Certificados Digitales para Entidades Publicas con Blockchain

LINKING DATA

Certificados

- Convención social para visibilizar un nuevo conjunto de información usualmente una afirmación.
- Tecnologías:
  - Papel: elementos de seguridad, guardar copia, entrega al receptor, no se puede revocar, verificación manual.
  - Certificados digitales: verificación central, firmas digitales (seguridad), varios estándares, guarda el emisor, verificación contra emisor o delegado.

Certificados digital

Estructura de los datos (estándar)

- Afirmación (información).
- Emisor
- Evidencia
- Receptor (opcional)
- Certificado (documento)
- Firma

Componentes o procesos

- Definición/Diseño con estándar abierto (Schema)
- Emisión (Orquestador modular)
- Compartir utilizando un medio.
- Validador general.

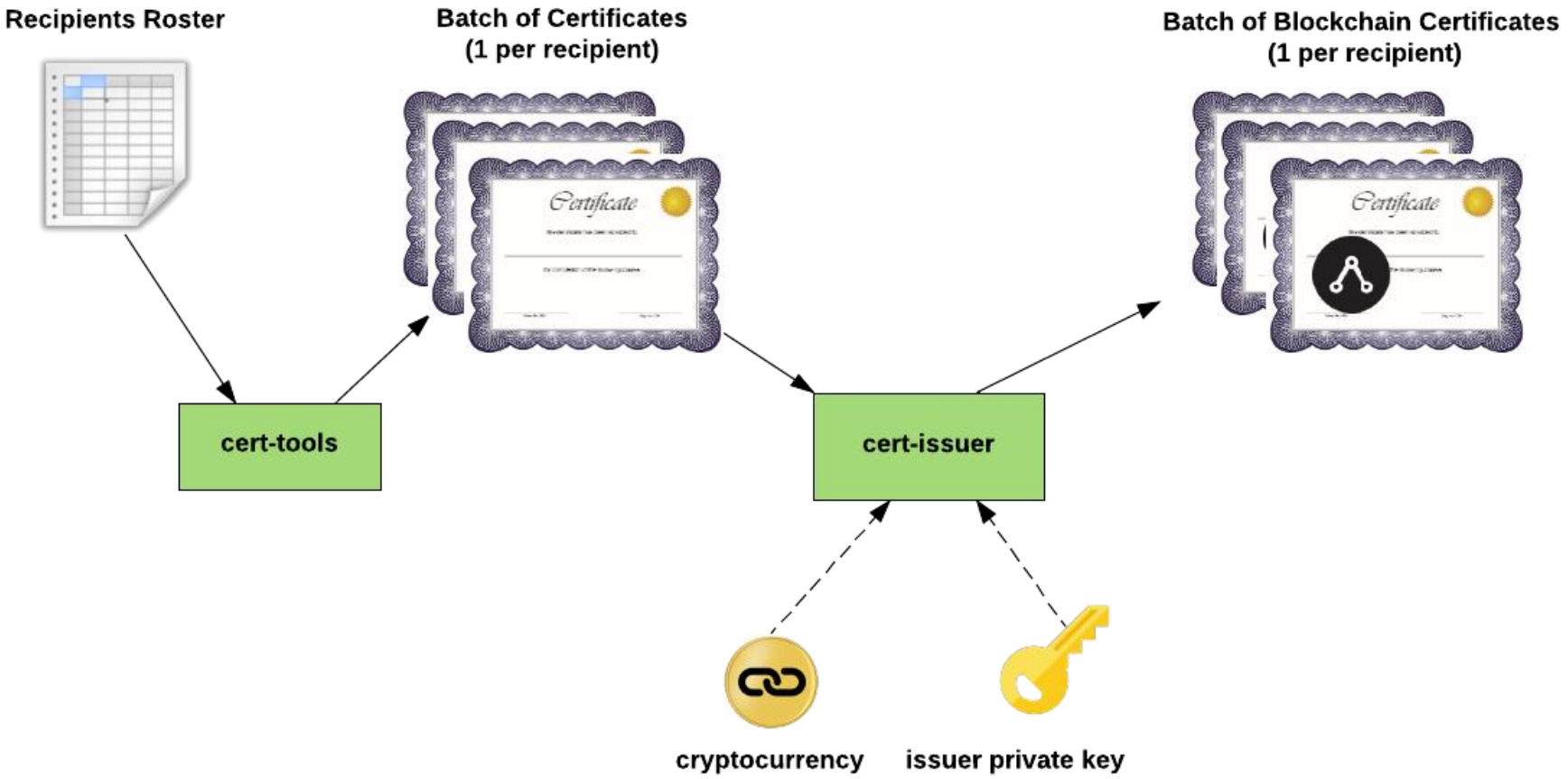
Certificados digitales utilizando Blockchain

- Permanencia y trazabilidad.
- Verificación independiente.
- Emisor (puede expirar/revocar emisión) tiene un sistema seguro y sin costos adicionales una vez emitido.
- Receptor (controla y es dueño de su información).
- Remplaza el sistema de verificación digital centralizado (firmas digitales).
- Proporciona una red amplia y no excluyente para compartir la información (Interoperabilidad).
- Complementa la identidad auto soberana.

Antecedentes en Educación: Blockcerts

- MIT/Machine Learning, 2015.
- MIT, UC Berkely, Toronto, Delf, TEC Monterrey, UC3,UN,..
- Estándar que extiende IMS Open Badges, W3C Verifiable Claims.
- Verificación:
  - Integridad del certificado: Los datos no han sido modificados. Firma Criptográfica.
  - Autenticación del emisor: Validación de la firma del emisor (externa o interna) y que el certificado no ha sido revocado.
  - Verificar la integridad de la cadena de bloques
  - Para blockchain sin permisos recibo de la transacción.

Generación de certificados end-to-end



Componentes Blockcerts

1. cert-tools:
    1. Función generar template (.py): a partir de un archivo de configuracion (.ini) se construye una estructura de datos (.json) con caracteristicas de emisor, información, repositorio imágenes, entre otros elementos del certificado.
    2. Función personalizar (.py): a partir del template (config) y un archivo (.csv roster) de individuos se introducen campos (name, pubkey, identity/email) al certificado. Nueva estructura datos (.json).

Generación mediante Blockcerts

1. cert-issuer: *“The cert-issuer project issues blockchain certificates by creating a transaction from the issuing institution to the recipient on the Bitcoin blockchain that includes the hash of the certificate itself”.*
2. cert-viewer/verifier: series de componentes en (.js y .py) que permiten visualizar la información del certificado. Igualmente contienen una serie de funciones (*.py, *.js) para verificar (autenticidad) el certificado, la funciones toman como input el certificado y la transacción sobre el blochchain (bitcoin o etherum).

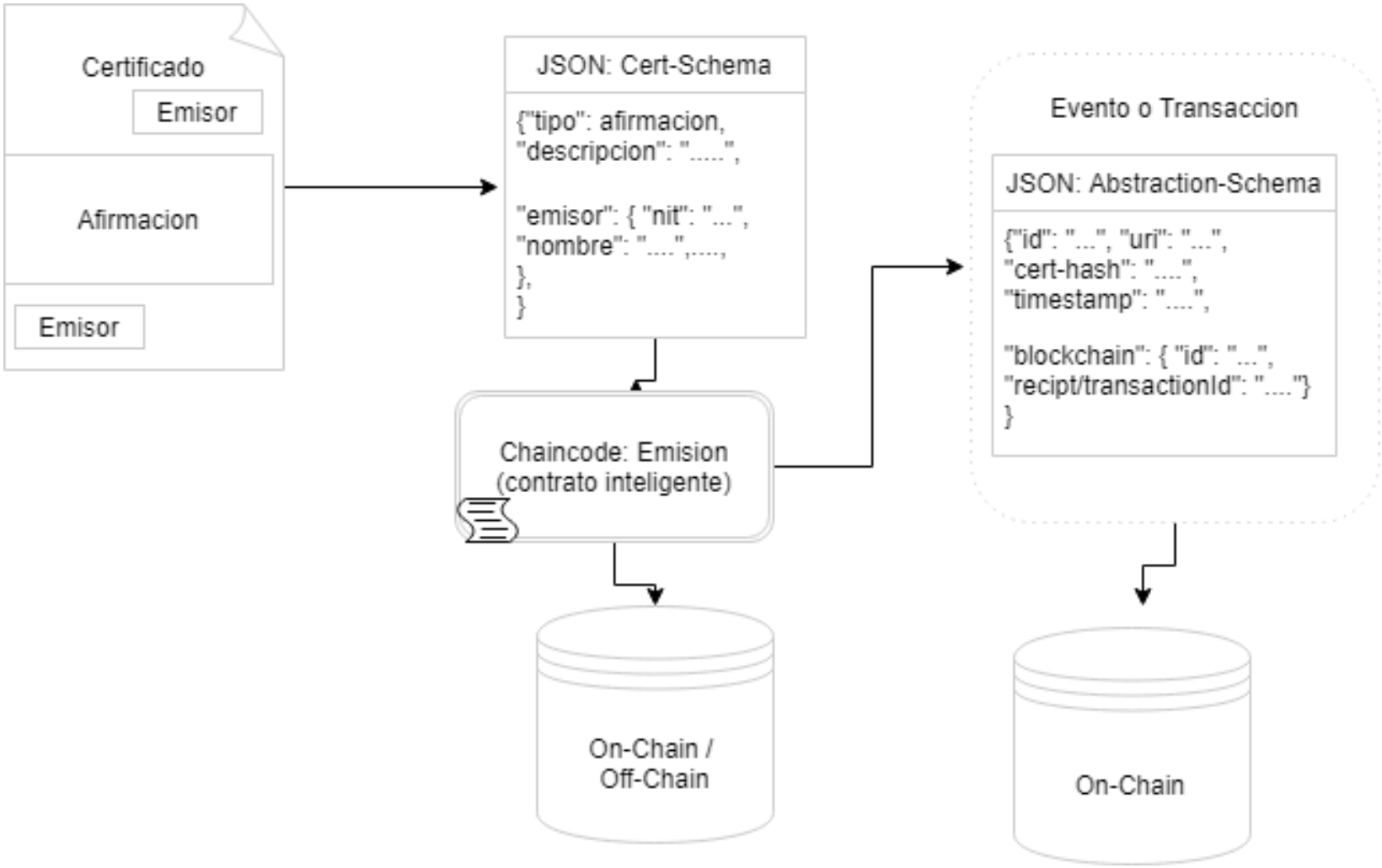
Antecedentes en Educación: OpenCerts

- GovTech Singapore
- Schema mas amplio que diploma (transcript).
- Componentes:
  - Emisión de certificado(s)
  - Validación de certificados: coherencia, integridad, recuperar contenido parcial o completo.
- JS
- Ethereum Blockchain

Estructura del proyecto

1. Explorar el tipo de certificados emitidos por entidades públicas para tener unos marcos de referencia.
2. Definir Estándar (Cert-Schema) con identificador único para diferentes blockchain (Abstraction-Schema).
3. POC, Composer Business Network Application (emisión y validación) para Blockchain permisionada. Cerrado, pero una primera aproximación al proceso
4. Experiencia de usuario y diseño de interfaces para la emisión y el validador universal.
5. Aplicación Frontend basada en Composer y Fabric para emisión.
6. Propuesta de red permisionada Hyperledger Fabric para entidades publicas, testnet.
7. Validador universal en python (BTC, ETH, Hyperledger Fabric, Sawthooth,…)

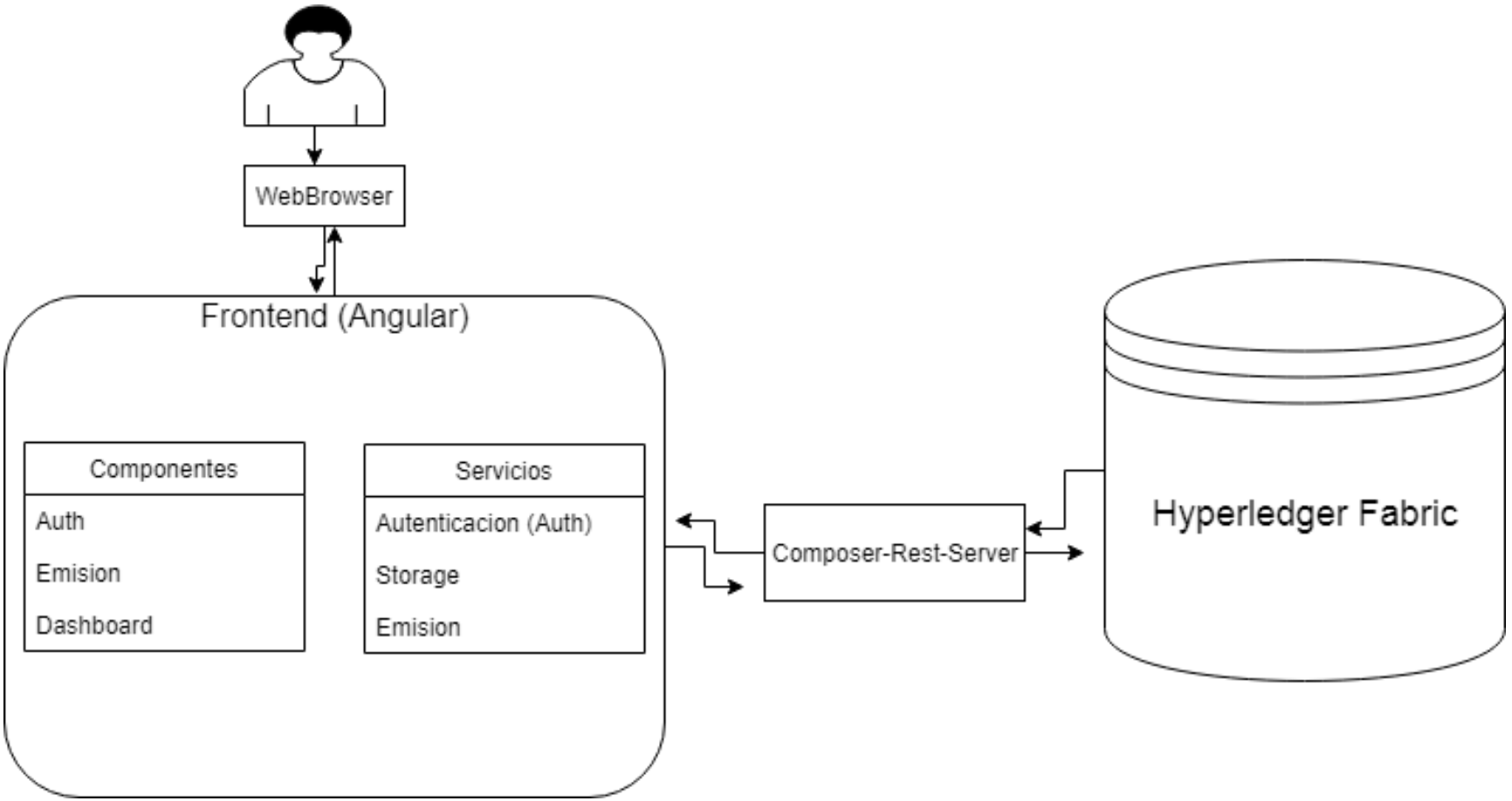
Proceso de emisión de un certificado



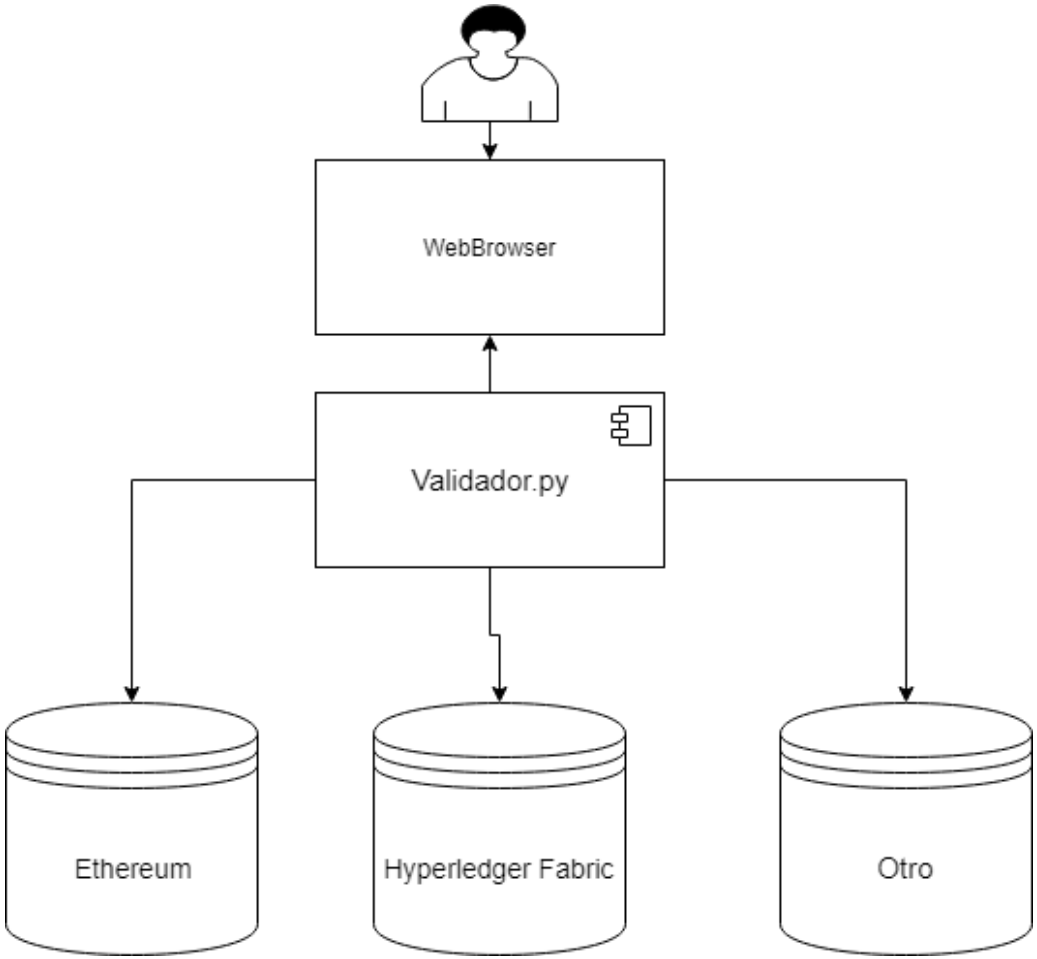
Experiencia de Usuario y diseño de las interfaces

- Diseño limpio, con tipografía y elementos visuales que se complementan y responden a los parámetros visuales dispuestos por las entidades para formularios que recolectan información y adaptable a la identidad visual de las mismas.
- Emisión: enfoque en equipos de escritorio (desktop).
- Verificación: *first mobile*

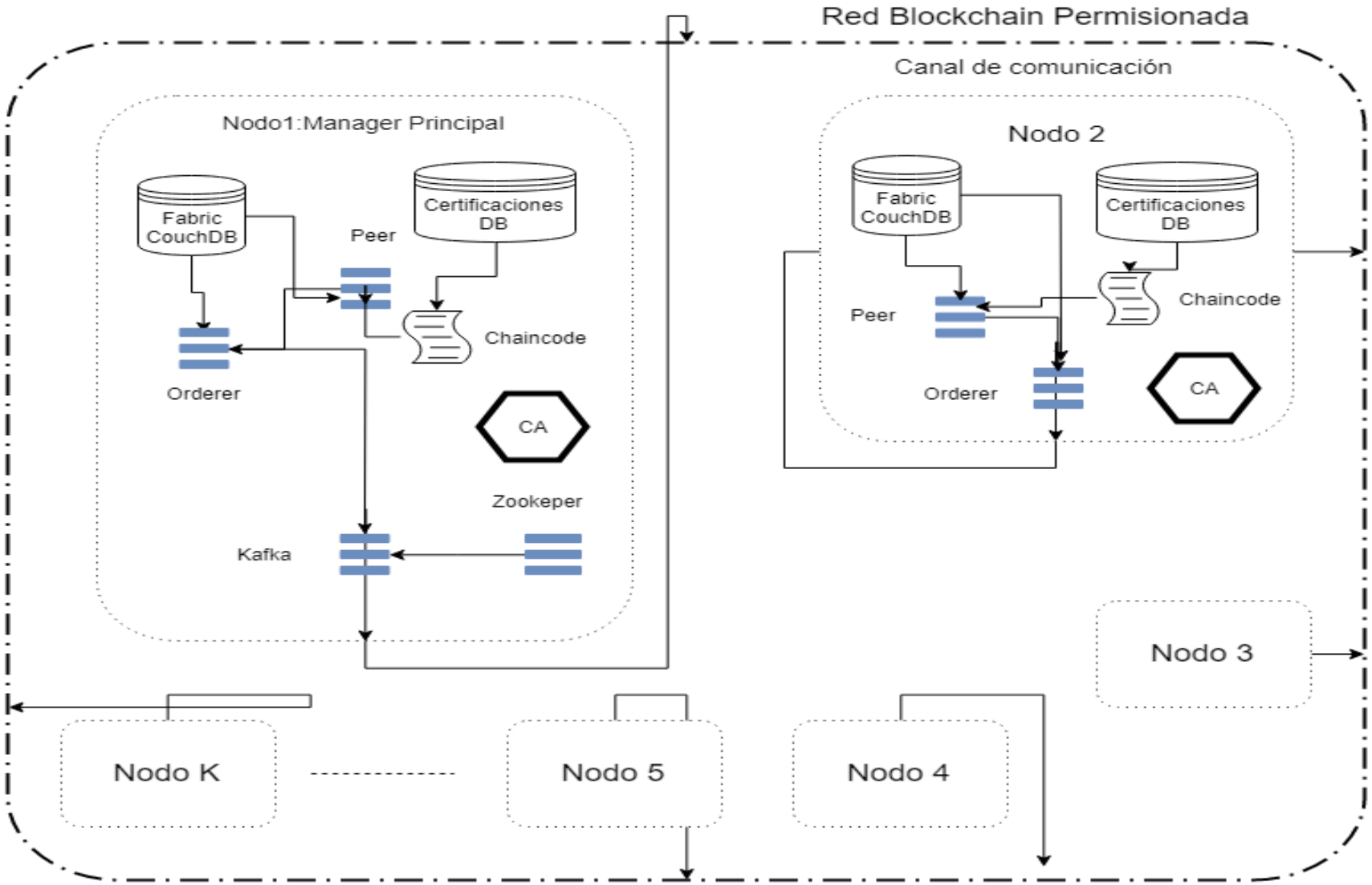
Arquitectura aplicación Emisor red permisionada



Arquitectura aplicación Validador General



Arquitectura red permisionada entidades publicas (escalable)



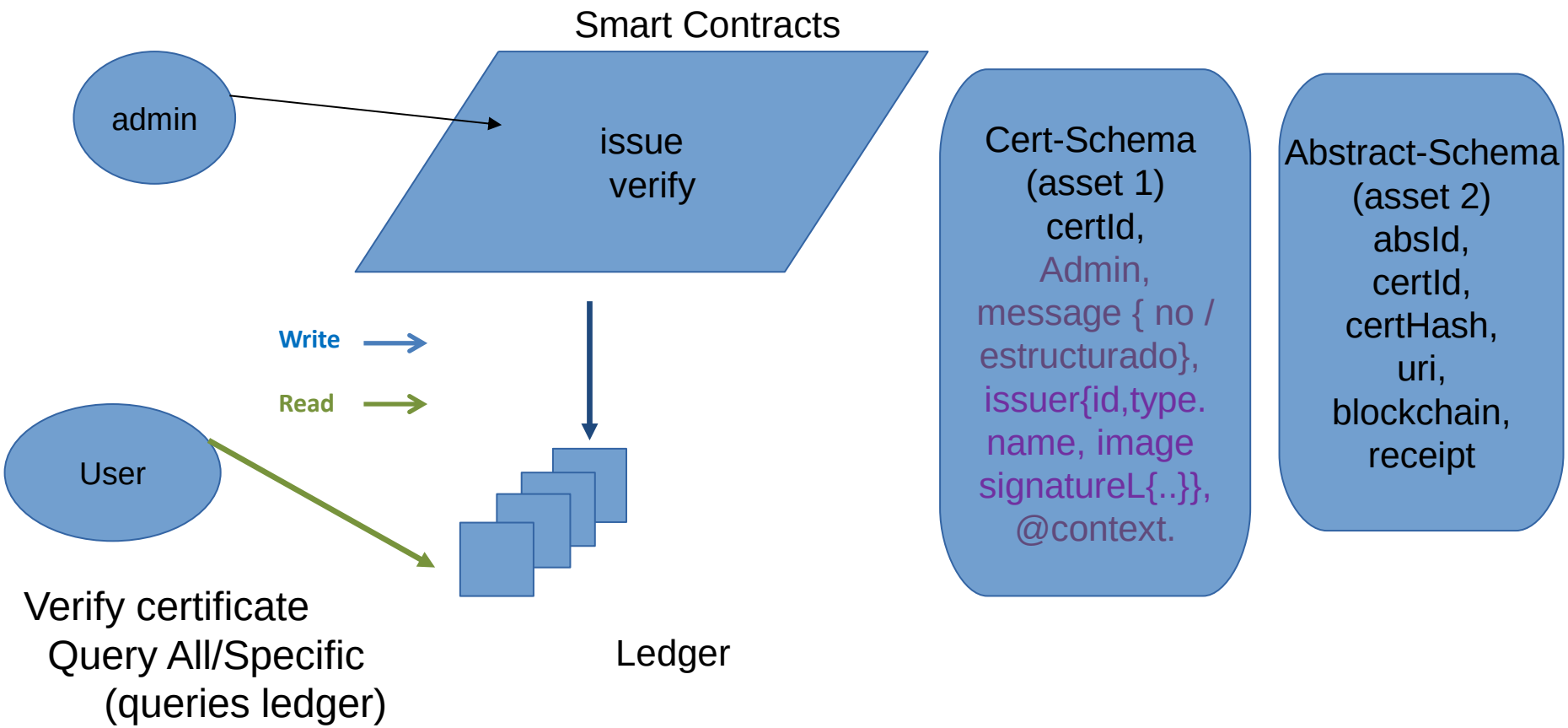
Componentes de proyectos anteriores

- Schema Blockcert
- Emision (Hyperledger), Js
- Validacion (Hyperledger), Js
- Repositorios
  - BNA: blockdegree, casaur
  - Frontend: blockdegree-frontend, casaur-frontend
- Validador general posibles ideas (Python)
  - blockchain-certificates/cert-verifier, bforos-wrapper, IPFS-Hyperledger-Integration

Tipos de certificados sector publico

- Procuraduría Antecedentes Disciplinarios.
- Invima Registro Sanitario.
- Certificado de la TRM Superfinanciera (validador).
- Contratos MinSalud (validador)

Business Network, picert.bna



Open Badges v2.0 Blockcerts-Extension

JSON schema