

Workshop

Identidad digital y Credenciales verificables con tecnología blockchain

Sesión 2



Blockchain básico

- Tecnología de ledger distribuido (DLT) que permite que múltiples participantes mantengan un registro seguro y transparente de manera **descentralizada**
- La estructura es una cadena de bloques en orden **cronológico** y enlazados usando **criptografía** que asegura la integridad de la data, así como la **inmutabilidad** de la cadena de bloques
- Los bloques contienen data o transacciones firmadas y cifradas criptográficamente que son visibles a todos los participantes de la red blockchain promoviendo la **transparencia** y **confianza**

Blockchain básico

- Una red de computadoras denominadas **nodos** participan en la escritura y validación de transacciones permitiendo un funcionamiento descentralizado
- La integridad de la cadena de bloques es garantizada empleando un **mecanismo de consenso** para la validación de transacciones y la generación de bloques (ejemplos: PoW, PoS, PoA)
- Existen diferentes tipos de cadenas de bloques, entre ellas Ethereum

Blockchain básico

- Redes blockchain basadas en el protocolo Ethereum emplean una máquina virtual: *Ethereum Virtual Machine* (**EVM**) que permite ejecutar código en forma de **contratos inteligentes**, procesar **transacciones** y mantener el **estado** de la cadena de bloques
- Los **contratos inteligentes** permiten **automatización** de procesos con reglas de negocio claramente establecidas que pueden ser **accionadas** por ciertas condiciones
- La naturaleza **inmutable** y **transparente** de una cadena de bloques hace que esta tecnología sea atractiva para crear y mantener **registros de confianza**

Tipos de redes blockchain ISO/TC 307*

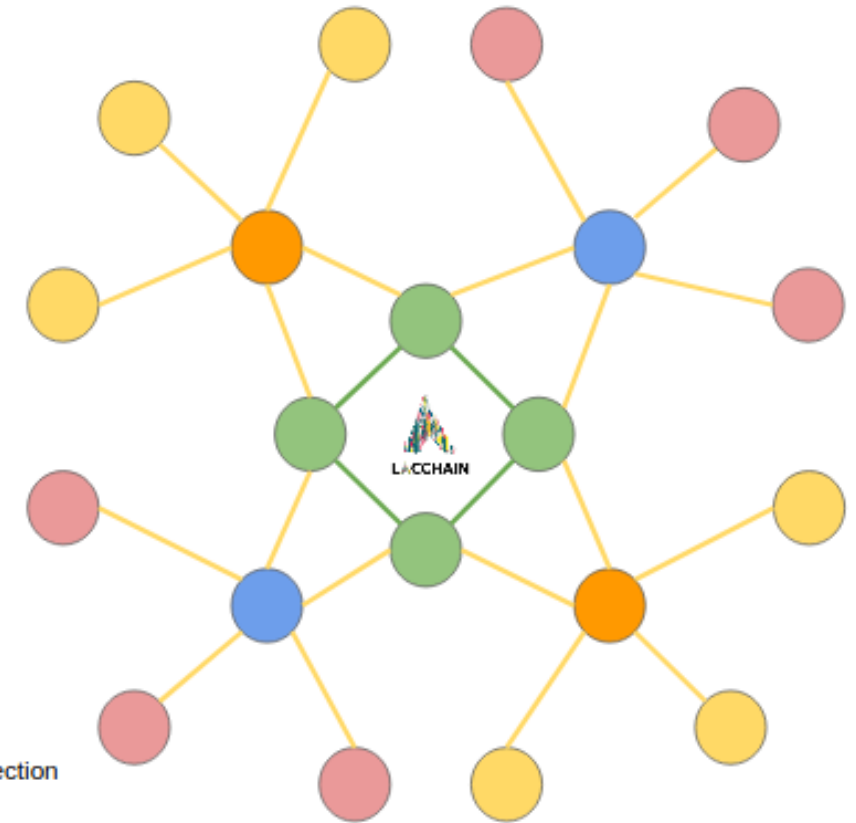
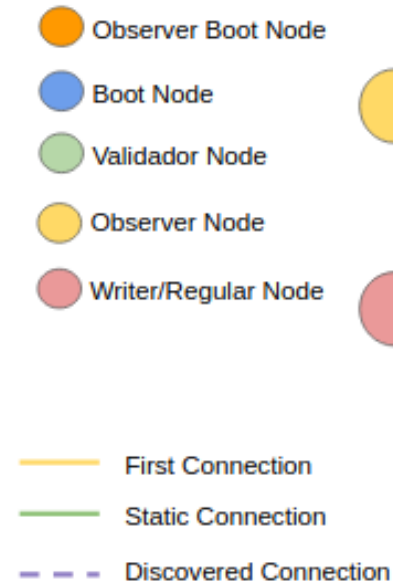
No permissionadas (criptos)	Permisionadas privadas (IBM)	Permisionadas públicas (LACChain)
Publicas (abiertas) ✓	Publicas (abiertas) ✗	Publicas (abiertas) ✓
Descentralizadas ✓	Descentralizadas ✗	Descentralizadas ✓
Transparentes ✓	Transparentes ✗	Transparentes ✓
Bajo costo transaccional ✗	Bajo costo transaccional ✓	Bajo costo transaccional ✓
Sin cripto asociada ✗	Sin cripto asociada ✓	Sin cripto asociada ✓
No anónimas (regulación habilitada) ✗	No anónimas (regulación habilitada) ✓	No anónimas (regulación habilitada) ✓
Privacidad habilitada ✗	Privacidad habilitada ✓	Privacidad habilitada ✓

* <https://www.iso.org/committee/6266604.html>

Blockchain básico

- LACChain red público-permisionada <https://lacnet.lacchain.net/documentation/>
- Nodos <https://lacnet.lacchain.net/our-networks-list-nodes/>
- Topología <https://lacnet.lacchain.net/topology/>

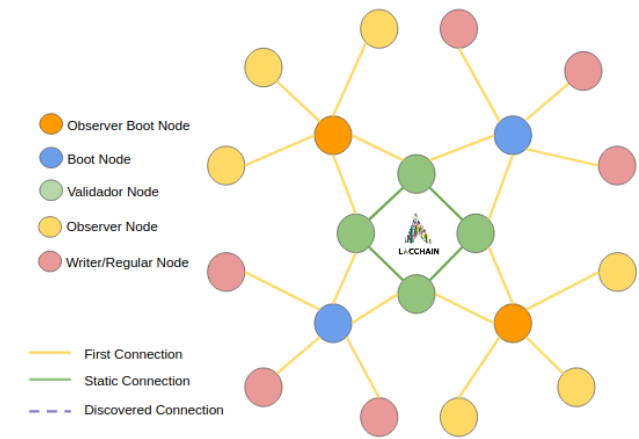
La topología describe los nodos y su rol en la red ➡



Topología de las redes LACChain

La topología describe los nodos y su rol en la red blockchain, según su rol se clasifican en nodos **Core** y nodos **Satélite**

- Los nodos **Core** son esenciales en la operación de la red, consisten de nodos *Boot* y nodos *Validadores*
- Los nodos **Satélite** consisten de nodos *Escritores* y *Observadores*
- Los nodos *Boot* actúan como enlace entre los nodos *Validadores* y nodos *Escritores/Observadores*, por lo tanto:
 - * Escuchan a los nodos *escritores* que transmiten transacciones a la red, que a su vez transmiten las transacciones a los nodos *validadores*
 - * Actualizan a los nodos *escritores/observadores* con los nuevos bloques generados por los nodos *validadores*
- Los nodos *validadores*:
 - * Participan en el protocolo de consenso, son responsables de la generación de nuevos bloques
 - * Están conectados entre sí y a los nodos *boot* por razones de seguridad y eficiencia en la operación de la red blockchain
- Los nodos *observadores* únicamente leen la red de bloques (ledger)



Infraestructura de Claves Públicas (PKI)

- Public Key Infrastructure (PKI) usa criptografía asimétrica que emplea un par de llaves (pública y privada)
- Es el conjunto de tecnologías, procesos, políticas y procedimientos para la creación, uso, almacenamiento, distribución y revocación de certificados digitales y claves públicas
- Un certificado digital identifica a un individuo u organización y asocia sus claves públicas, permitiendo autenticarse, así como cifrar y firmar datos
- Los protocolos HTTPS (SSL/TLS) y SSH son casos de uso de PKI
- Componentes relevantes de PKI
 - Autoridad certificadora
 - Directorio público
 - Registro de certificados
 - Certificados revocados

Autoridad Certificadora (CA)

- Certificate Authority (CA)
- Agentes de confianza que emiten certificados para vincular las identidades de organizaciones o individuos con sus claves públicas
- Autoridad certificadora realiza un proceso de verificación de la organización o individuo que realiza una petición para un certificado digital
- Una vez verificada la organización o individuo, la CA emite un certificado X.509 firmando información particular como el nombre de la organización/individuo, su clave pública y el período de validez del certificado

Certificado X.509

- Un certificado X.509¹ es un formato estándar para certificados de llaves públicas soportado por el International Telecommunications Union (ITU) de las Naciones Unidas
- Es un documento digital que asocia de manera segura pares de llaves criptográficas con identidades como sitios web, individuos u organizaciones
- La especificación RFC5280¹ de la IETF² describe:
 - * Certificado X.509 v3
 - * Lista de revocación de certificados (CRL)
 - * Algoritmo para validación de la ruta del certificado X.509

1. <https://datatracker.ietf.org/doc/html/rfc5280>

2. <https://www.ietf.org/>

Autoridad Certificadora (CA)

- En el certificado X.509 se puede verificar la firma de la Autoridad Certificadora (emisor) lo cual permite verificar la integridad y validez del certificado, así como su clave pública
- Las Autoridades Certificadoras pueden emitir y firmar certificados para otros CA que a su vez emiten certificados a organizaciones o individuos creando una cadena de verificación que se denomina **Cadena de Confianza**

Identidad Digital



A person stands on a rock in a river, looking towards a large dam in the background. The scene is overlaid with a semi-transparent green filter.

Billeteras digitales para la inclusión y la sostenibilidad en la era de la Web3

LACCHAIN

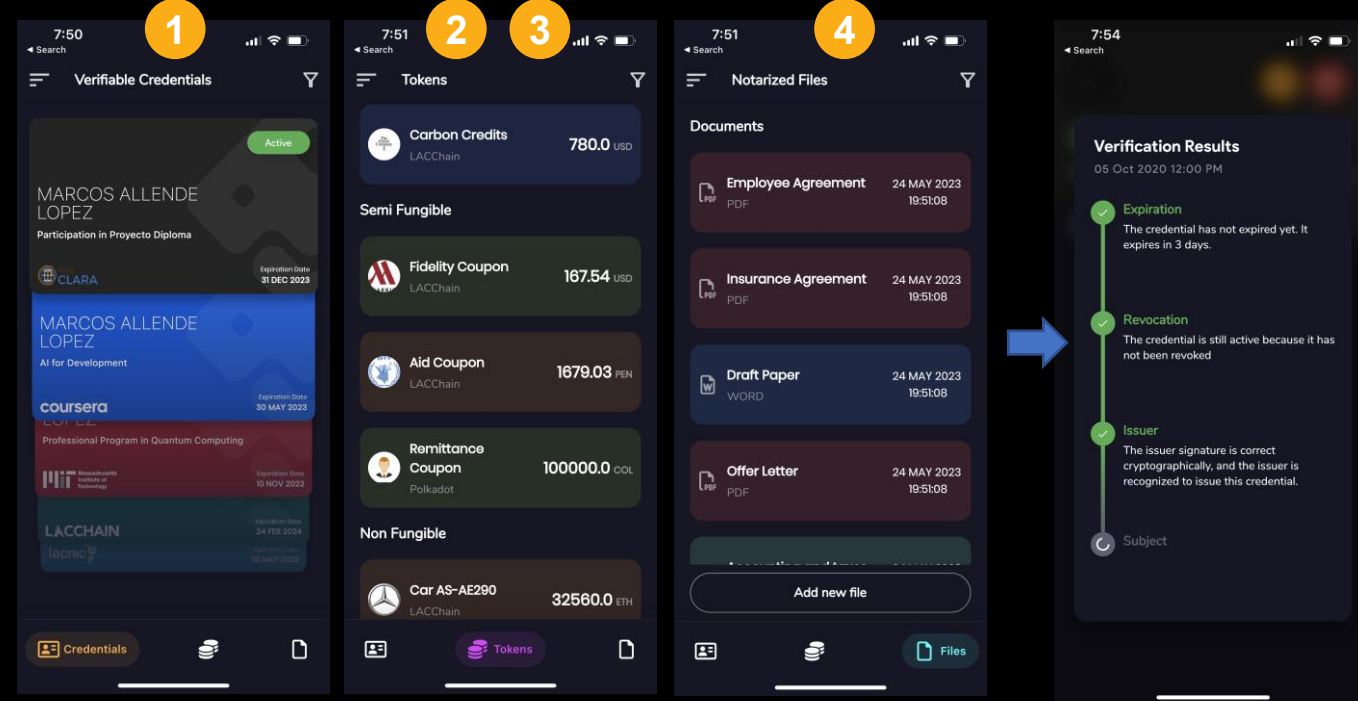


Billetera Digital

Mi billetera y documentos



Mi billetera digital



LACCHAIN

IDB | LAB



Workshop de Identidad digital y Credenciales Verificables

Agenda

- Billeteras digitales
- Registro de confianza
- Billetera digital web
- Billetera digital móvil
- Identidad digital
- Artefactos de Identidad digital

Billeteras y Agentes digitales

- Aplicaciones que permiten a los usuarios finales administrar sus credenciales verificables y claves criptográficas asociadas
- Permiten a los usuarios demostrar información relacionada con su identidad, y cuando sea posible revelar selectivamente atributos particulares de sus credenciales

Identidad digital

- Identidades descentralizadas (DIDs)
- Credenciales verificables (VCs)

Billetera Digital Móvil



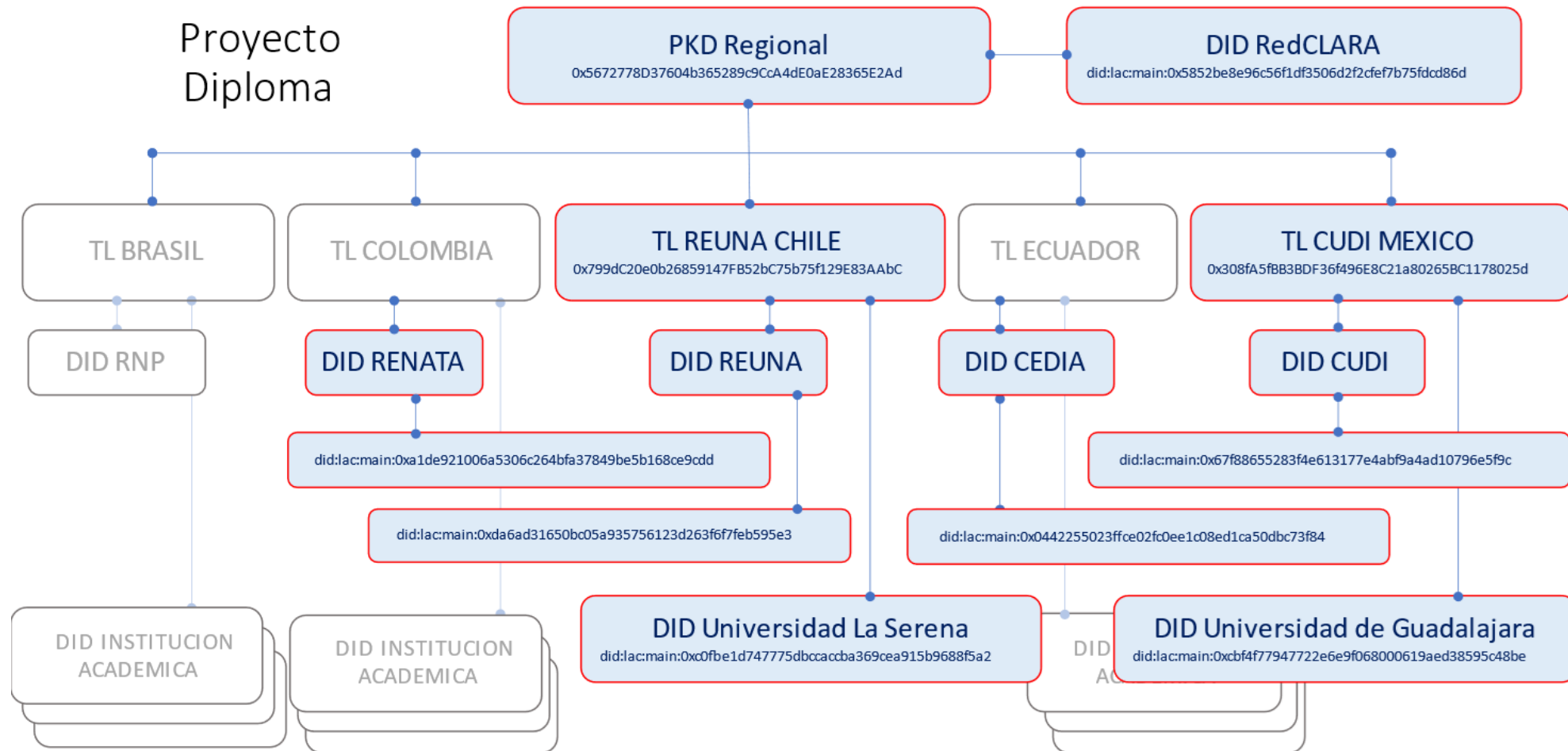
Navegación billetera digital móvil

- DID
- Emisores
- Credenciales
- Verificadores

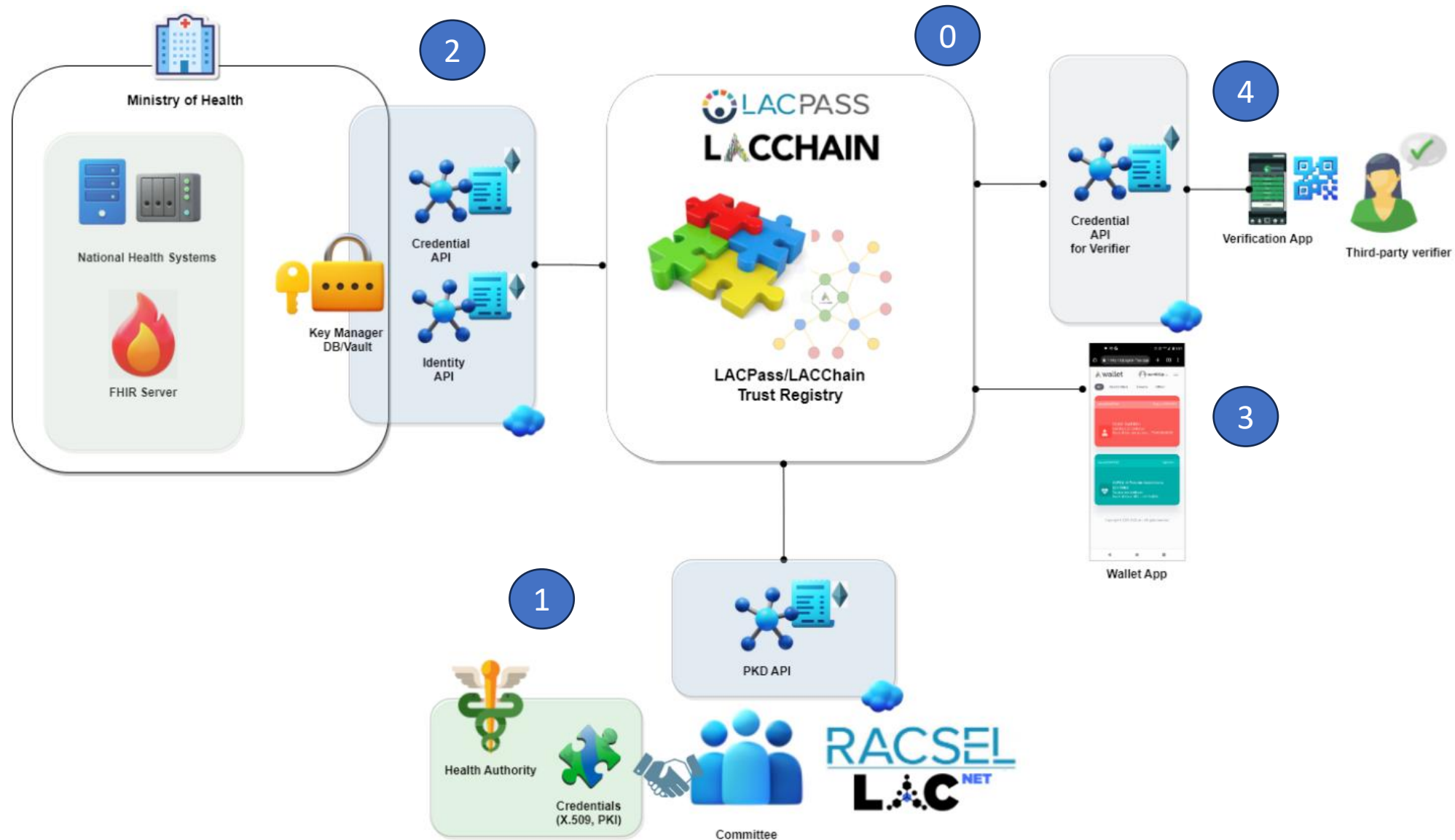
Registro de confianza

- Directorio de registros de individuos u organizaciones (entidades) mantenido por una autoridad confiable con fines de transparencia y gobernanza
- Los registros contenidos en este directorio pueden ser usados para identificar entidades que participan en ciertos contextos
- Los registros contienen información particular de las organizaciones o individuos, así como los certificados digitales y claves públicas asociadas

Registro de confianza regional



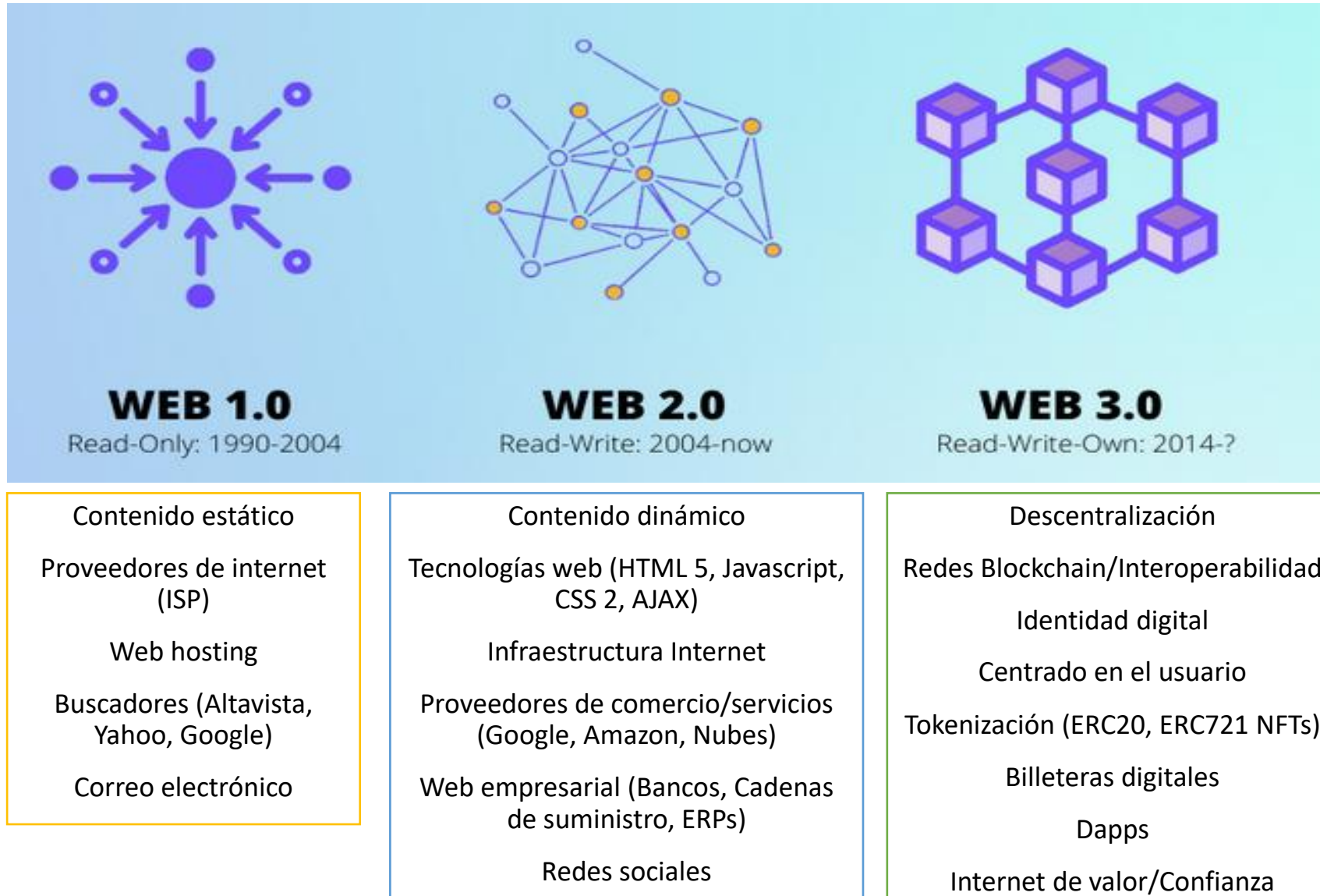
Escenario LACPass



Web 3.0 básico

- Evolución de la tecnología Web 2.0 que considera la descentralización empleando tecnologías blockchain
- Autenticación y verificación por servicios propietarios y autoridades centralizadas son retos en la evolución de la tecnología web
- La capacidad descentralizada de la tecnología blockchain permite una alternativa ligera a los mecanismos de autenticación usando DIDs y VCs para servicios y aplicaciones
- La tecnología Web 3.0 está orientada y centrada en el usuario
- Permite crear ecosistemas descentralizados usando tecnología blockchain
- Permite crear ecosistemas con economías basadas en tokens

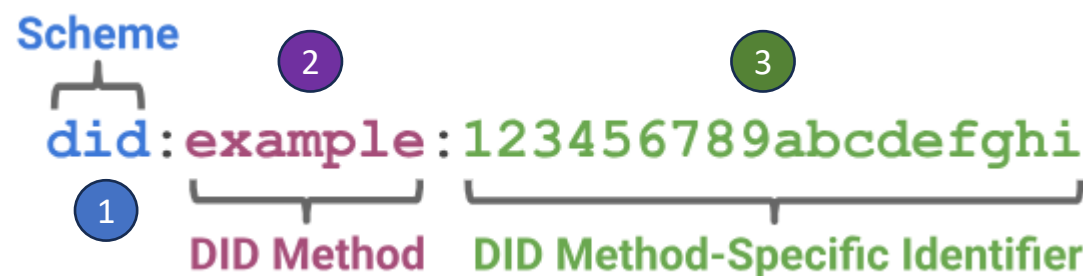
Web 3.0 básico



Identificador descentralizado (DID)

- Estándar soportado por el World Wide Consortium (W3C)¹
- Según W3C, un DID es un *nuevo tipo de identificador que permite una identidad digital descentralizada y verificable*
- Definido como un identificador global y único que no requiere una autoridad centralizada de registro y generalmente se genera o registra criptográficamente
- Un DID identifica cualquier sujeto (individuo, organización, entidad, modelo de datos, entidad abstracta)
- Un DID es un URI que asocia un sujeto DID con un **documento DID** que permite interacciones confiables con el sujeto y contiene información de los métodos de autenticación para probar la propiedad del DID
- Un DID es un string de texto que consiste de tres partes:

1. Identificador del schema URI did
2. Identificador del método DID
3. Identificador específico al método DID



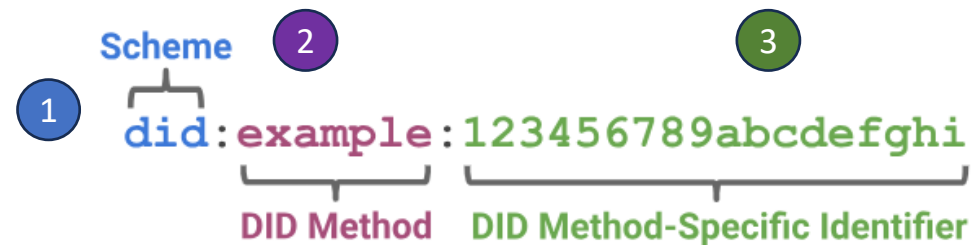
- Un DID también puede representar un par de llaves (pública y privada) en una red basada en Ethereum

1. <https://w3c.github.io/did-core/>

Identificador descentralizado (DID)

Un DID es un string de texto que consiste de tres partes:

1. Identificador del schema URI did
2. Identificador del método DID
3. Identificador específico al método DID



`did:lac:openprotest:0xd9854190ad3b2c460d38fa63397bb9770cdf7277`

Artefactos de Identidad digital

Smart contracts

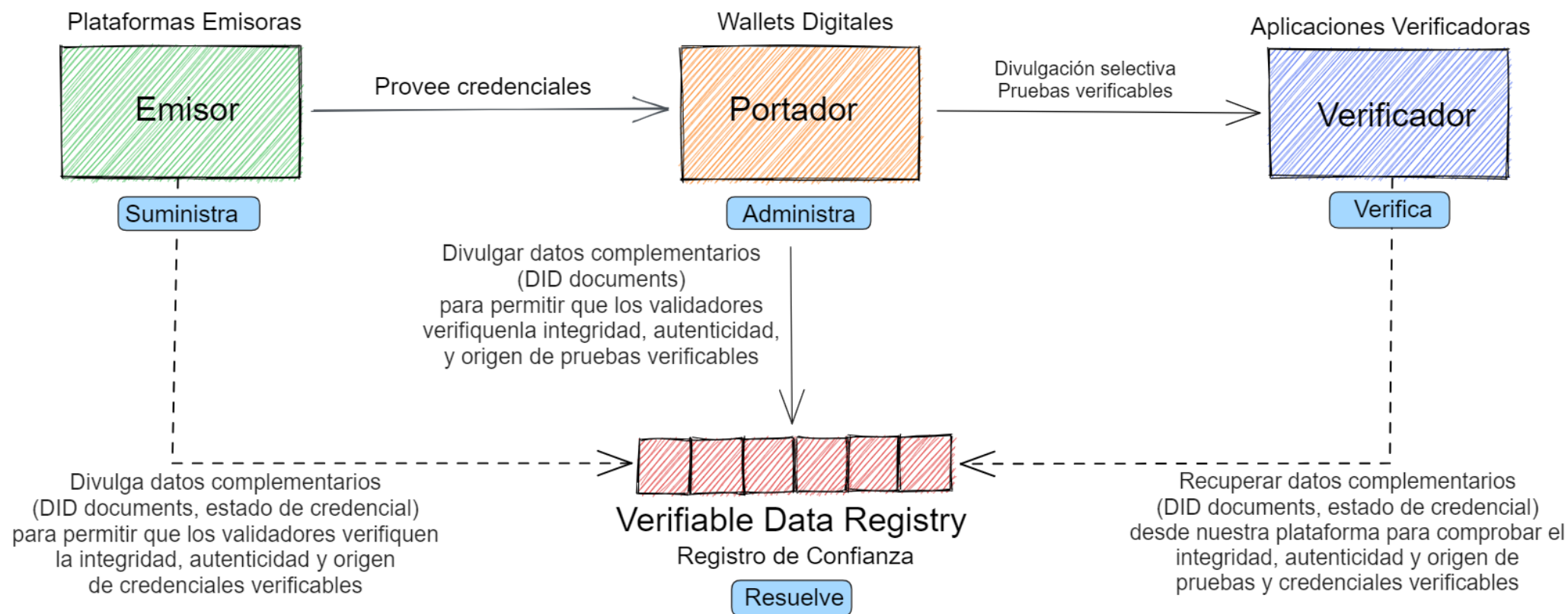
<https://lacnet.com/decentralized-identifiers/>

- DID Registry
- DID Resolver
- Credential Registry
- Claims verifier
- PKD/TL (Registro de confianza)

Mailbox

<https://lacnet.com/verifiable-credentials/>

Modelo de emisión/verificación de credenciales



Verificación de una Credencial Verificable (Smart contracts)

1. DID Registry
2. Credential Registry
3. Claims Verifier
4. PKD
5. TL

Credenciales verificables

- Estándar del W3C <https://www.w3.org/TR/vc-data-model/>
- Una credencial verificable es un archivo digital:
 - Contiene una o más declaraciones de valor (por ejemplo, nombre, fecha de nacimiento, género, calificaciones, ciudadanía, etc.) denominados **claims**
 - Sobre una entidad denominada *sujeto* o *portador* o *titular*
 - Emitida por otra entidad denominada *emisor*
 - Verificable por cualquier otra entidad denominada *verificador*
- El titular de una credencial verificable es el identificador descentralizado (DID) de la entidad a la que corresponden los atributos de la credencial
- Cambio de paradigma ofrece a los usuarios mayor soberanía sobre su información y empoderamiento para gestionar su identidad digital

Credenciales verificables

Proyecto Diploma

- Repositorio de credenciales <https://github.com/lacchain/vc-repository>

Proyecto Diploma

```
7165 {
7166   "claimsVerifier": "0x1586478D4114c944125491134f6415bF06b2Cela",
7167   "trustedList": "0x04cDA9461318F26d2758EF0c57A702911AC95051",
7168   "data": {
7169     "name": "Certificado Título",
7170     "expirationDate": "2028-12-15T16:04:16.297Z",
7171     "subject": {
7172       "did": "did:lac:openprotest:0xd9854190ad3b2c460d38fa63397bb9770cdf7277",
7173       "givenName": "Antonio",
7174       "familyName": "Leal Batista",
7175       "email": "antonio.leal@gmail.com",
7176       "nationalId": "987654321"
7177     },
7178     "signers": [
7179       {
7180         "did": "did:lac:main:0x1242f0480065c925cc46afc0f4cc184c9ec7cd22",
7181         "name": "María Pérez Soto - Directora de Docencia"
7182       },
7183       {
7184         "did": "did:lac:main:0x7836ccd039271d104c5140cc3875ac18124db335",
7185         "name": "Juan Soler Molina - Secretario General"
7186       }
7187     ],
7188     "diploma": {
7189       "title": "Ingeniero en Computación",
7190       "description": "Título",
7191       "category": "Computer and information sciences",
7192       "modality": "modalidad",
7193       "url": "http://admisión.userena.cl/carreras/ingenieria-en-computacion",
7194       "issued": "2023-12-15T16:04:16.297Z",
7195       "educationalInstitution": "Universidad de La Serena",
7196       "courseID": "2534",
7197       "approved": true,
7198       "grade": "6.9",
7199       "campusName": "La Serena",
7200       "city": "CL",
7201       "country": "Chile",
7202       "recordID": "1294;99572;3079",
7203       "hashQR": "https://phoenix.cic.userena.cl/verificacion.php?doc=052%2ByEb4Wo8pwmag2yJLo2fShnLKVo2VN%2B9NQWuLUB8%3D"
7204     }
7205   }
7206 }
```

Credencial
verificable

Proceso de Verificación de una CV

1. Verificación de la billetera digital (certificada)
2. Verificación de la integridad (no modificada)
3. Verificación del estatus (no revocada)
4. Verificación del emisor (registro de confianza)
5. Verificación del presentador
6. Verificación de los claims

Antecedentes

Escenario para emisión y verificación de credenciales académicas (Proyecto Diploma)

