Aplicaciones Blockchain

Carlos Castro, Universidad del Rosario, Colombia
Alexander García, University of Graz, Austria

Estructura

- Tecnología Blockchain
- Implementacion
- Hyperledger
- Casos de Uso
  - Certificados de logros educativos.
  - Registro digital de objetos de investigación (blockchain4openscience).
  - Registros Notariales.
  - Activos Financieros

Tecnología Blockchain

- Colección de tecnologías para registrar información (base de datos, BD) con las siguientes características:
  - Descentralizado (*distributed ledger*), información se encuentra en los nodos de la red y se comunica y actualiza en tiempo real (*peer-to-peer vs client-server*).
  - Seguridad, utiliza criptografía, firmas digitales o una estructura de permisos para probar identidad, autenticación habilitando el proceso lectura/escritura sobre la base de datos.
  - El registro histórico es inmutable.
  - Contiene una serie de reglas que garantizan consistencia interna y un orden en el proceso de registro de la información.

Bitcoin Blockchain

- **Publica (quien puede leer la BD) y sin permisos (quien puede escribir en le BD)**, teóricamente cualquier individuo puede participar en la introducción de nueva información (creación de nuevos bloques).
- Para resolver conflictos sin una autoridad central introduce una serie de reglas de juego e incentivos que garantizan un orden en la creación de nuevos bloques.

Bitcoin Blockchain

Resolución de conflictos:

- Cual es la cadena sobre la cual se agregan nuevos bloques? el *consenso* es que sea la cadena mas larga.
- Compatibilidad de incentivos sobre la creación/validación de nuevos bloques (quienes: los mineros) mediante: *proof of work* (resolver un puzzle, costo computacional y tiempo).
- Pago de incentivos mediante una aplicación: **criptomoneda**.
- Registro inmutable de transacciones sobre la criptomoneda y sus derivados (otras aplicaciones).

Implementación

- Etherium, solución (publica y sin permisos) descentralizada que permite el procesamiento de datos a través de *smart contract* sin necesidad de una autoridad central.
  Criptomoneda (ETH)
- Soluciones (publicas o privadas) con permisos (control de acceso) para implementación privada principalmente.
  Administradores asignan roles y permisos dentro de la red.
  - Corda (consorcio instituciones financieras).
  - Quorum (JP Morgan)
  - IOTA
  - BigChainDB
  - Chain Core

Hyperledger

- Proyecto (Diciembre 2015) open source y colaborativo liderado por The Linux Foundation, con el proposito de impulsar la tecnologia Blockchain a o largo de diferentes industrias.
- Crear un marco de referencia y herramientas para DLT que permitan soportar un sistema transaccional para diferentes tipos de aplicaciones.

Hyperledger

- Blockchain basada en permisos y desarrollado para funcionar sobre una lógica de negocio donde existen relaciones de confianza.
- No utiliza una criptomoneda.
- Permite procesamiento de datos a traves de smart contracts.

Ethereum vs Hyperledger Fabric vs R3 Corda, Sandner (2017)

Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	– Generic blockchain platform	– Modular blockchain platform	– Specialized distrib-uted ledger platform for financial industry
Governance	– Ethereum developers	– Linux Foundation	– R3
Mode of operation	– Permissionless, public or private[4]	– Permissioned, private	– Permissioned, private
Consensus	– Mining based on proof-of-work (PoW) – Ledger level	– Broad understand-ing of consensus that allows multiple approaches – Transaction level	– Specific understand-ing of consensus (i.e., notary nodes) – Transaction level
Smart contracts	– Smart contract code (e.g., Solidity)	– Smart contract code (e.g., Go, Java)	– Smart contract code (e.g., Kotlin, Java) – Smart legal contract (legal prose)
Currency	– Ether – Tokens via smart contract	– None – Currency and tokens via chaincode	– None

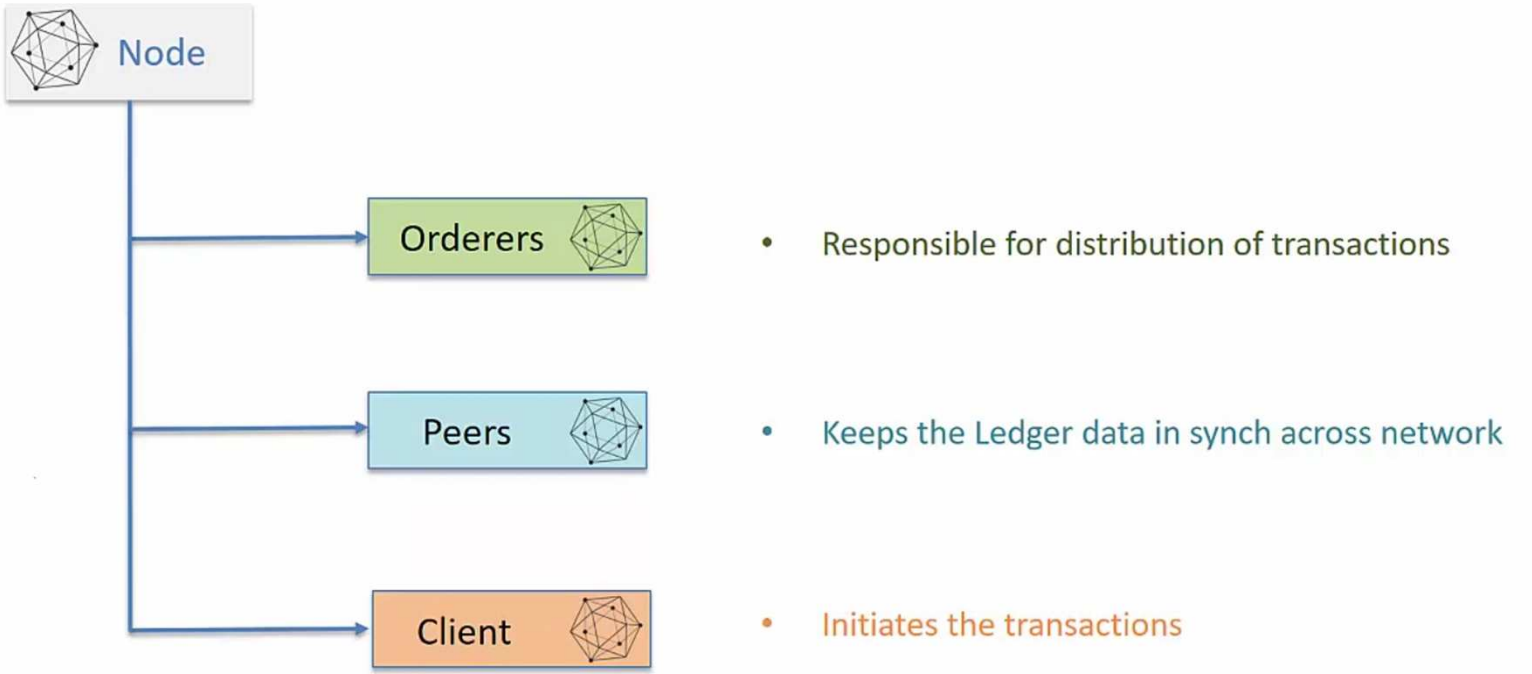
Hyperledger

- Marcos de referencia: Sawtooth (construcción, lanzamiento y administración de DL), Iroha (moviles), Fabric (desarrollo de aplicaciones sobre DL), Burrow (smart contracts), Indy (identidad des-centralizada)
- Herramientas: Cello (lanzamiento y administración de DL), Composer (diseño de DL y desarrollo de smart contracts), Explorer (visualizar y explorar una DL), Quilt (interoperabilidad entre DL), Calliper (benchmarking).

Hyperledger: Fabric

Marco de referencia que permite desarrollar la arquitectura de la red de manera modular, escalable y flexible. Administra permisos y privacidad.

Elementos de la red: nodos (Udemy, 2018).



Hyperledger: Fabric (Hyperledger, 2018)

Committing Peer

- Maintains ledger and state
- Commits transactions
- May hold smart contract (chaincode)

Endorsing Peer

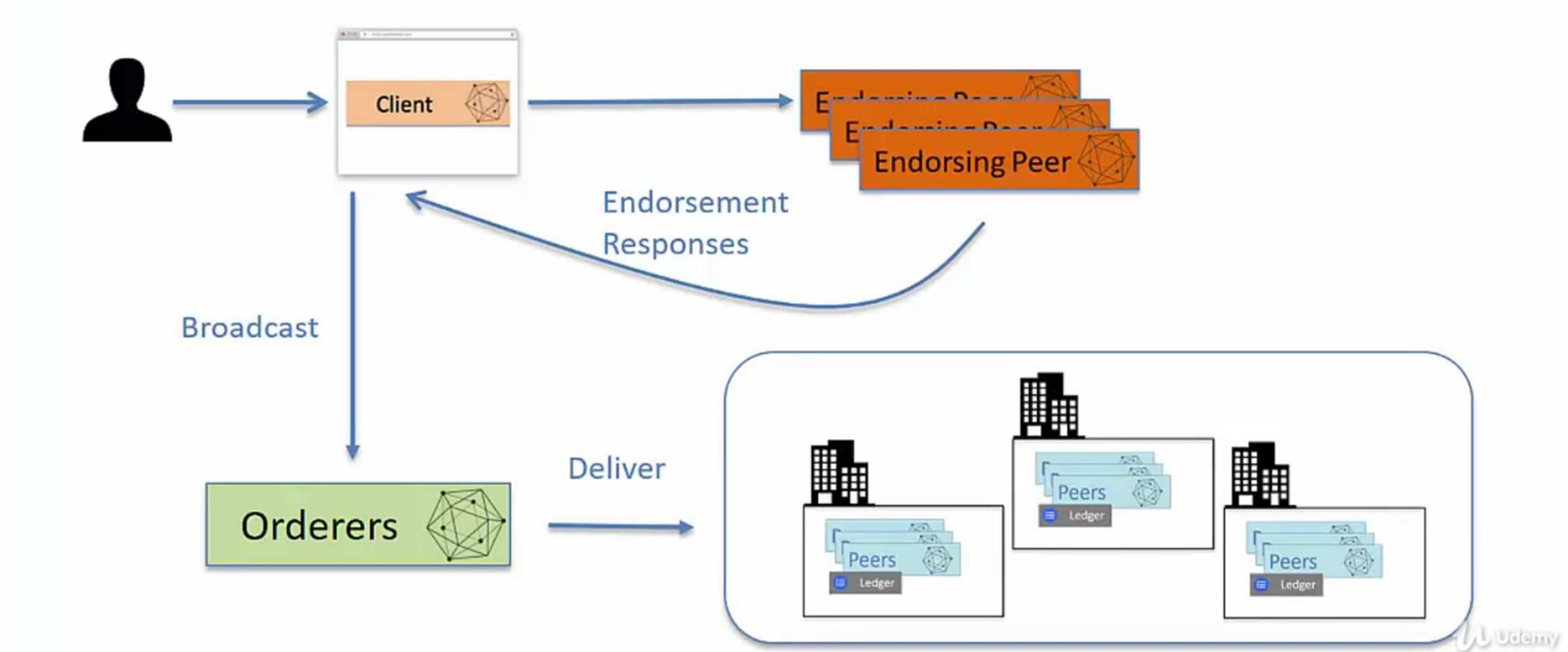
- Receives a transaction proposal for endorsement, responds granting or denying endorsement
- Must hold smart contract
- Verifies that its content obeys a given smart contract
- Endorser “signs” the contract

Ordering Node

- Approves the inclusion of transaction blocks into the ledger and communicates with committing and endorsing peer nodes
- Controls what goes in the ledger making sure that the ledger is consistent
- Does not hold smart contract
- Does not hold ledger

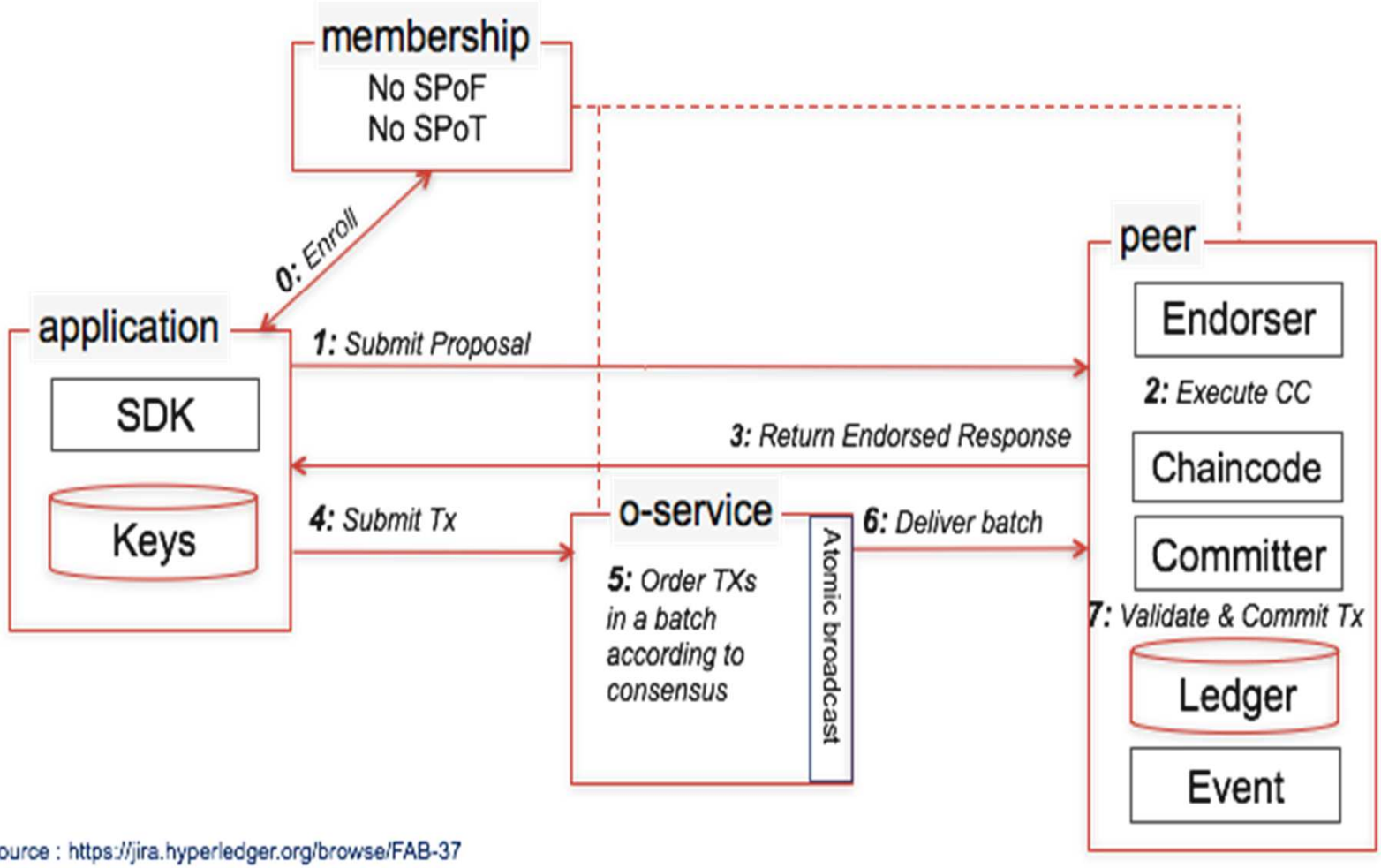
Hyperledger: Fabric

(resumen de transacción)



Hyperledger: Fabric (Hyperledger, 2017)

(resumen de transacción)



Source : https://jira.hyperledger.org/browse/FAB-37

Hyperledger: Composer

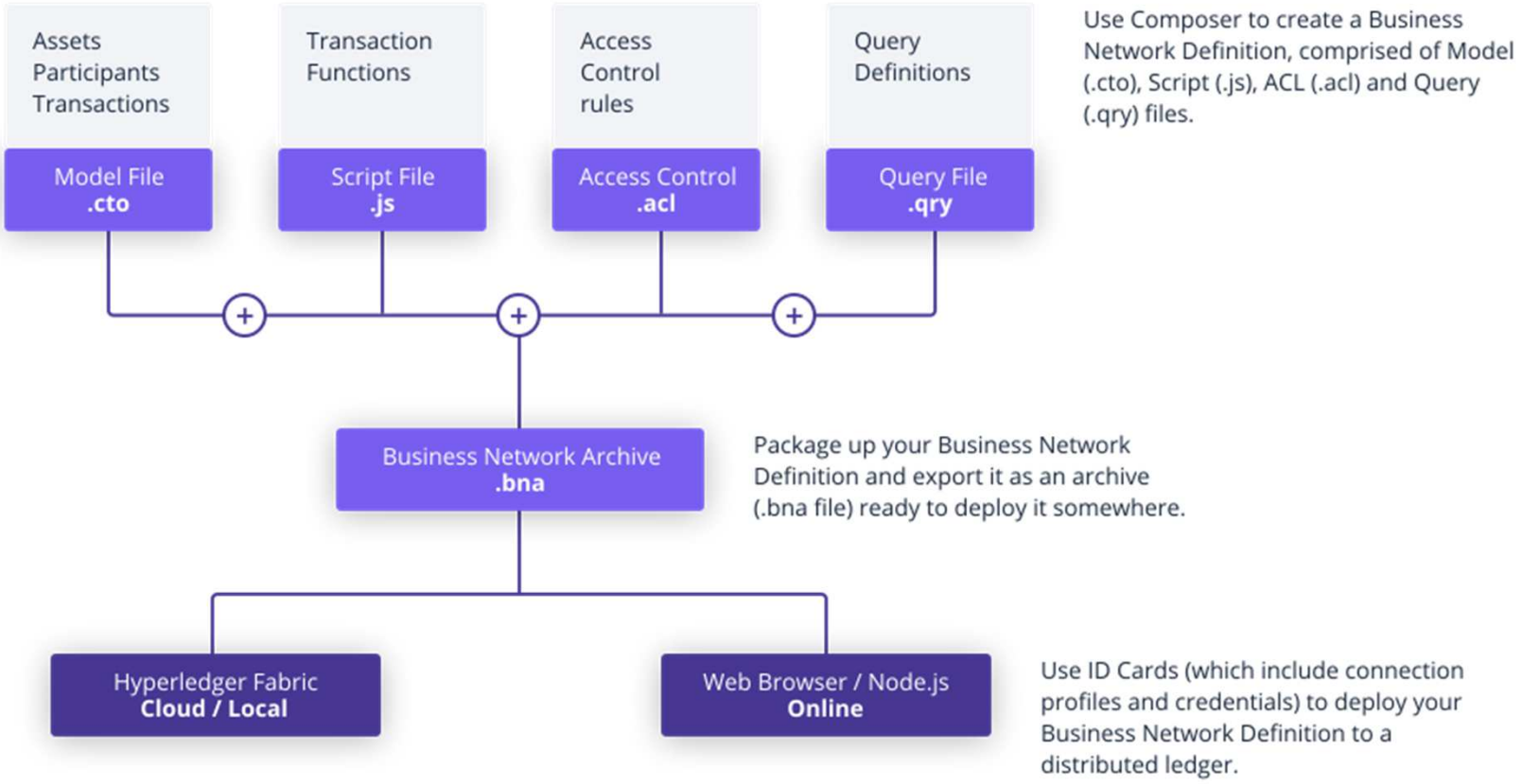
Herramienta para diseñar Business networks (.bna).

No es muy diferente a pensar en un modelo económico y sus elementos:

- Activos (bienes)
- Participantes (agentes)
- Transacciones (relaciones)

Cualquier interacción (creación, transacciones, modificación) genera un registro inmutable en el *ledger*. Existe otro registro que puede cambiar y que guarda el estado actual de activos y participantes.

Hyperledger: Composer (Hyperledger, 2018)
(Diseño Business Network)



Casos de Uso

Certificación Digital

- Los certificados son una convención social utilizada para señalar un logro, una membresía o en general un nuevo conjunto de información relevante para una persona o institución Sin embargo el sistema actual de emisión, validación y administración se caracteriza por ser un proceso lento, complicado e ineficiente y en muchos caso poco seguro; por ejemplo: titulación educativa nacional y extranjera, registros civiles, ...

Certificación Digital

- Facilitar el proceso de verificación y transferencia de los certificados es una ventaja de pensar en sistemas de certificación digital. Para hacer esto realidad se necesita una plataforma abierta pero a su vez segura como lo es la tecnología Blockchain. Este tipo de infraestructura permitiría a las personas o instituciones compartir sus logros y credenciales de una forma rápida, segura y confiable.

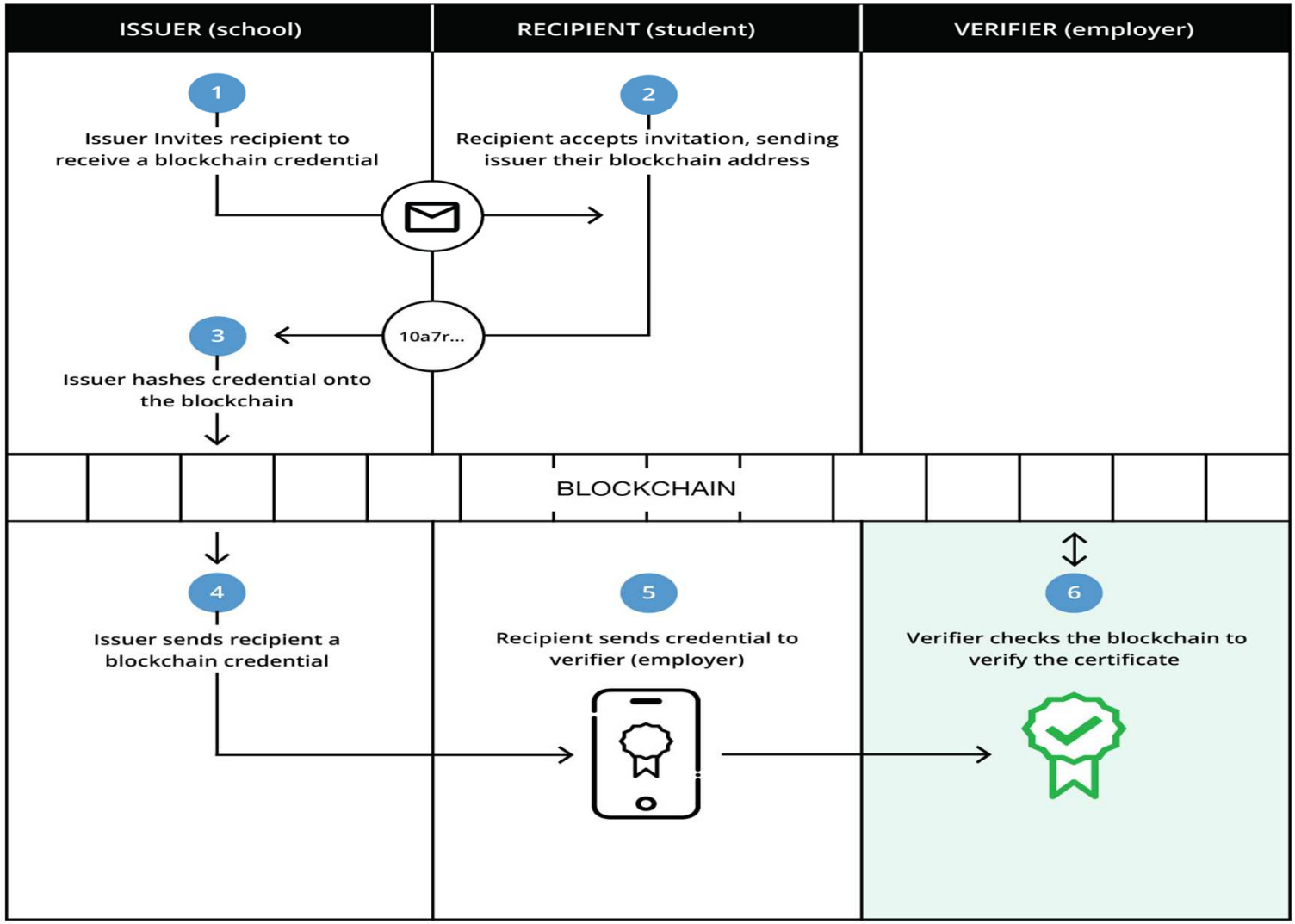
Estandares de Certificación

- Tecnologia Blockchain se viene desarrollando de manera autonoma, pero dentro de una comunidad interesada en desarrollar estándares que permitan acelerar la difusión y aprovechar externalidades de red (ISO/TC 307, Standards Australia).
- La certificación digital se asocia usualmente a a un estandard de comunicación segura conocido como SSL (secure socket layer).

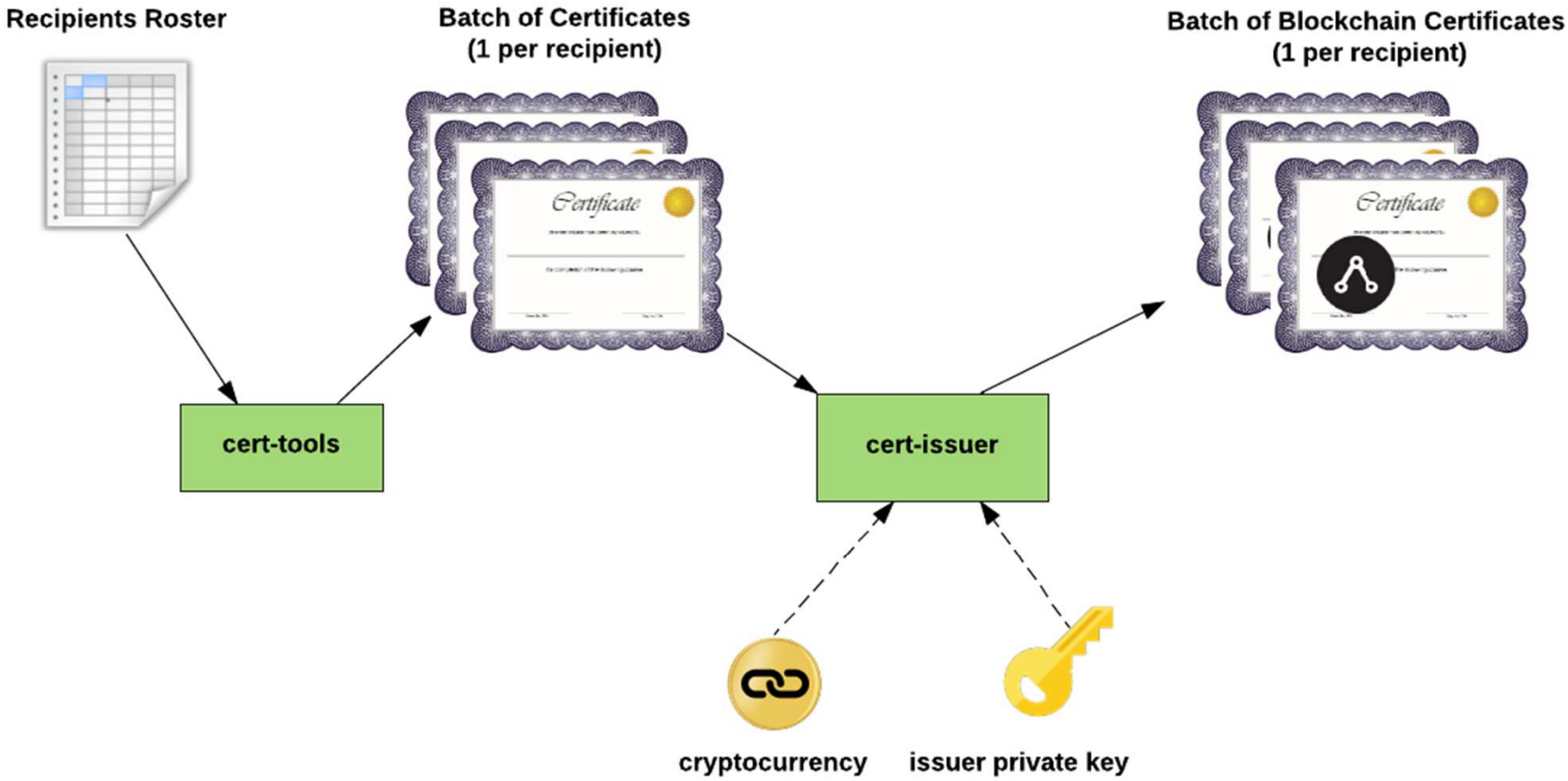
Estandares de Certificación

- La inmutabilidad de la tecnología Blockchain, se viene utilizando para garantizar la validez de un certificado que ha sido emitido.
- Blockcerts: the open innitiative for Blockchain certificates (MIT media Lab/Learning Machine)
- La firma digital de los bloques de certificados se incluye en el bitcoin blockchain.
- Incluye otras herramientas para verificar las firmas, visualizar certificados.
- Desarrolla estándares abiertos.

Como funciona Blockcerts



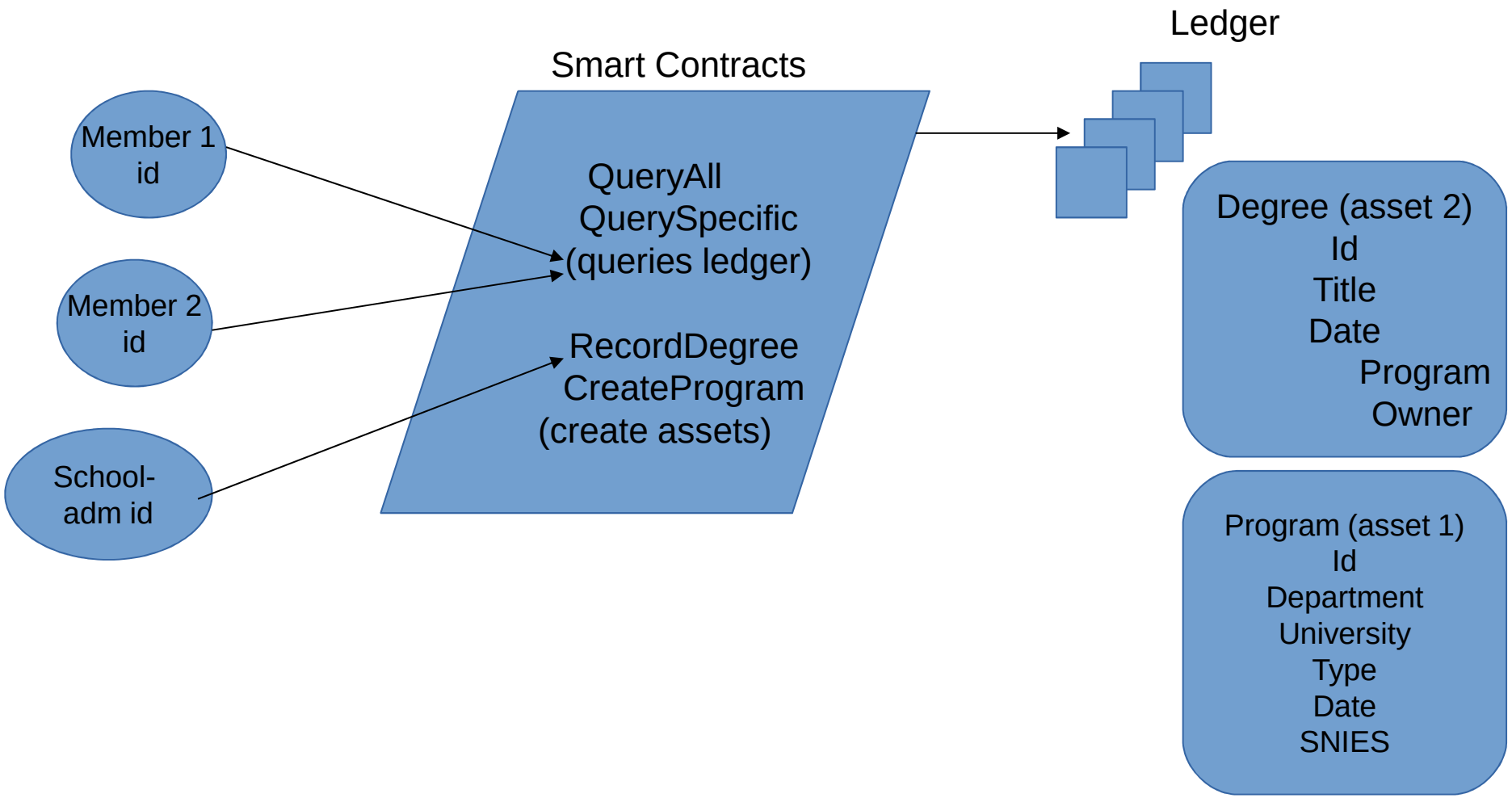
Generación de certificados



Certificados de logros educativos

- Aplicación Hyperledger (abierta-leer con permisos-escribir).
- No requiere criptomoneda.
- Ajustado Estándar de Blockcerts (procedimiento, campos y sub-campos): id; badge-issuer; recipient:publicKey, name; seguridad y autenticación.
- Prototipo funcional para una o varias organizaciones (registro, secretarias academicas); diseño de la red.

Business Network, edu-degree-network-v1.bna (playground)



Registro digital de objetos de investigación

Blockchain4openscience

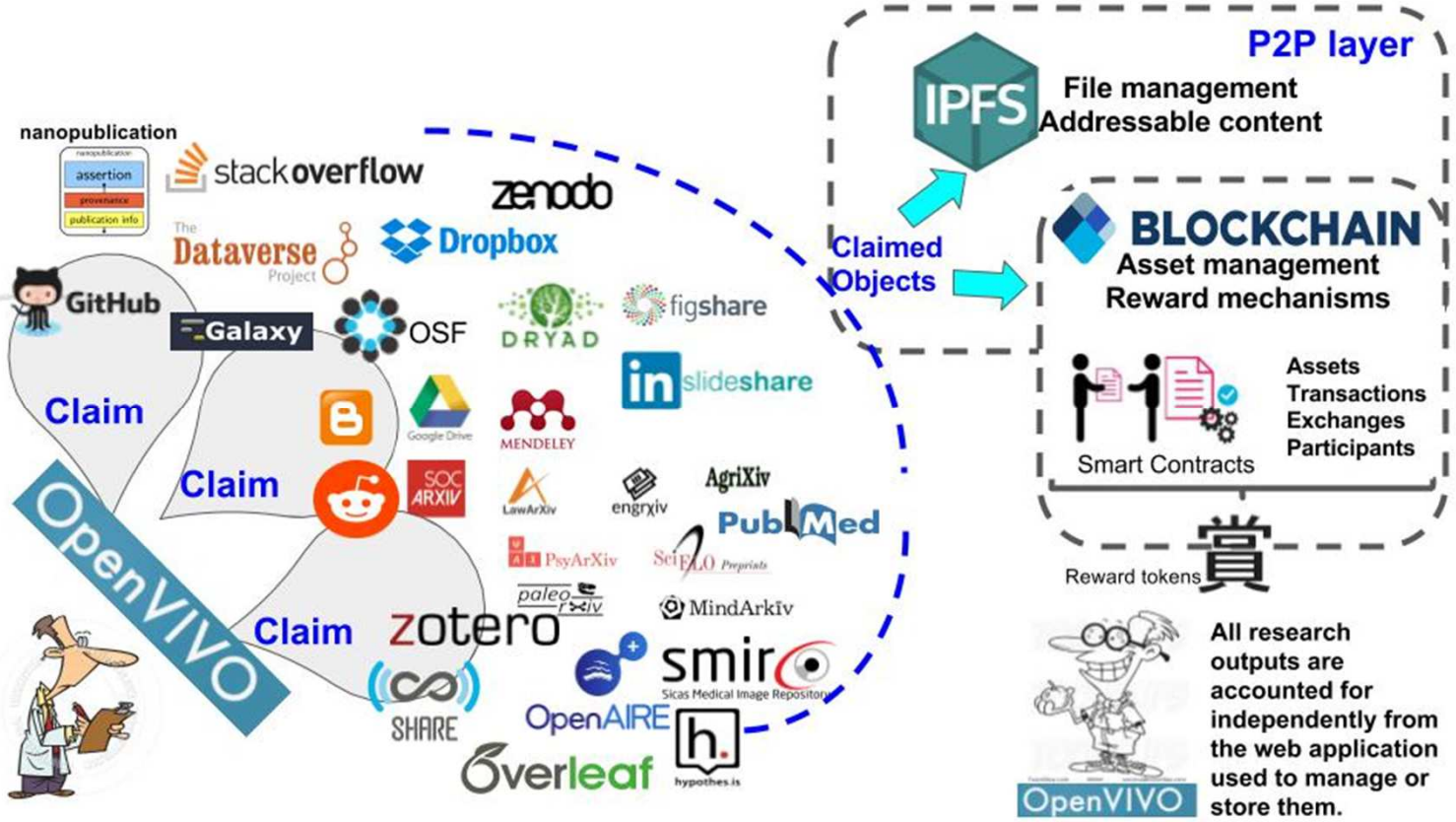
Open science is a new movement in science that promotes principles of open access to research data, publications, and scientific collaboration. Open science promises to increase transparency and quality of research, provide reproducibility by reusing scientific datasets and increasing trust in the scientific collaboration.

Blockchain4openscience

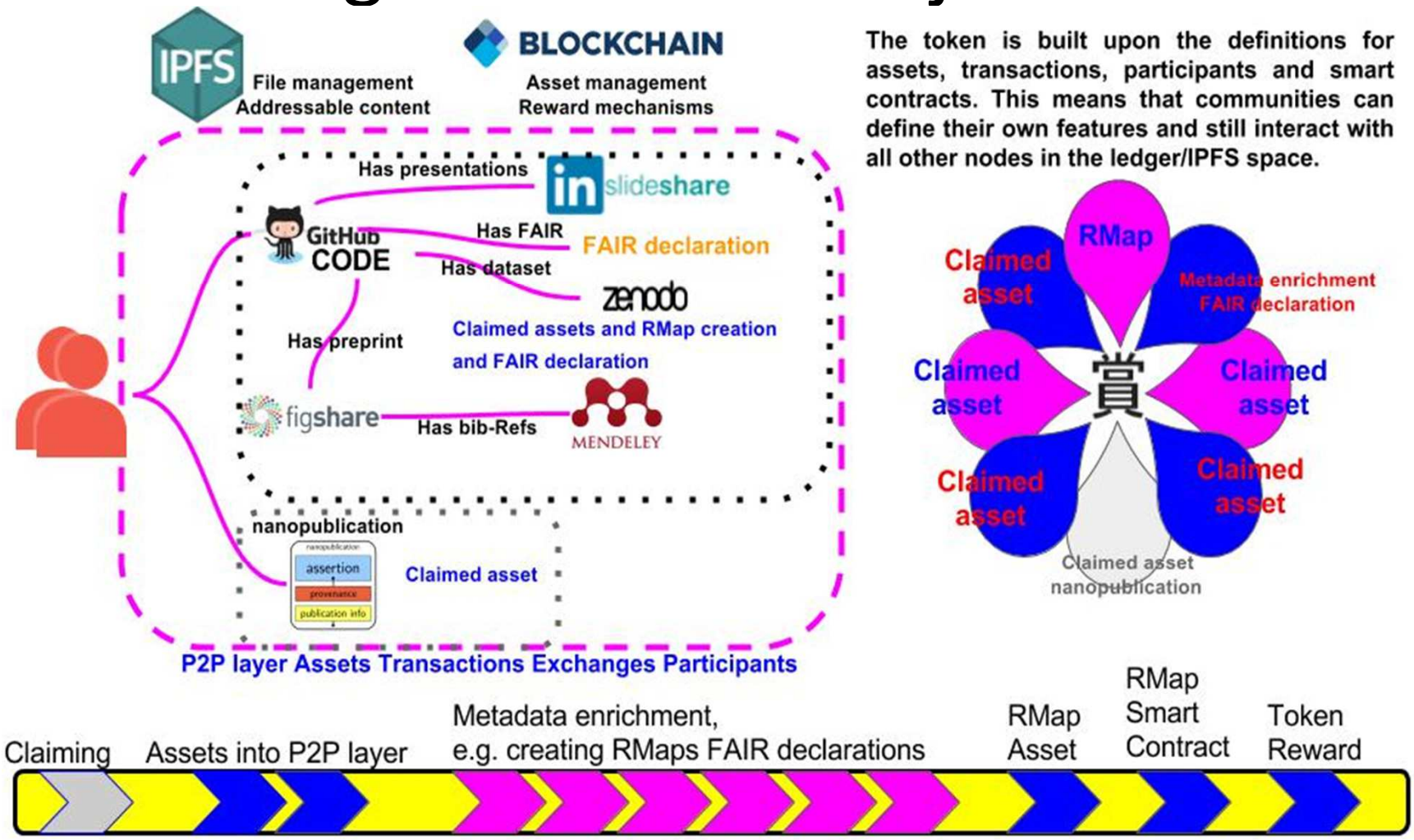
Blockchain fits the mindset of open science and can help to fulfill open science principles: transparency and availability of blockchain makes scientific outputs open & transparent; disintermediation removes subjectivity from scientific reviews; integrity and possibility to secure transactions in the competing environment increases trust in scientific results; smart contracts allows to manage access to scientific outputs; immutability represents precise relationships between the works with such features as richness, time-based relationships, and logical precursors: a digital continuum

Blockchain4openscience

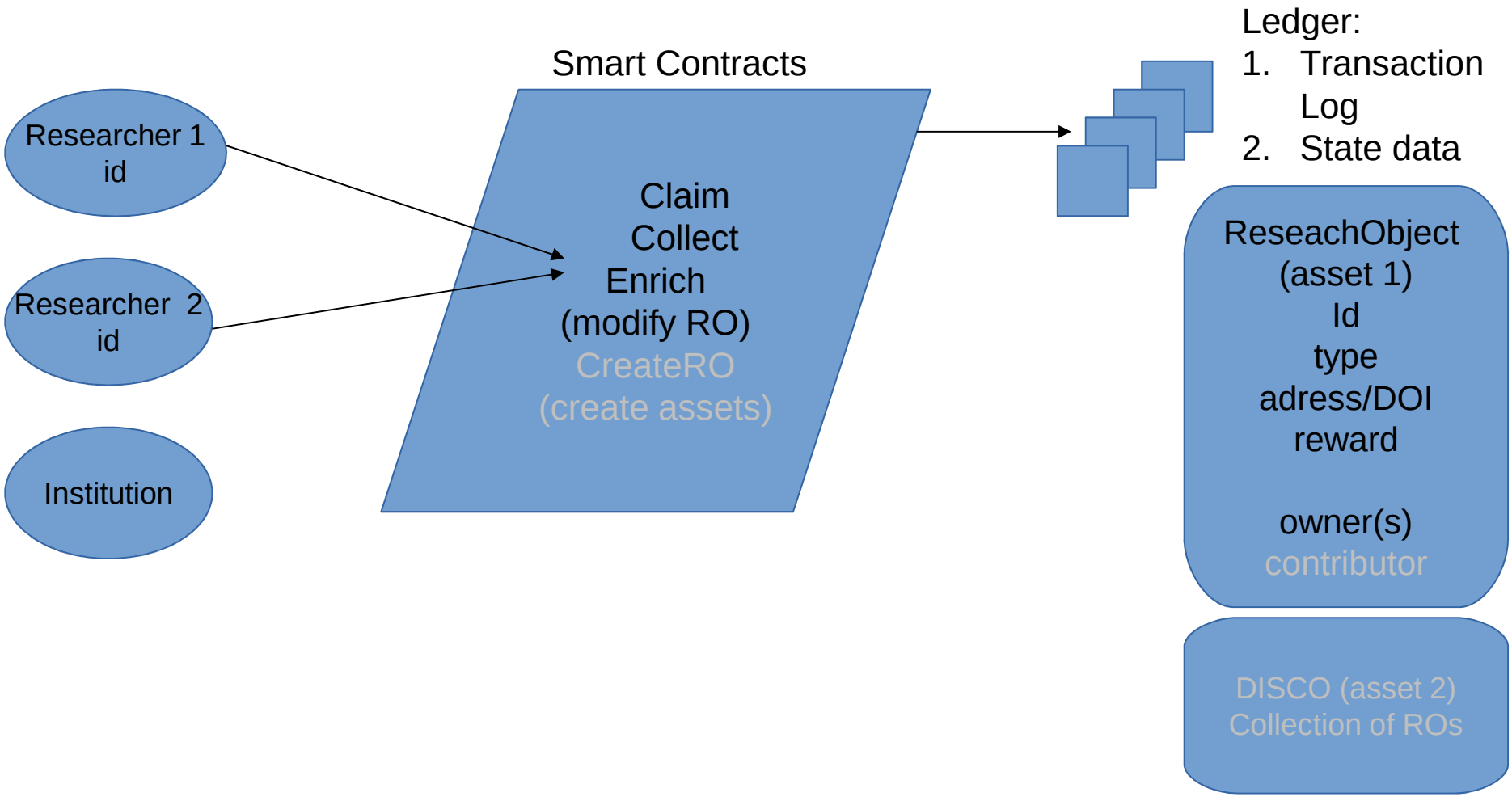
Successful integration of a registry, the storage of the asset and a reward system (tokens), using existing frameworks:



Claim, enrich and get rewards from digital research objects



Business Network, blockchain4sciencev1.bna (playground)



Registro digital de objetos de investigación

Blockchain4openscience

- Esfuerzo de investigadores en US y Europa
- Recibió un Catalyst Grant (2018-2019)
- genenetwork.org (2018-2019)
- Whitepaper (Julio, 2018)
- POC (Diciembre, 2018)

Propuesta Urosario

- Desarrollar capacidades e implementar aplicaciones basadas en tecnología Blockchain.
- Proyecto conjunto Finanzas-Fac. Economia / MACC-Fac. Ciencias / otras facultades o escuelas?
- Empezar con una aplicación sencilla: certificados de logros educativos; involucrar áreas de tecnología y registro de la Universidad.

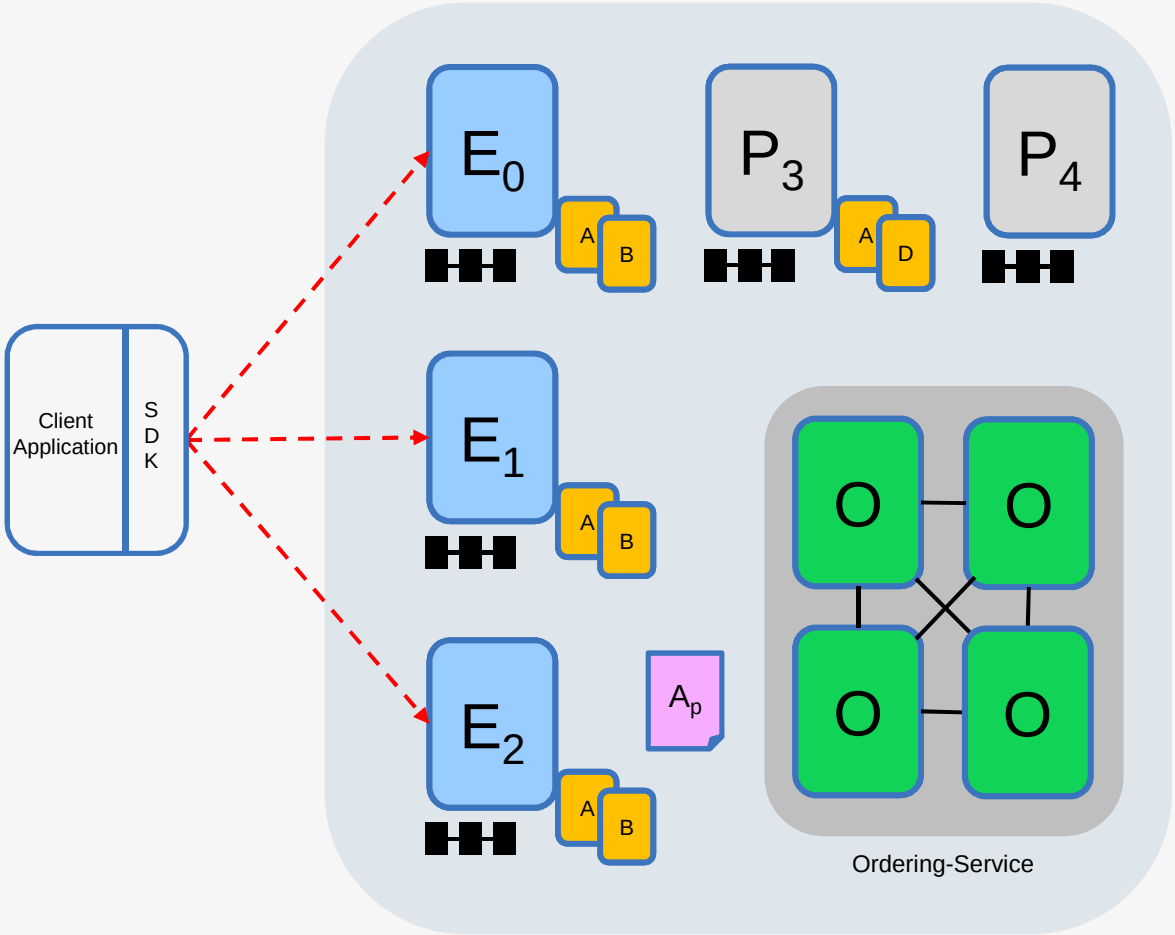
Propuesta Urosario

- Visibilidad en comunidad hyperledger.
- Crear https://www.meetup.com/pro/hyperledger en Colombia. ViveLab, realizo un meetup en febrero 2018, pero no hay continuidad?
- Escribir proyecto para plantear a rectoría o aplicación FIUR 2019 y desarrollar un prototipo funcional (Proof of Concept).

Anexo

(Hyperledger, 2017)

Sample transaction: Step 1/7 – Propose transaction



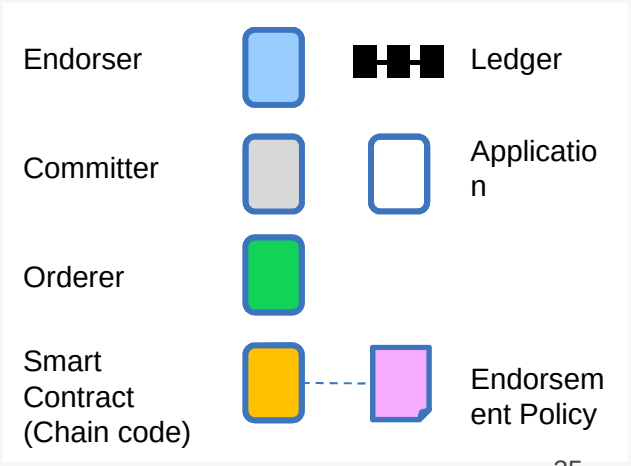
Hyperledger Fabric

Application proposes transaction

Endorsement policy:
- "**E_0, E_1** and **E_2** must sign"
- (**P_3, P_4** are not part of the policy)

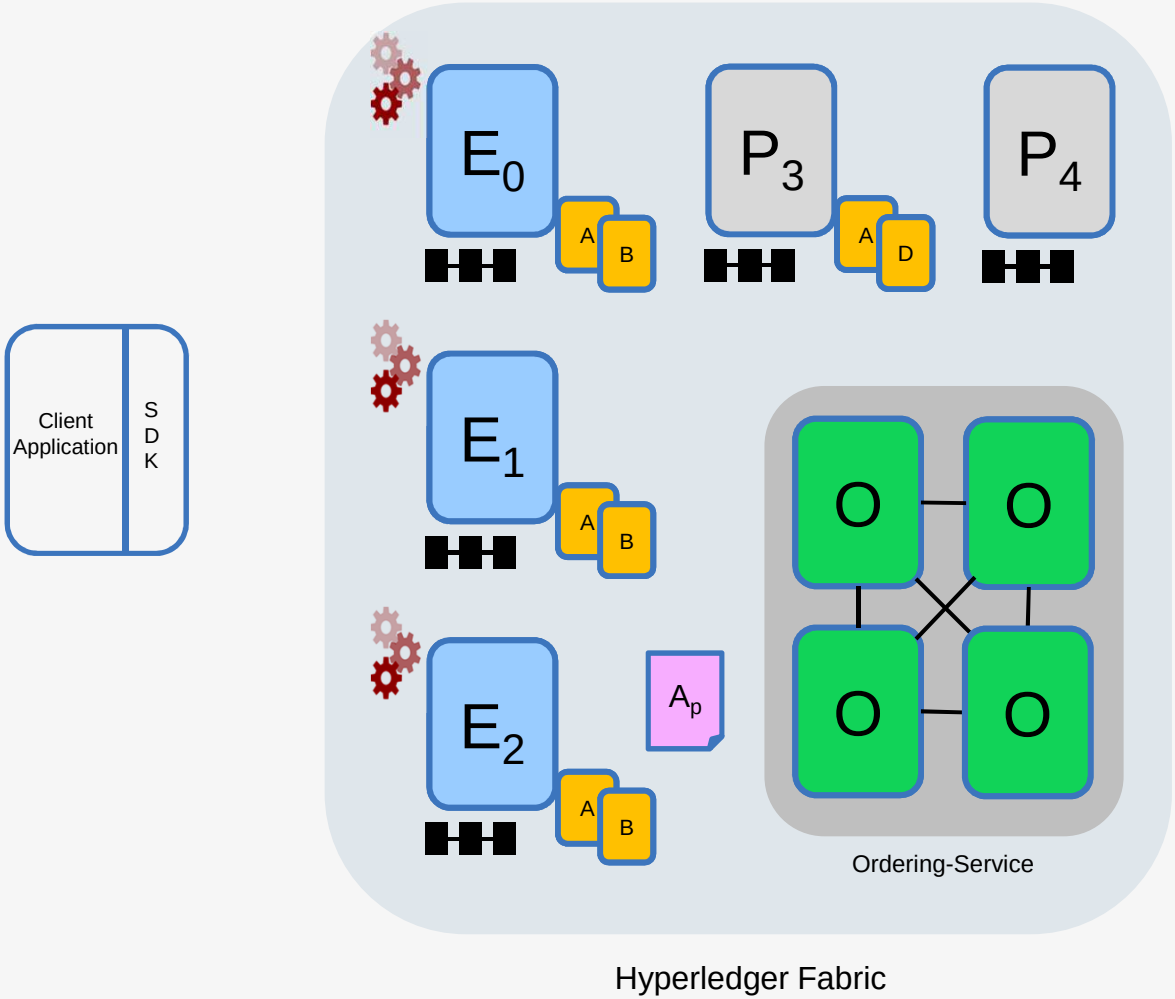
Client application submits a transaction proposal for **chaincode A.** It must target the required peers {**E_0, E_1, E_2**}

Key:



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Sample transaction: Step 2/7 – Execute proposal



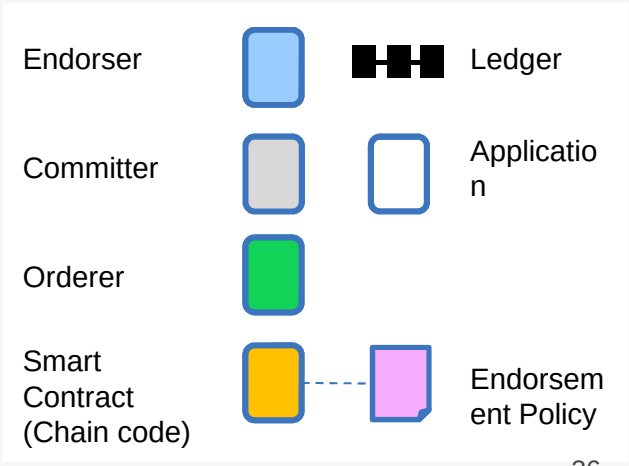
Hyperledger Fabric

Endorsers Execute Proposals

E_0, **E_1** & **E_2** will each execute the *proposed* transaction. None of these executions will update the ledger

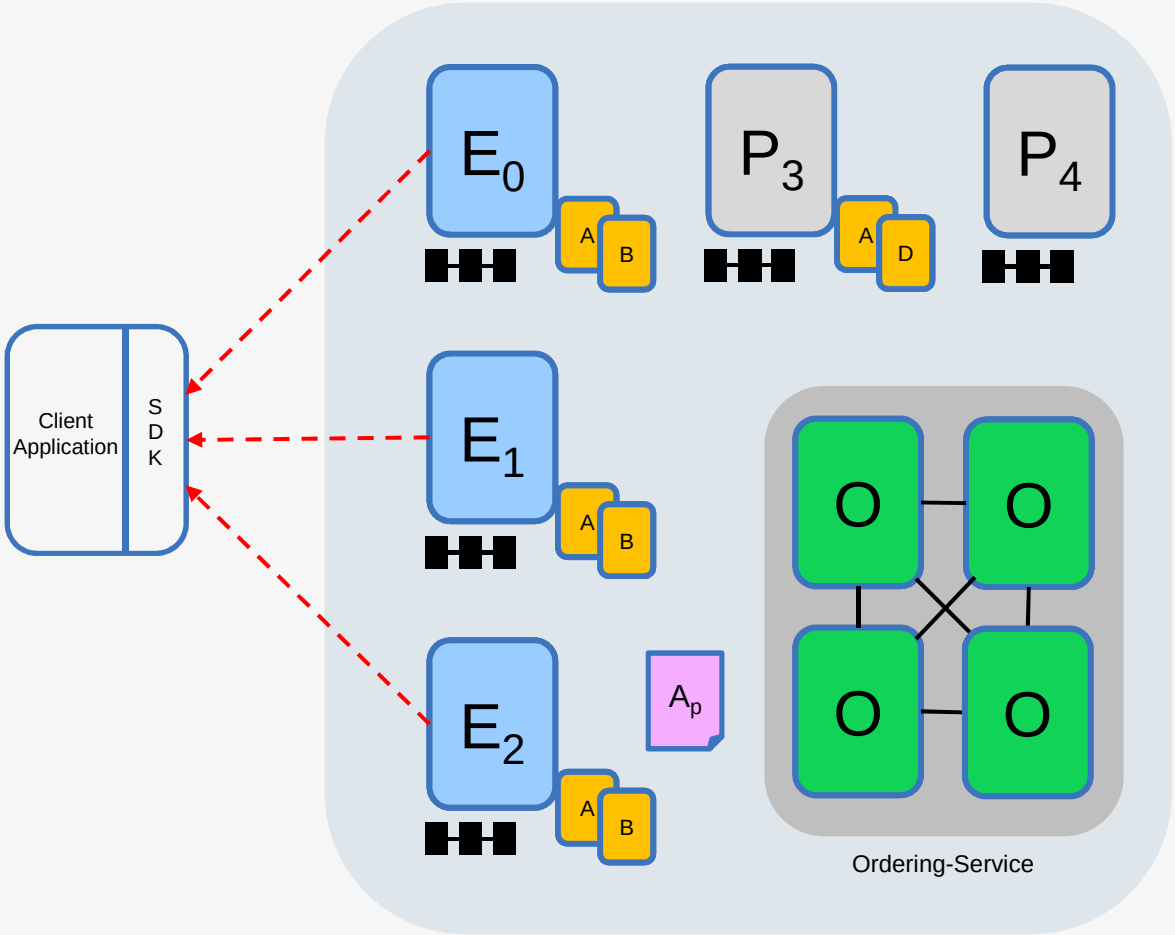
Each execution will capture the set of **R**ead and **W**ritten data, called **RW sets,** which will now flow in the fabric.

Key:



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Sample transaction: Step 3/7 – Proposal Response

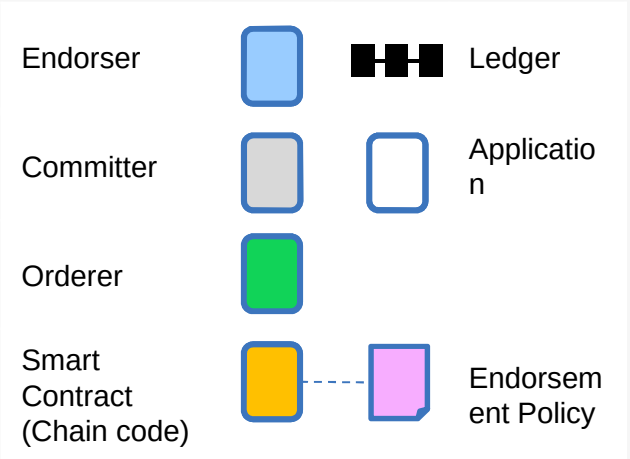


Hyperledger Fabric

Application receives responses

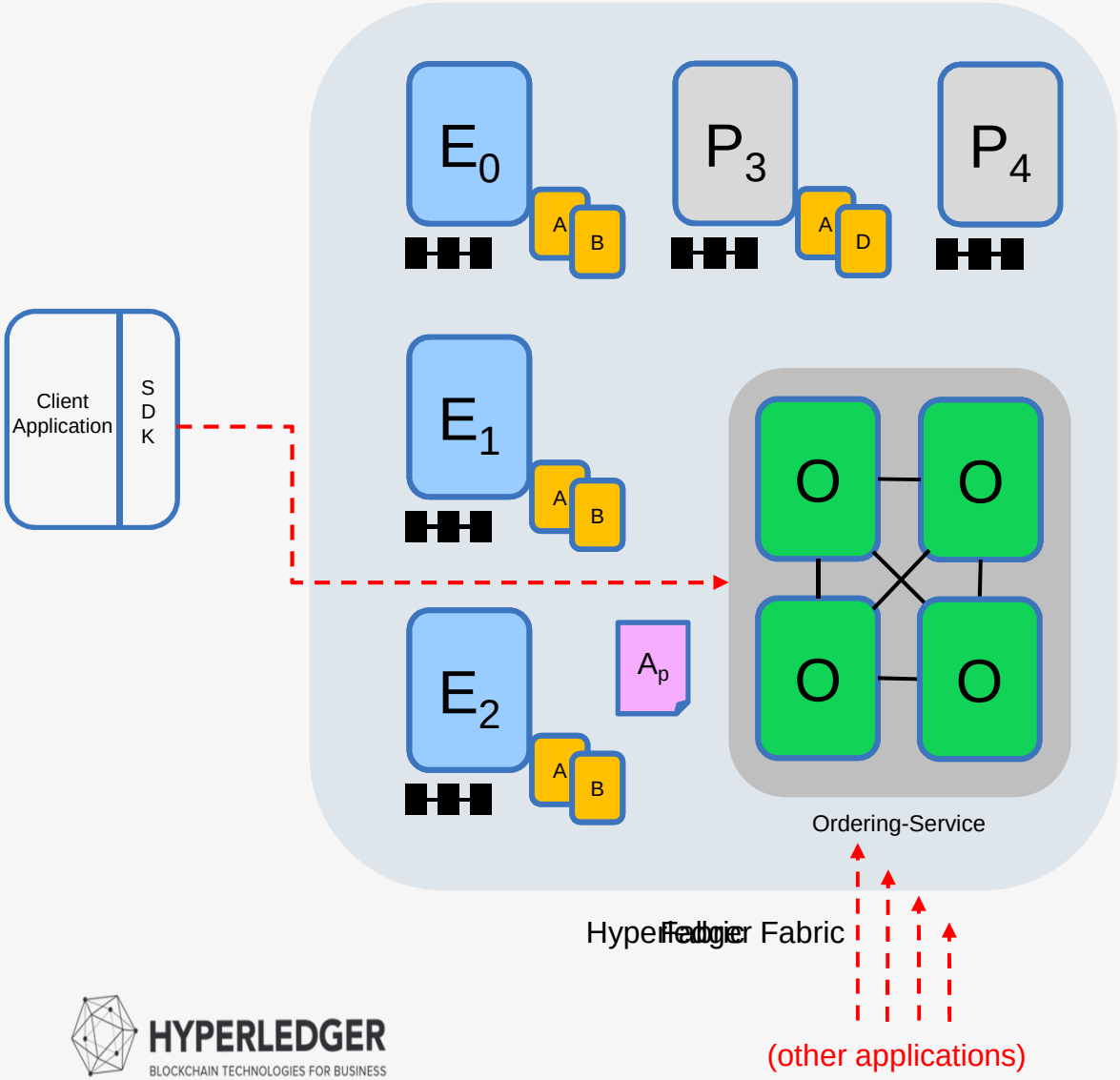
The RW sets are signed by each endorser and returned to the application

Key:



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Sample transaction: Step 4/7 – Order Transaction

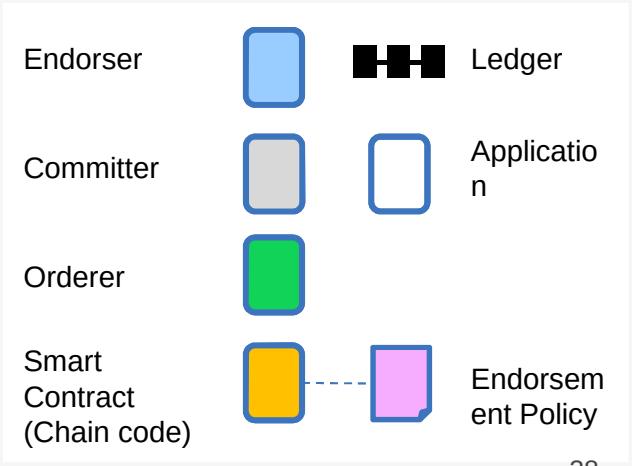


Application submits responses for ordering

Application submits responses as a **transaction** to be ordered.

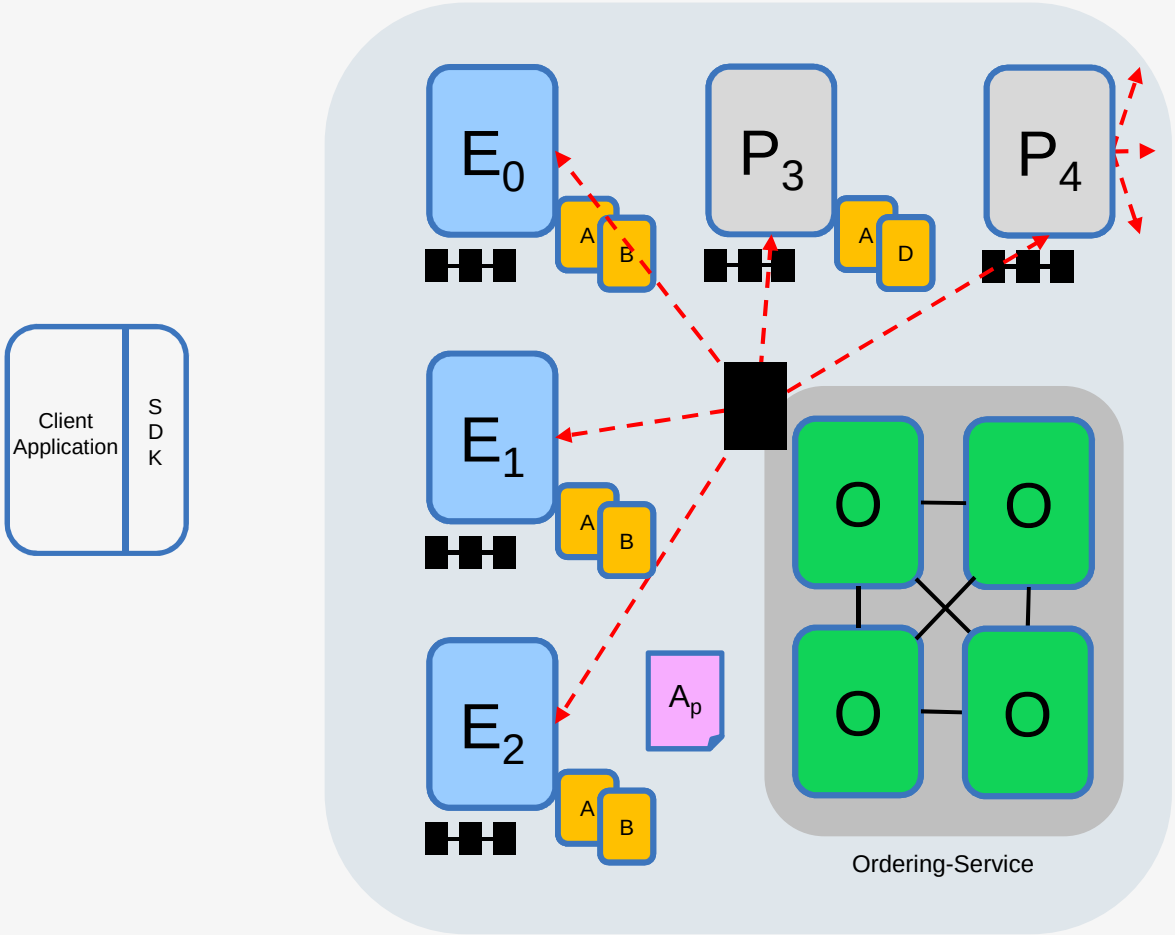
Ordering happens across the fabric in parallel with transactions submitted by other applications

Key:



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Sample transaction: Step 5/7 – Deliver Transaction



Hyperledger Fabric

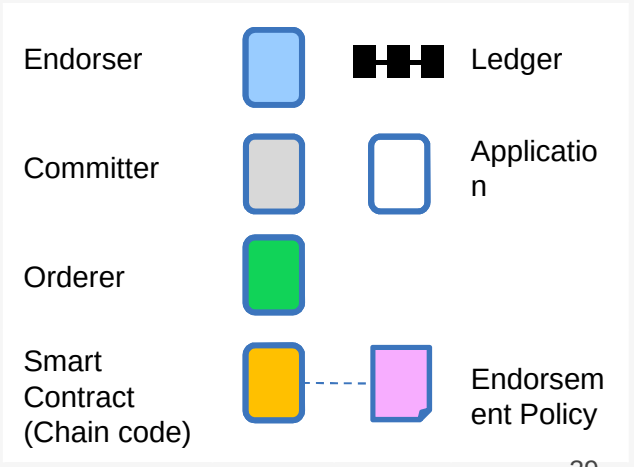
Orderer delivers to all committing peers

Ordering service collects transactions into blocks for distribution to committing peers. Peers can deliver to other peers using gossip (not shown)

Different ordering algorithms available:

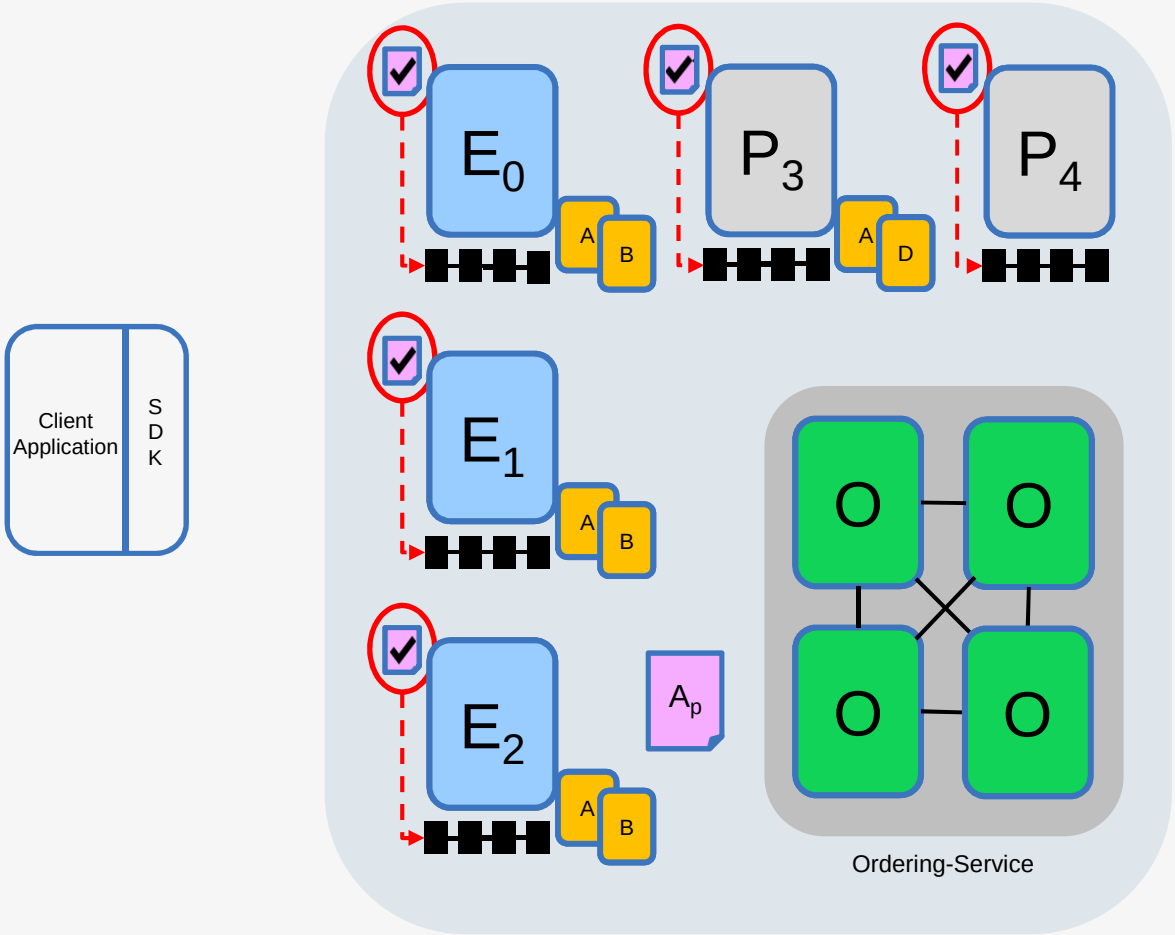
- SOLO (single node, development)
- Kafka (blocks map to topics)
- SBFT (tolerates faulty peers, future)

Key:



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Sample transaction: Step 6/7 – Validate Transaction



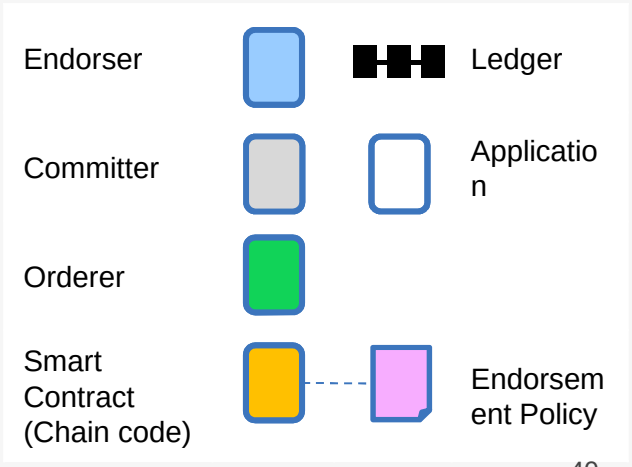
Hyperledger Fabric

Committing peers validate transactions

Every committing peer validates against the endorsement policy. Also check RW sets are still valid for the current state

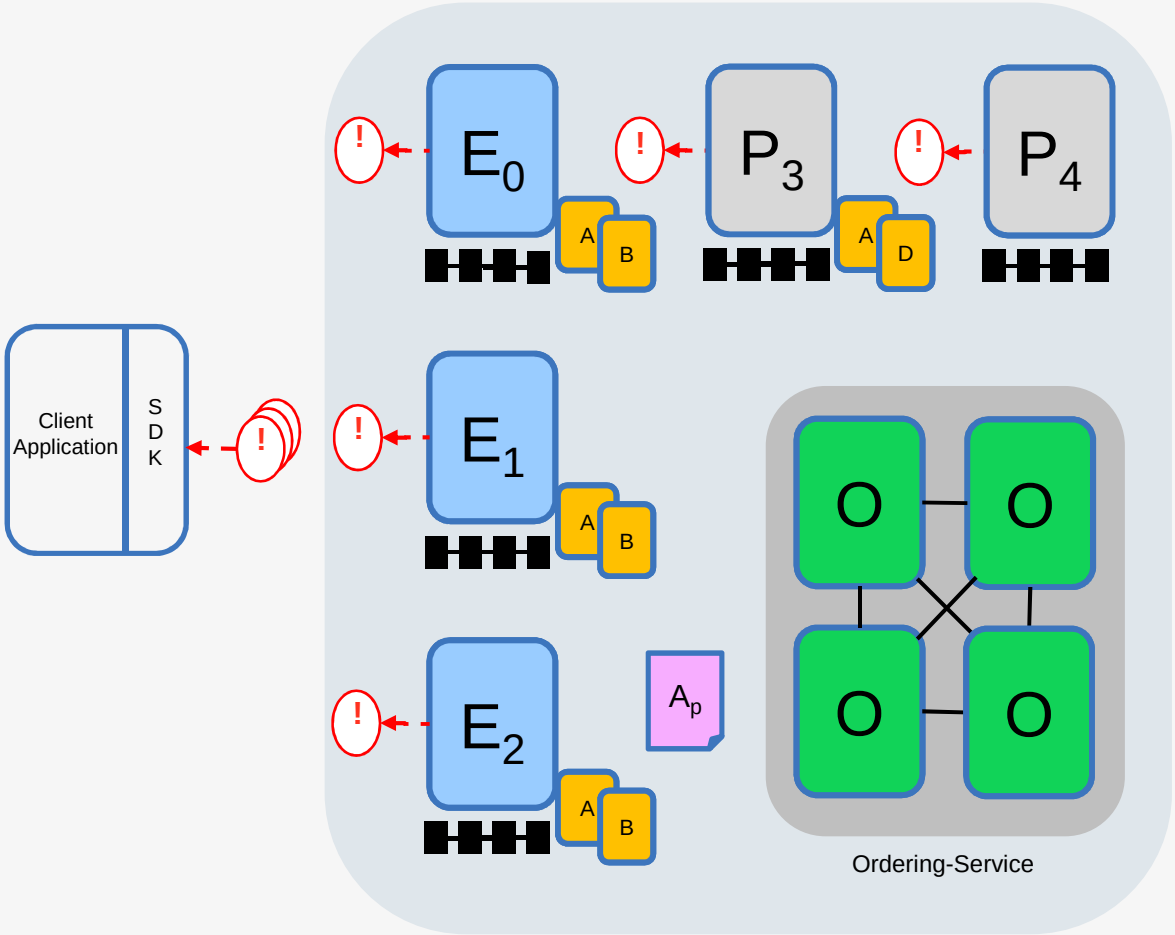
Transactions are written to the ledger and update caching DBs with validated transactions

Key:



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Sample transaction: Step 7/7 – Notify Transaction



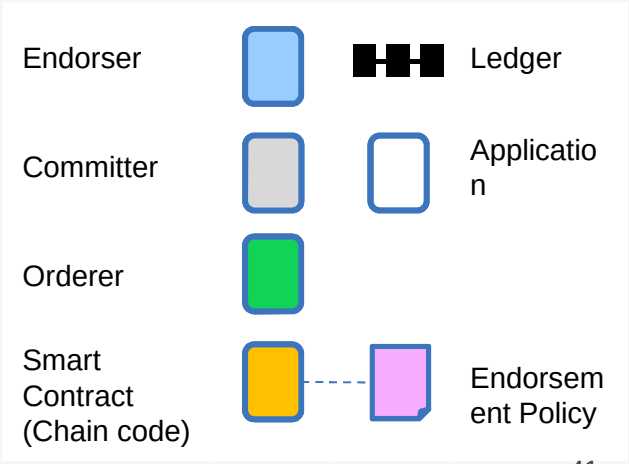
Hyperledger Fabric

Committing peers notify applications

Applications can register to be notified when transactions succeed or fail, and when blocks are added to the ledger

Applications will be notified by each peer to which they are connected

Key:



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS