modules and Defined Interfaces

Re-use of Common Building Blocks

Extensible Codebases

Diverse Developer Community

Rapid Experimentation

Comparing Hyperledger with Bitcoin and Ethereum

	Bitcoin	Ethereum	Hyperledger Frameworks
Cryptocurrency-based	Yes	Yes	No
Permissioned	No	No	Yes*
Pseudo-anonymous	Yes	Yes	No
Auditable	Yes	Yes	Yes
Modularity	No	No	Yes
Smart contracts	No	Yes	Yes
Consensus protocol	PoW	PoW	Various#

* Sawtooth can be configured to be permissionless.

Key Hyperledger consensus protocols are Apache Kafka in Hyperledger Fabric, PoET and RAFT in Hyperledger Sawtooth, RBFT (Plenum) in Hyperledger Indy, Tendermint in Hyperledger Burrow, and Yet Another Consensus (YAC) in Hyperledger Iroha.

Case Study: Cross-Border Payments

The Challenge

Transferring money across international borders is still complicated, time consuming and expensive.

The Collaboration

A global team of developers from Hyperledger members SWIFT, ANZ, BNP Paribas, BNY Mellon and Wells Fargo create a cross-border POC. built with Hyperledger Fabric.

The Technology

The blockchain trial was built on Hyperledger Fabric and is now ready for its next phase of testing.

ANZ BNP PARIBAS BNY MELLON SWIFT WELLS FARGO

Case Study: Diamond Supply Chain

The Challenge

The Kimberley Process Certification Scheme established in 2003 to prevent conflict diamonds is a long, paperwork-heavy process with a history of fraud from missing documents.

The Collaboration

Hyperledger members SAP Ariba and IBM are collaborating with Everledger on a pilot to prevent blood diamonds from entering the supply chain.

The Technology

The distributed ledger diamond track and trace system using Hyperledger Fabric v1.0 allows everyone in the industry to write to it, from miners, distributors and retailers, using the light pattern that is unique to every diamond to create an ID.

everledger IBM SAP

Case Study: Green Assets Management

The Challenge

Generating carbon assets more efficiently, helping to build a green, low-carbon and environmentally-friendly future in China.

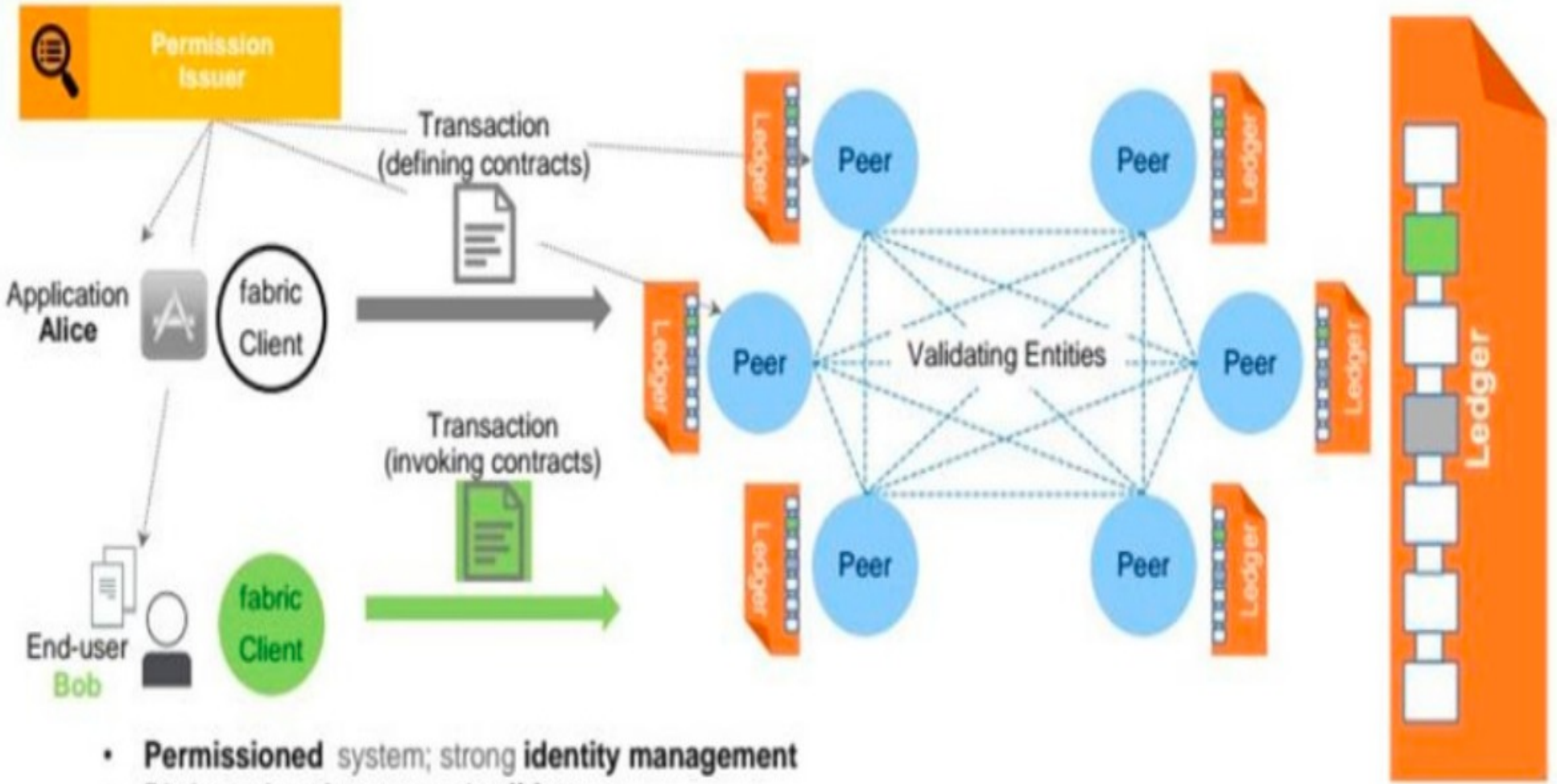
The Collaboration

General Hyperledger member Energy Blockchain Labs partnered with Premier member IBM on the world's first blockchain-based green assets management platform. based on Hyperledger Fabric.

The Technology

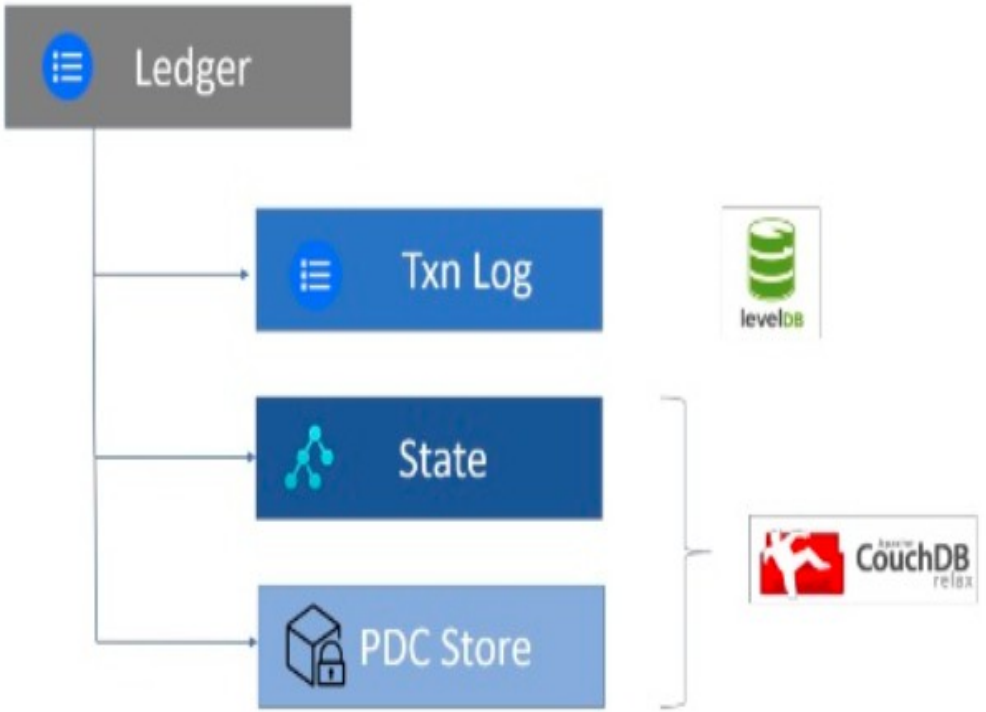
Blockchain technology, like the use of Hyperledger Fabric here, is expected to become an important means for effective control of carbon emissions in China, the world's largest source of carbon emissions. Carbon asset development, is one of the most popular ways of encouraging enterprises to decrease emissions and use low carbon emission technology.

Permissioned Network



- **Permissioned** system; strong **identity management**
- Distinct roles of **users**, and **validators**
- Users **deploy** new pieces of code (chaincodes) and **invoke** them through **deploy & invoke** transactions
- Validators evaluate the effect of a transaction and reach consensus over the new version of the **ledger**
- **Ledger** = total order of transactions + hash (global state)
- **Pluggable consensus** protocol, currently PBFT & Sieve

A Hyperledger Fabric ledger is a blockchain storing the immutable, sequenced transactions and the current state



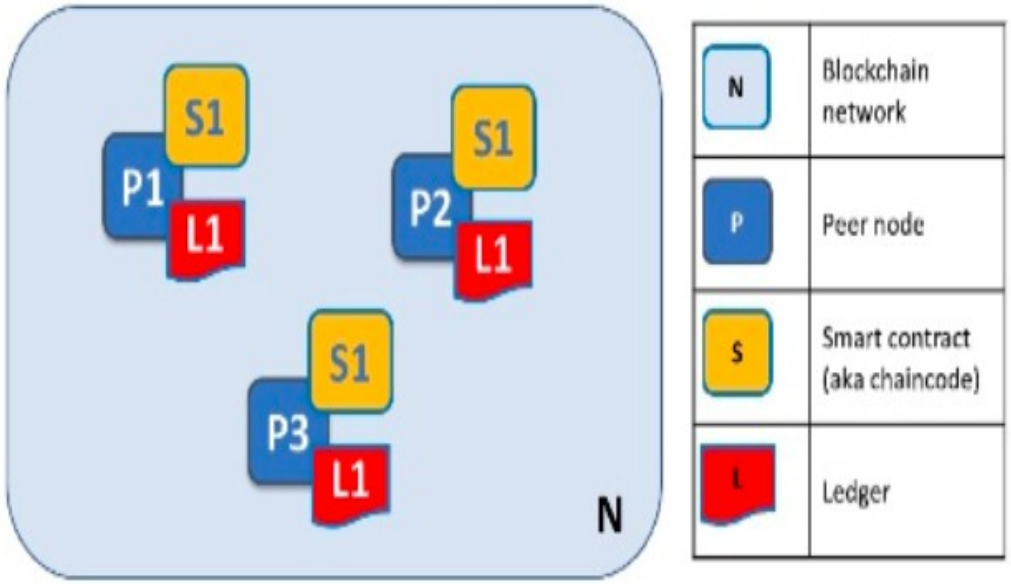
PDC = Private Data Collection

- The ledger has a replaceable data store for the world state
- By default, the world state is a LevelDB database containing key-value pairs
  - Production system normally uses CouchDB
- The transaction log does not need to be pluggable
- It simply records the before and after values of the ledger database being used by the blockchain network

Chaincode defines assets & the business logic in the form of transaction instructions for modifying the assets

- Whereas a ledger holds facts about the current and historical state of a set of business objects, a smart contract defines the executable logic that generates new facts that are added to the ledger
- In general, a smart contract defines the transaction logic that controls the lifecycle of a business object contained in the world state
- A smart contract is then packaged into a chaincode which is then deployed to a blockchain network.
- Chaincodes execute against the ledger's current state database and are initiated through a transaction proposal and result in a set of key-value writes (write set) that can be submitted to the network and applied to the ledger on all peers

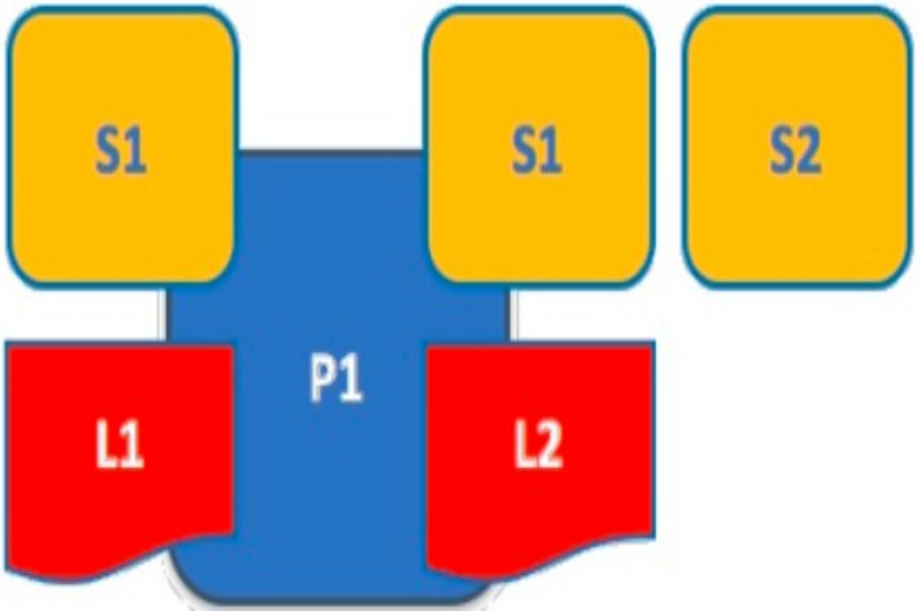
A blockchain is comprised of peer nodes, each of which can hold copies of ledgers and copies of smart contracts



N	Blockchain network
P	Peer node
S	Smart contract (aka chaincode)
L	Ledger

- A blockchain network is comprised primarily of a set of peer nodes (or, simply, peers)
- Peers are a fundamental element of the network because they host ledgers and smart contracts
- Smart contracts and ledgers are used to encapsulate the shared processes and shared information in a network, respectively

A peer can host multiple ledgers and each ledger can have one or more chaincodes applicable to it



- A peer is able to host more than one ledger, which is helpful because it allows for a flexible system design
- Peers host one or more ledgers, and each ledger has zero or more chaincodes that apply to them

Consensus is a full verification cycle

- In distributed ledger technology, consensus has recently become synonymous with a specific algorithm, within a single function
- However, consensus encompasses more and this differentiation is highlighted in Hyperledger Fabric through its fundamental role in the entire transaction flow
  - Proposal
  - Endorsement
  - Ordering
  - Validation
  - Commitment
- In a nutshell, consensus is defined as the full verification cycle of the correctness of a set of transactions comprising a block

Food Supply Chain Transparency in Walmart

https://www.hyperledger.org/resources/publications/walmart-case-study


GERSON
How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric

Challenge

- When an outbreak of a food-borne disease happens, it can take days, if not weeks, to find its source.
- Better traceability could help save lives by allowing companies to act faster and protect the livelihoods of farmers by only discarding produce from the affected farms.

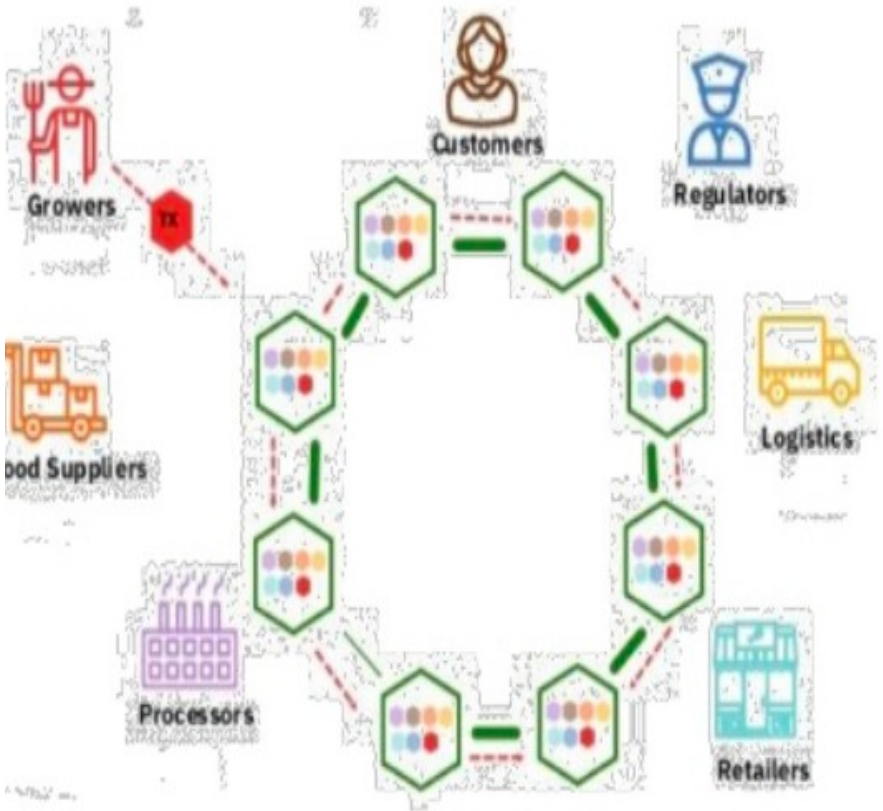
Approach

- Walmart created a food traceability system based on Hyperledger Fabric.
- Two proof of concept projects.
- One project was about tracing mangos sold in Walmart's US stores.
- The other aimed to trace pork sold in its China stores.

Results

- For pork, Walmart could upload certificates of authenticity to the blockchain, bringing more trust to the system.
- For mangoes, the time needed to trace their provenance went from 7 days to 2.2 seconds.
- Walmart can now trace the origin of over 25 products from 5 different suppliers.

Food traceability needs to be open as it involves a large number of participants and possibly different technologies

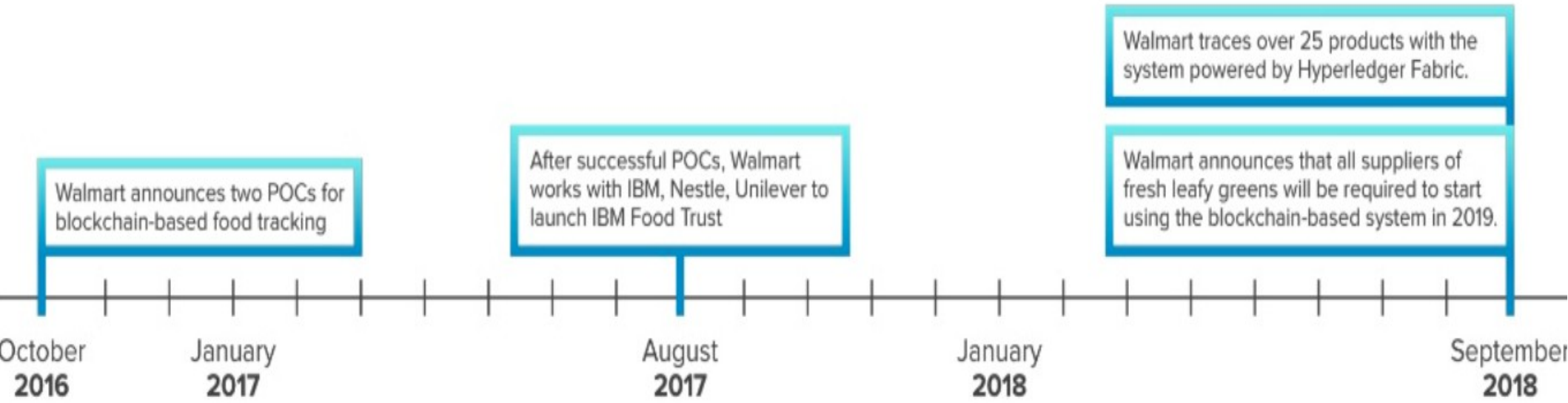


- After reviewing different blockchain technologies, Walmart decided to go with Hyperledger Fabric because it met most of their needs plus being an enterprise-grade solution supporting permissioned networks
- The team also found it important to work with an open-source, vendor-neutral blockchain
- Since the food traceability system was meant to be used by many parties, including Walmart's suppliers and even direct competitors, the technology ecosystem underlying it needed to be open

In October 2016, Walmart announced the two projects: one for pork sold in China and one for tracing mangos sold in US

- For pork in China, it allowed uploading certificates of authenticity to the blockchain, bringing more trust to a system where that used to be a serious issue
- For the mango POC, the team started by creating a benchmark
  - The leader bought a packet of sliced mangoes at a nearby Walmart store and asked his team to identify which farm they had come from – as fast as possible
  - The team started calling and emailing distributors and suppliers, and eventually had an answer almost seven days later
- Walmart worked with GS1 to define the data attributes for upload to the blockchain and IBM wrote the chaincode
- Suppliers used new labels & uploaded their data through a web-based interface

From POC to production, from Walmart to IBM Food Trust



- Walmart wanted to make sure that many players could be involved
  - Walmart reached out to other food companies, including other retailers
- Wal-Mart collaborated with IBM and others to set up IBM Food Trust, involving prominent players in the food industry, like Nestle and Unilever

Implementation Tips

1. Let the business lead the project, not the IT department.
2. Understand the business case deeply. Make sure that you know and can explain why blockchain is the right solution.
3. Think about all the different departments that will be affected by the projects. Meet with these stakeholders early on and explain what you are trying to do.
4. People don't get inspired by technology, but by a vision. For Walmart, it was the story of mangoes: 7 days against 2.2 seconds with blockchain.
5. Participate in forums that allow you to speak to other companies who have launched similar projects successfully.
6. Start small, with a POC.

Important Elements

Channel

Some Points To Consider :

- One can have multiple channels across a consortium.
- One can have Multiple chain codes across channels.
- One can make a channel policy and endorsement policy.
- One can use either level DB or CouchDB as a world state store.
- One can use private data collections which reduce no of channels
- Support for cryptogen or Fabric certificate authority or own

In general Certificate Authority, issues & manages certificates for users. Hyperledger Fabric has CA which is the default certificate authority for Fabric but it is completely pluggable. CA can handle the requests for registration and enrollments of user identities.

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

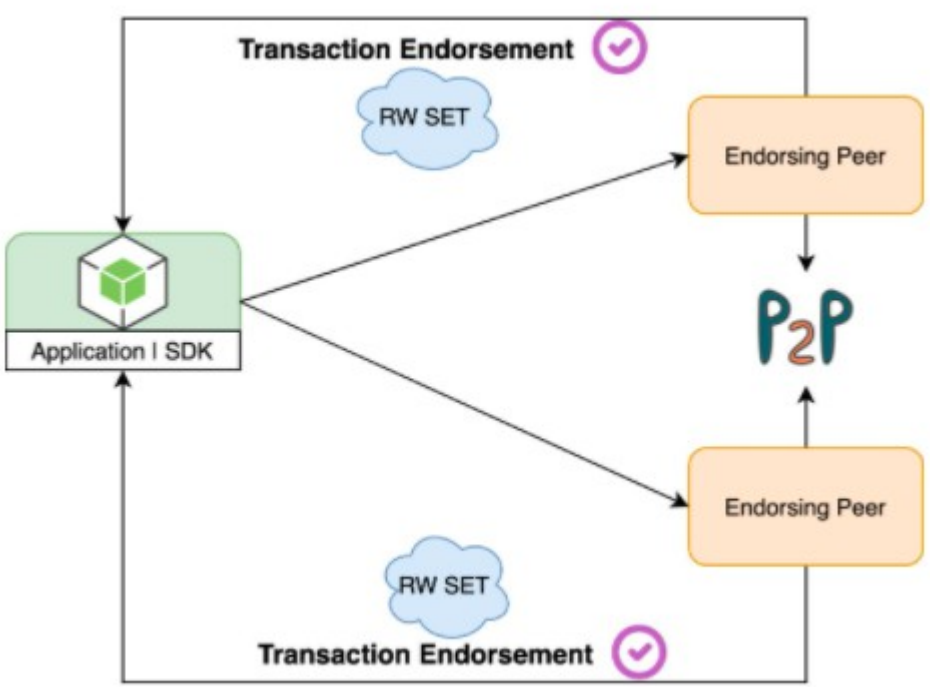
2) Ordering Transactions in to blocks ready to commit by peers

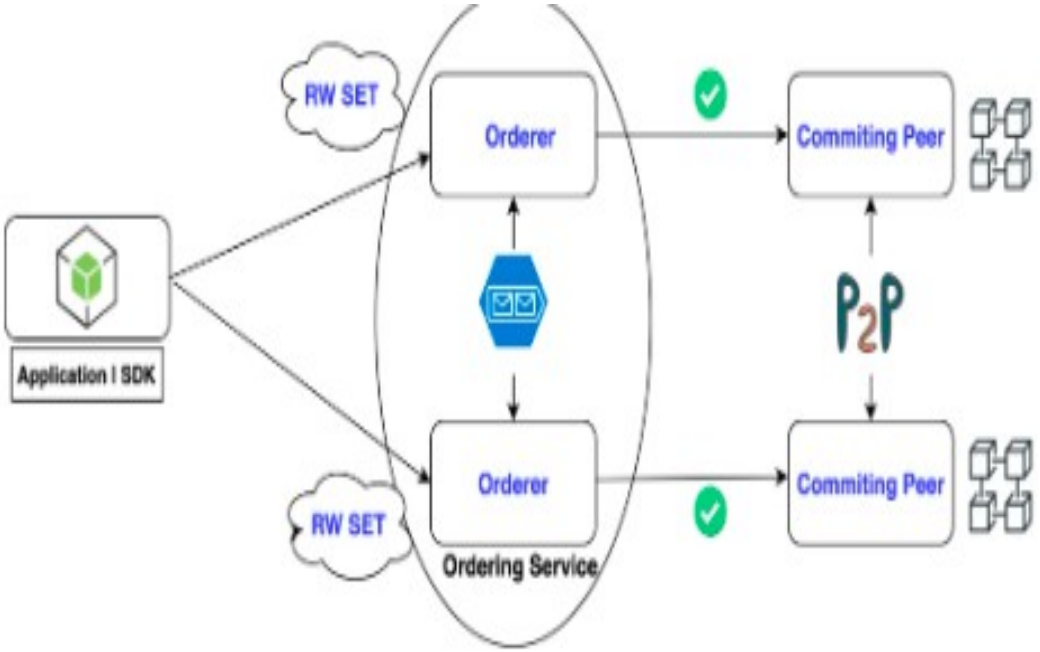
3) Validate the endorsement

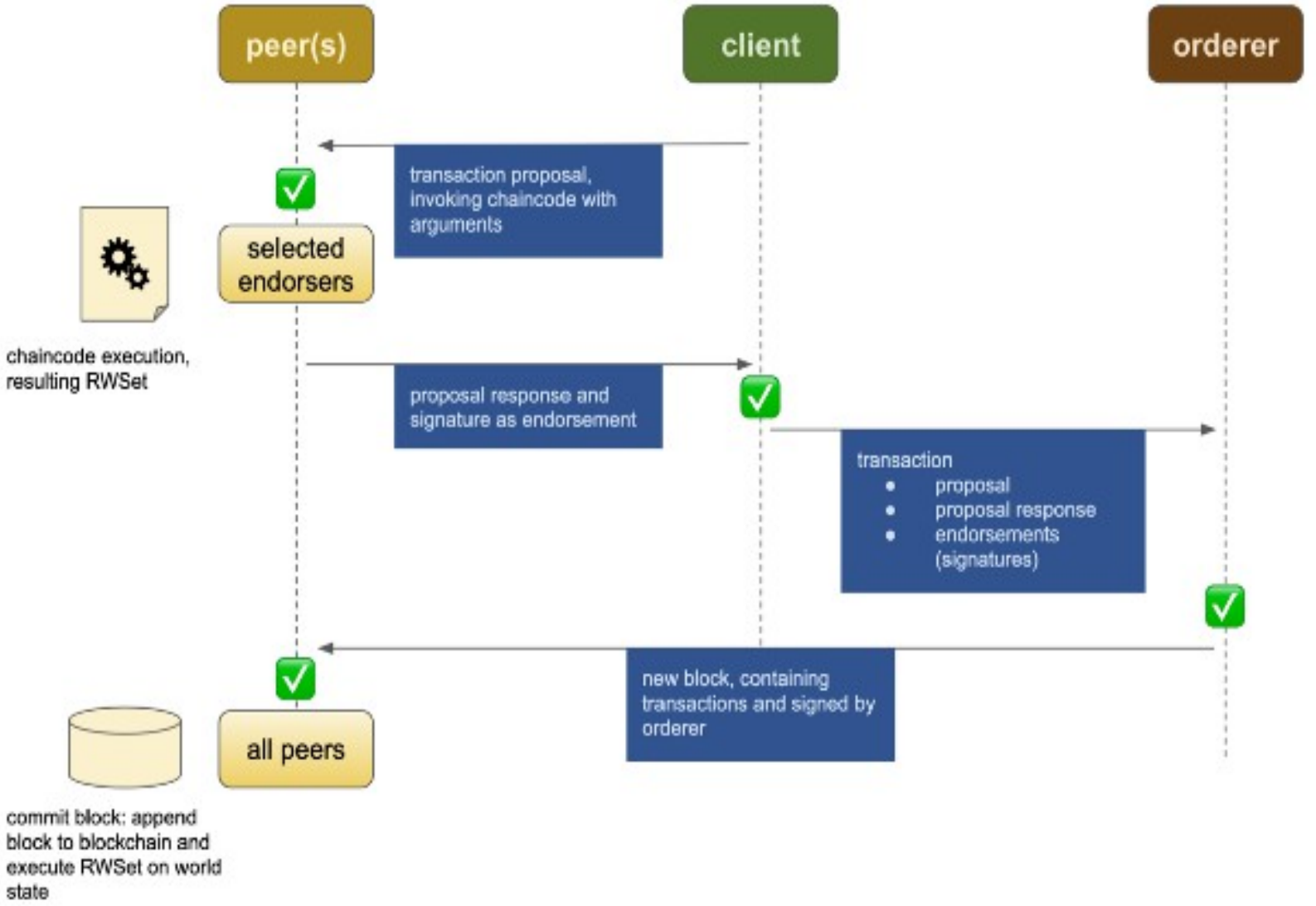
HF allows users from organisations to define policies around the lifecycle of chaincode.

Transaction Flow

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






peer(s)
client
orderer
transaction proposal, invoking chaincode with arguments
selected endorsers
chaincode execution, resulting RWSet
proposal response and signature as endorsement
transaction
proposal
proposal response
endorsements (signatures)
new block, containing transactions and signed by orderer
all peers
commit block: append block to blockchain and execute RWSet on world state

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)

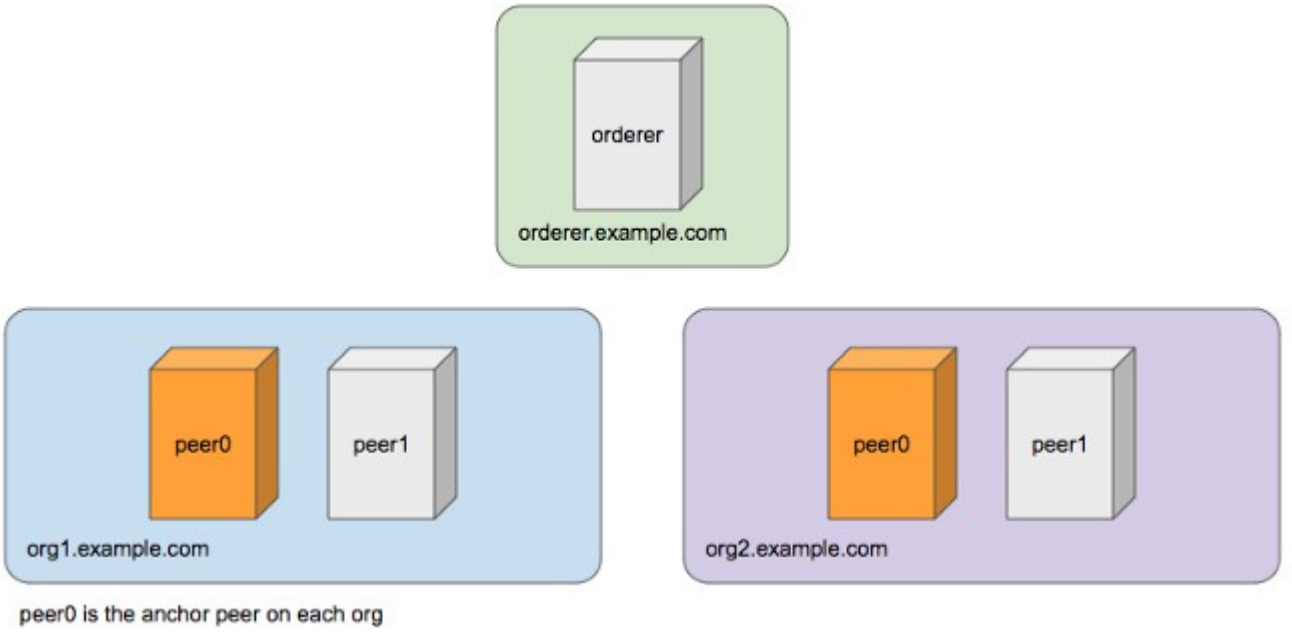
Docker, Docker-Compose, Code editor (e.g. Visual Studio Code), Git

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

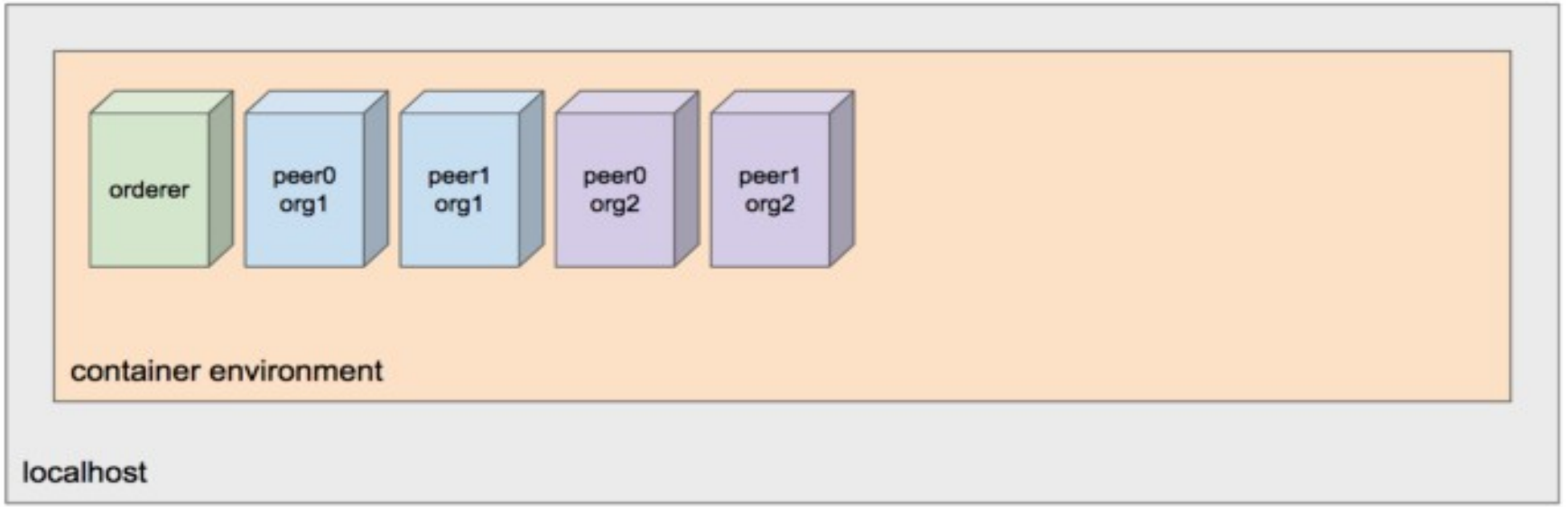
Basic JavaScript knowledge

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

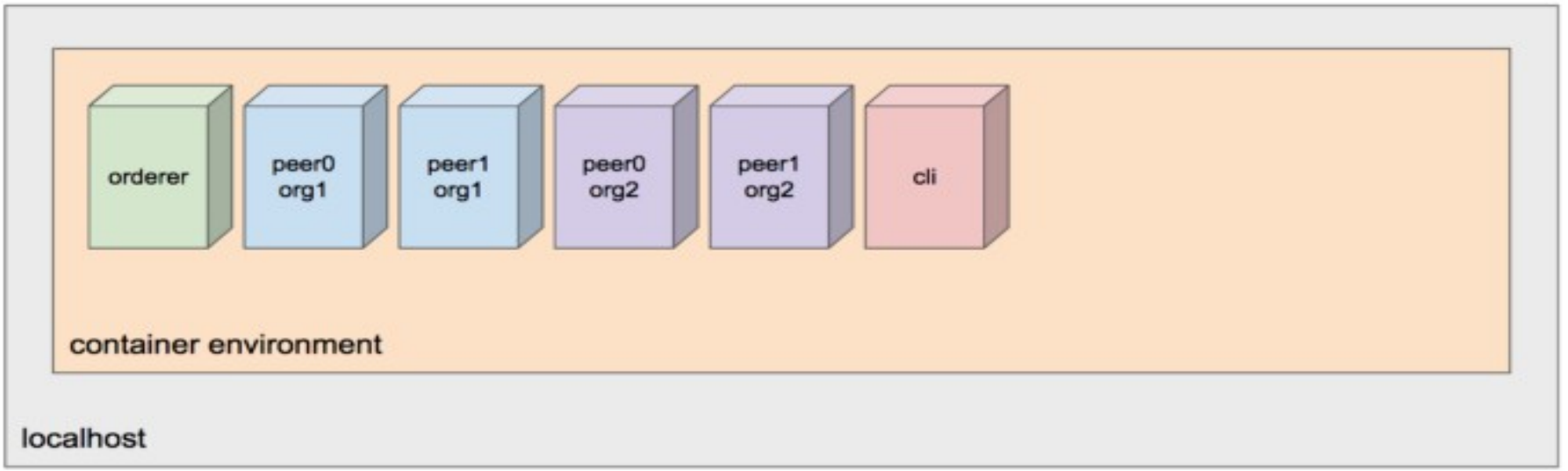
$ docker ps

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.