Análisis del modelo de Identidad Auto-Soberana

"Tesis presentada para obtener el grado de

Magister en Redes de Datos"

Autor: Facundo Nicolás Montero

Director: Hugo Dionisio Ramón

Co Director: Adrián Pousa

Facultad de Informática – Universidad Nacional de La Plata

Mes y año: Mayo 2024

A mis padres por haberme dado la vida y por su constante apoyo a lo largo de ella.

Agradecimientos

Quiero agradecer al Mg. Hugo Ramón (Director de Tesis) y al Dr. Adrián Pousa (Codirector de Tesis) por su apoyo y guía a lo largo del desarrollo de la presente tesis de maestría.

Me gustaría también agradecer y resaltar la importancia de las universidades públicas de nuestro país, y con especial cariño a la Universidad Nacional del Noroeste de la Provincia de Buenos Aires, lugar que me dio la oportunidad de estudiar, trabajar y formarme profesionalmente.

Resumen

Identidad Auto-Soberana (IAS) nace como respuesta a la demanda de control y autonomía de identidad en el mundo digital por parte de los usuarios. En este paradigma, es el propio usuario quien almacena, resguarda y administra sus credenciales e identificadores en repositorios personales evitando tener que recurrir a bases de datos de los proveedores de servicios.

El desarrollo de soluciones y estándares de Identidad Auto-Soberana se encuentran en pleno auge, y se espera que sea una de las principales tecnologías unificadoras entre el control de identidad de las personas y el mundo descentralizado.

Durante el desarrollo de este trabajo, se describirán los requerimientos tecnológicos y no tecnológicos necesarios para realizar la implementación de una solución de IAS.

Se analizará el estado del arte de las tecnologías más relevantes de la actualidad que están llevando a cabo gobiernos, organizaciones no gubernamentales (ONGs) y empresas sobre IAS.

Luego se expondrá sobre las herramientas Hyperledger Indy y Aries con las que se desarrollará un prototipo de solución IAS en un ambiente controlado.

La expectativa es poder brindar una primera experiencia en el uso de IAS con éstas tecnologías dentro del ámbito académico donde el tesista se desempeña, del cual seguramente surgirán más proyectos de I+D+i (Investigación, Desarrollo e Innovación) en el futuro.

Abstract

Self-Sovereign Identity (SSI) was born in response to the demand for identity control and autonomy in the digital world by users. In this paradigm, it is the user himself who stores, safeguards and manages his credentials and identifiers in personal repositories, avoiding having to resort to service provider databases.

The development of Self-Sovereign Identity solutions and standards is booming, and is expected to be one of the main unifying technologies between people's identity control and the decentralized world.

During the development of this work, the technological and non-technological requirements necessary to carry out the implementation of an SSI solution will be described.

The state of the art of the most relevant technologies currently being carried out by governments, non-governmental organizations (NGOs) and companies on SSI will be analyzed.

Then, the Hyperledger Indy and Aries tools will be discussed, with which an SSI solution prototype will be developed in a controlled environment.

The expectation is to be able to provide a first experience in the use of SSI with these technologies within the academic field where the thesis student works, from which more R+D+i (Research, Development and Innovation) projects will surely emerge in the future.

INDICE GENERAL

Agradecimientos 3

Resumen 4

Abstract 5

1. INTRODUCCIÓN 12

1.1 OBJETIVOS 13

1.2 MOTIVACIÓN 14

2. ESTADO DEL ARTE 16

3. MARCO TEÓRICO 20

3.1 Identidad 20

3.2 Identidad Digital 21

3.3 Modelos de Identidad 23

3.3.1 Modelo Centralizado 23

3.3.2 Modelo Federado 24

3.3.3 Modelo Distribuido 25

3.4 Identidad Auto-Soberana 27

3.4.1 Libro Mayor Distribuido y Blockchain 30

3.4.2 Identificadores Descentralizados 33

3.4.3 Credenciales y Presentaciones Verificables 42

3.4.4 Billeteras Digitales y Agentes 48

3.4.5 Sistema de Administración de Claves Descentralizado 53

4. TRABAJO EXPERIMENTAL 55

4.1 Tecnologías utilizadas 56

4.1.1 Hyperledger Indy 56

4.1.2 Hyperledger Aries 59

4.1.3 Lissi ID-Wallet 63

4.2 Diseño de Arquitectura IAS 64

4.2.1 Prueba de concepto 65

4.2.2 Registro del DID y Documento DID 66

4.2.3 Definición del esquema a utilizar 69

4.2.4 Invitar a los usuarios a conectar 72

4.2.5 Emitir Credencial Verificable 75

4.2.6 Realizar una prueba de Presentación Verificable 77

4.2.7 Revocar una Credencial Verificable 79

5. CONCLUSIONES 82

6. TRABAJOS A FUTURO 84

7. REFERENCIAS 85

INDICE DE FIGURAS

Ilustración 1 - Esquema de Microsoft Entra 16

Ilustración 2 - Proyectos de Hyperledger 17

Ilustración 3 - Modelo Centralizado 23

Ilustración 4 - Modelo Federado 24

Ilustración 5 - Modelo Distribuido 26

Ilustración 6 - Tecnologías de Capa 8 28

Ilustración 7 - Lista de bloques encadenada 32

Ilustración 8 - Ejemplo de un DID y sus estructura resaltada 33

Ilustración 9 - Ejemplo de un Documento DID 34

Ilustración 10 - Arquitectura DID 35

Ilustración 11 - Ejemplo de un id definido en un Documento DID 36

Ilustración 12 - Ejemplo de un Documento DID 37

Ilustración 13 - Ejemplo de un controlador definido en un Documento DID 38

Ilustración 14 - Algunos de los 166 métodos DIDs 39

Ilustración 15 - Ejemplo de consulta de atributos en la especificación Sovrin 39

Ilustración 16 - Distintos escenarios donde aplicar Resolución de DIDs 41

Ilustración 17 - Grafo de Claims de una entidad 42

Ilustración 18 - Gafo de los componentes de una Credencial Verificable 43

Ilustración 19 - Grafo de una Presentación Verificable 45

Ilustración 20 - Relación entre los actores en el ecosistema de Credenciales Verificables 47

Ilustración 21 - Imagen de una Billetera Digital para celulares y sus credenciales 48

Ilustración 22 - Arquitectura conceptual de una Billetera Digital y un Agente 49

Ilustración 23 - Ejemplo de un mensaje DIDComm en formato de texto plano 52

Ilustración 24 - Encapsulamiento de mensajes DIDComm 52

Ilustración 25 - Generación del Identificador único en KERI 54

Ilustración 26 - Interfaz pública del estado de la DLT BCovrin Test 58

Ilustración 27 - Descripción general de la arquitectura propuesta por ACA-Py 59

Ilustración 28 - Interfaz de comunicación del agente ACA-Py 60

Ilustración 29 - Controladora desarrollada para comunicarse con el agente. 61

Ilustración 30 - Billetera Lissi ID-Wallet ejecutándose en un celular 63

Ilustración 31 - Diseño de Arquitectura propuesta y sus componentes 64

Ilustración 32 - Consulta de DID del agente 66

Ilustración 33 - Registro del DID en la DLT 67

Ilustración 34 - Objeto ATTRIB 68

Ilustración 35 - ID del Esquema y Definición de Credenciales a utilizar 69

Ilustración 36 - Registro del Esquema en la DLT 70

Ilustración 37 - Registro del Claim Definiton en la DLT 71

Ilustración 38 - Código QR para invitar al usuario a conectar 72

Ilustración 39 - Mensaje de conexión 73

Ilustración 40 - Conexiones y sus estados 73

Ilustración 41 - Mensaje de texto recibido 74

Ilustración 42 - Carga de datos de la Credencial Verificable 75

Ilustración 43 - Credencial ofrecida al usuario..... 76

Ilustración 44 - Presentación Verificable emitida 77

Ilustración 45 - Proof Request superada..... 78

Ilustración 46 - Índice del Archivo de Colas y cálculo del Acumulador 79

Ilustración 47 - Cambio del valor del acumulador luego de revocar credenciales 80

1. INTRODUCCIÓN

Desde su concepción Internet fue creada sin un sistema de identificación de usuarios ni estándar para identificación de personas, lo que llevó a que cada sitio y sistema web resuelva el problema de la identificación de forma independiente, a lo cual hoy en día nos encontramos con múltiples soluciones a este problema, cada una con sus ventajas y desventajas. Además, con el crecimiento del impacto de Internet en la vida de las personas y la multitud de servicios que actualmente se ofrecen en ella, nos encontramos con que las personas deben poseer múltiples credenciales para cada servicio, y en muchos de ellos pueden llegar a tener más de una identificación con diferentes niveles de acceso y permisos.

A estos problemas se suma que la información que vuelcan las personas en los sistemas centralizados de identificación, en poder de empresas u organizaciones, muchas veces se utiliza con fines comerciales o se vuelven un blanco atractivo para ciberdelincuentes.

Ante esta situación nace el concepto de Identidad Auto-Soberana, un nuevo paradigma de gestión de identidad que tiene como objetivo principal dar a las personas el control sobre su identidad digital, sus datos personales relacionados a ésta y cómo se utilizan.

En esta Tesis para el grado de Magister en Redes de Datos se pretende investigar sobre el estado del arte de las tecnologías y proyectos desarrollados alrededor de Identidad Auto-Soberana y brindar una prueba de concepto dentro del ámbito académico, del cual seguramente surgirán más proyectos de I+D+i (Investigación, Desarrollo e Innovación) en el futuro.

1.1 OBJETIVOS

El objetivo de la presente tesis es el de estudiar el concepto de IAS, analizando cuáles son sus componentes necesarios para poder hacer su implementación, en particular haciendo foco en el análisis de las tecnologías y desarrollos que la soportan, tanto soluciones de software para generar, almacenar y verificar credenciales, como mecanismos de prueba de identidad, nuevos protocolos de comunicación y estándares asociados.

Se investigará el estado del arte de las nuevas tecnologías desarrolladas específicamente para el despliegue de una implementación de IAS integral y casos de uso de las mismas.

Por último, dentro del ambiente académico universitario donde se desarrolla profesionalmente el tesista, se buscará implementar y analizar un prototipo funcional de identidad digital auto soberana para alumnos de la universidad basado en las herramientas de software libre disponibles y que garantice los siguientes puntos:

- Poder generar un esquema de credenciales que describa aptitudes académicas relevantes.
- Que las credenciales emitidas por las organizaciones sean de confianza, pudiéndose validar contra alguna tecnología del tipo Libro Mayor Distribuido (DLT) como blockchain.
- Que los individuos tengan control sobre las mismas pudiéndolas administrar desde una billetera virtual.
- Que se las puedan validar contra registros públicos, sin necesidad de interactuar con el emisor de las mismas.

El aporte de esta tesis será el de poder brindar una primera experiencia en el uso de IAS dentro del ámbito académico con algunas de las herramientas que se encuentran actualmente disponibles para su despliegue analizando la maduración de las mismas y detallando los desafíos encontrados. Se espera surjan más proyectos de I+D+i enmarcando en el uso de ésta tecnología, que se encuentra en pleno auge y desarrollo.

1.2 MOTIVACIÓN

Actualmente existen múltiples modelos y protocolos para la identificación de usuarios. Desde el clásico modelo centralizado, en el cual una herramienta de software administra una base de datos contra la que constatar las credenciales que presenta el usuario, pasando por modelos más modernos como los de identidad provista por terceros, en el cual hay entidades que funcionan como Proveedoras de Servicios que confían en otras llamadas Proveedoras de Identidad, actualmente implementada en protocolos ampliamente utilizados como Identificadores Abiertos (OpenID), Autorización Abierta (OAtuh) o Lenguaje de Marcado para Confirmaciones de Seguridad conocido como (SAML) [1].

Sin embargo, en estos modelos mencionados el usuario no es el verdadero dueño de sus datos identificatorios, ya que no los almacena ni controla, y normalmente sólo posee un usuario y contraseña para autenticarse, estando el resto de sus metadatos e información administrados de forma centralizada por la misma entidad que brinda el servicio, y de que el usuario también depende para su resguardo y validación.

En los últimos años se viene desarrollando el modelo de Identidad Auto-Soberana, el cual propone que el usuario es el que tiene la gobernanza de su identidad digital y es el mismo usuario el que almacena y administra sus credenciales en repositorios personales, llamados billeteras virtuales, de manera segura y confiable. Este modelo presenta enormes ventajas, entre ellas, la capacidad del usuario de a la hora de presentar sus credenciales válidas para acceder a algún servicio, poder hacerlo presentando sólo la cantidad de información justa y necesaria que se requiera, sin necesidad de revelar todos los datos de su credencial [2].

En el modelo Identidad Auto-Soberana se propone la soberanía del usuario no en la emisión de las credenciales de identidad, sino en su administración y presentación. Estas credenciales serán emitidas a los usuarios por una entidad considerada de confianza como organizaciones o gobiernos, y otorgadas a través de un proceso de petición y entrega en conexiones peer-to-peer (punto a punto), de las cuales se almacenarán pruebas criptográficas de la emisión en una red distribuida, como por ejemplo, una blockchain contra la cual validar la autenticidad de dichas credenciales. Esto otorga la capacidad de que un tercero que quiera confiar en el

poseedor de credenciales lo pueda hacer contrastándolas directamente contra una cadena de bloques (blockchain) [3].

Motiva el desarrollo de esta propuesta de tesis el investigar sobre el desarrollo de este nuevo modelo de identificación distribuido, que empodera al usuario en la utilización de sus datos personales, analizando los nuevos protocolos y tecnologías desarrolladas y sus características para una posible adopción y utilización dentro del ambiente universitario, que sin duda alguna otorgará grandes beneficios a los usuarios y redefinirá los casos de uso de cómo éstos deben autenticarse frente a los sistemas que lo implementen, pasando del modelo clásico de credenciales tipo usuario y contraseña a uno en el que se utilicen credenciales almacenadas en billeteras virtuales.

2. ESTADO DEL ARTE

Desde mediados de la década del 2010 el concepto de Identidad Auto-Soberana comenzó a desarrollarse bajo la demanda de control y autonomía de identidad en el mundo digital por parte de los usuarios [4]. En la actualidad gracias a los avances tecnológicos e iniciativas públicas y privadas existen muchos proyectos que buscan contribuir a la inclusión social y económica de personas en situación de pobreza y vulnerabilidad a través del desarrollo de una implementación de IAS basada en blockchain.

En la actualidad existen distintas soluciones para implementar IAS basadas en nuevos protocolos de comunicación o que hacen uso de los ya existentes. Entre ellas podemos nombrar:

- **Microsoft Entra**: En el año 2022 Microsoft lanzó al mercado un servicio en la nube de identidad descentralizada pensada para la emisión de credenciales de acceso y control de permisos a empleados de distintas organizaciones, esto gracias a la integración de información que dispone de ellos en su otro servicio Active Directory [5]. Esta solución hace uso del protocolo ya existente OpenID.

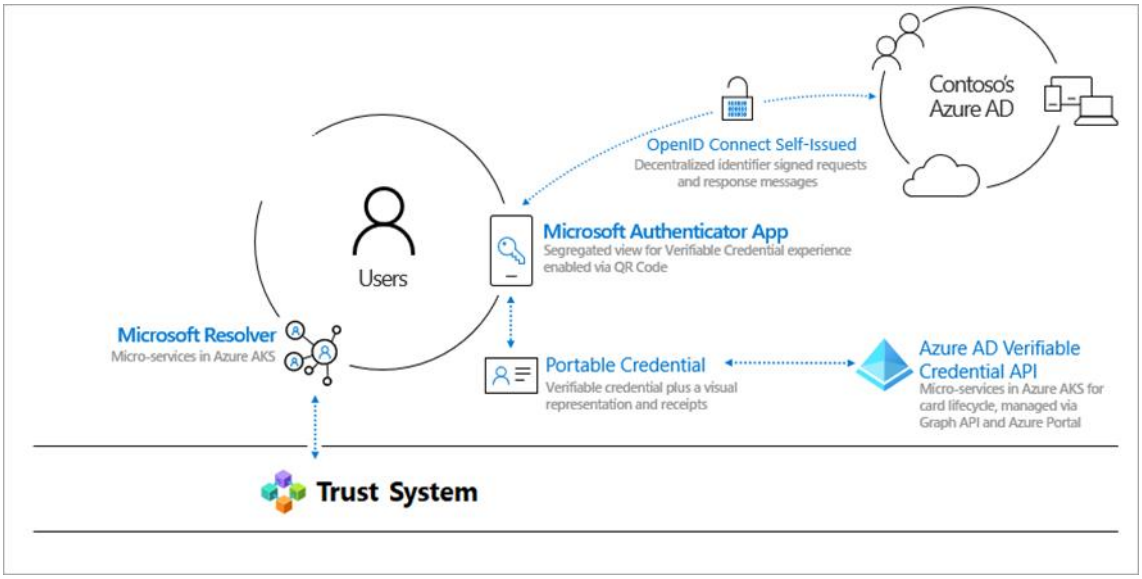

Ilustración 1 - Esquema de Microsoft Entra

Fuente: Microsoft (2023)[5]

- **Hyperledger**: Es un multi-proyecto de código libre iniciado en el año 2015 por la Fundación Linux [6] que engloba distintos subproyectos para distintas soluciones basadas en ledgers distribuidos y blockchain. Entre sus subproyectos se encuentran los siguientes relacionados con Identidad Auto-Soberana:

    - **Indy**: Tiene el objetivo brindar las herramientas, y componentes necesarios para poder desplegar una blockchain diseñada especialmente para dar apoyo a ledgers con Identidad Descentralizada.

    - **Aries**: Ofrece un kit de herramientas para desarrollar soluciones centradas en la creación, transmisión y almacenamiento de credenciales digitales verificables. A estas soluciones se las conoce como Agentes. En esta arquitectura la comunicación de lleva a cabo bajo el nuevo protocolo DIDComm desarrollado por la Fundación de Identidad Descentralizada.

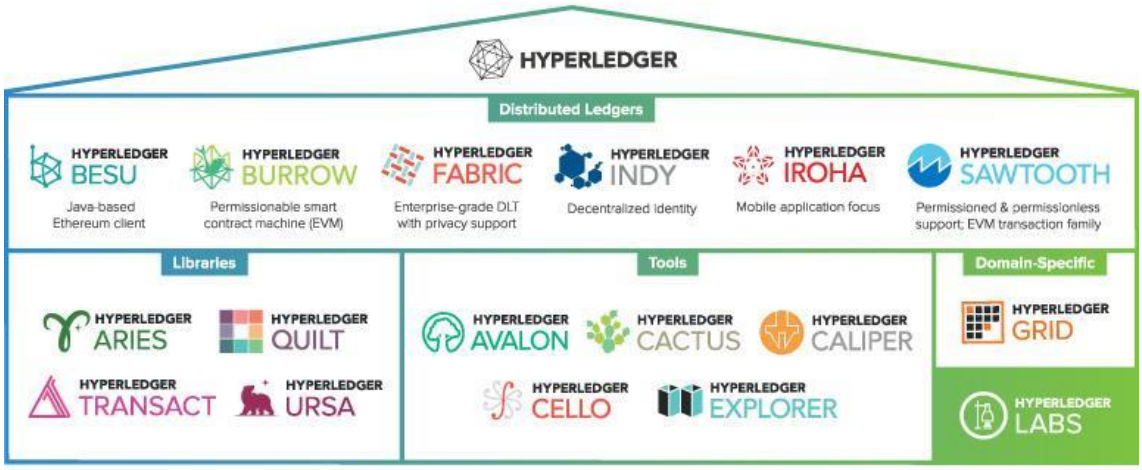

Ilustración 2 - Proyectos de Hyperledger

Fuente: Hyperledger (2022) [6]

Para la adopción de IAS no sólo son necesarios avances tecnológicos sino que también son necesarias regulaciones y guías que entidades como la Unión Internacional de Telecomunicaciones, Grupo de Acción Financiera Internacional o la Unión Europea han

ido desarrollado estos últimos años para que los gobiernos adopten y puedan legislar en base a ellas. Actualmente ninguna de estas guías, como la sistema europeo de reconocimiento de identidades electrónicas (eIDAS) [7] o el Reglamento General de Protección de Datos de la Unión Europea (RGPD) [8], hablan explícitamente de Identidad Auto-Soberana pero son compatibles perfectamente con su uso.

EU Blockchain [9], es otro proyecto de la Unión Europea con que promueve la investigación, desarrollo y adopción de soluciones basadas en blockchain, entre ellas las de Identidad Auto-Soberana, con el cual alega que se llevará transparencia y ahorro económico en todas las transacciones, se evitarán fraudes fiscales y mejorará la seguridad de la información.

Otros esfuerzos también se han hecho desde la Unión Europea como el proyecto European Self Sovereign Identity Framework Laboratory (eSSIF-Lab) [10] finalizado el 31 diciembre del año 2022, cuyo objetivo final fue adelantar la asimilación a gran escala de IAS como solución de próxima generación para una identidad digital de confianza y abierta, creando un marco que facilite la interacción transfronteriza entre los países miembros.

En el año 2017 las principales corporaciones españolas crearon el consorcio Alastria, que actualmente cuenta con más de 500 miembros, con el objetivo de crear una de las plataformas blockchain con permiso público más grandes del mundo y promover el desarrollo e investigación de diferentes proyectos sobre la misma, entre los que destaca AlastriaID 1.0 [11], una solución de IAS sobre su propia red.

Aunque en la actualidad todavía ningún país haya adoptado una solución de Identidad Auto-Soberana integral para todas sus transacciones existen diferentes proyectos que impulsan su adopción, como la alianza LACChain que integra diferentes actores del entorno blockchain de todo el mundo y es liderada por el Laboratorio de Innovación del Grupo del Banco Interamericano de Desarrollo (BID Lab) con el objetivo de desarrollar soluciones basadas en blockchain en América Latina y el Caribe [12].

Otro ejemplo es LACNet, una asociación internacional sin fines de lucro, fruto de la alianza entre RedCLARA y LACNIC en colaboración con BID Lab, creado en el marco de la Alianza Global LACChain para orquestar de manera neutral y sostenible las redes

blockchain LACChain [13]. Algunos de sus proyectos que están actualmente en desarrollo son:

- **DIDI**: Su objetivo es mejorar el acceso a bienes y servicios de calidad de poblaciones de barrios vulnerables. A través de una app móvil, DIDI permite generar una identidad digital y un pasaporte digital descentralizado, verificable, portable, seguro y privado; así como la generación de un perfil crediticio certificado por distintas instituciones para facilitar el acceso al sistema financiero alternativo para sectores que no pueden acceder al sistema tradicional. Actualmente desarrollándose en Argentina.

- **Certijoven**: El Ministerio del Trabajo del gobierno de Perú lanzó una solución que, gracias al uso de la tecnología blockchain, permite que las personas menores de 29 años puedan comprobar certificados de antecedentes no penales, certificados judiciales, policiales, académicos, de grados obtenidos o de experiencia laboral formal, impactando de manera positiva en la tasa de ocupación laboral.

- **Ni1+**: Solución basada en blockchain para mitigar los efectos de la violencia de género, facilitando la producción y autogestión de pruebas administrativamente válidas de actos violentos. Aplicación móvil para el registro de pruebas y legalización en línea, habilitando procesos civiles, administrativos o penales. Actualmente desarrollándose en Colombia.

Otro proyecto con alcance global es el de la Fundación Sovrin [14], una organización sin fines de lucro que desde el año 2018 dispone de una red blockchain desplegada de utilidad pública global para el despliegue de soluciones de Identidad Auto-Soberana llamada Red Sovrin y un Marco de Gobernanza que es la base legal de la red. El uso de la red del proyecto es arancelado a bajo costo para poder mantener los nodos y su despliegue está basado en el proyecto de código abierto Hyperledger de la Fundación Linux, proyecto que se detallará más adelante en esta tesis.

3. MARCO TEÓRICO

3.1 Identidad

Para poder comprender los conceptos de Identidad Digital e Identidad Auto-soberana primero debemos definir lo que conocemos por Identidad.

En las personas, la identidad es un concepto fundamental para la comprensión de nosotros mismos y de los demás, refiere a la esencia de quiénes somos como individuos. Son el conjunto de nuestras características, creencias, personalidad, historia y experiencias que nos definen como individuos únicos. Es algo dinámico y cambiante que evoluciona a lo largo del tiempo, y es influenciada por múltiples factores como nuestras relaciones interpersonales, cultura, entorno, etc.

La identidad también adquiere múltiples dimensiones [15]:

- Nuestra identidad: Cómo nos identificamos como individuos. Son rasgos y características únicos asociados con un individuo; el propietario de la información de identificación personal. Aquí se engloban los datos biométricos, nombre, género, profesión, nacionalidad, hábitos, etc.
- Representación de la Identidad: Es toda la documentación digital o física que es proveída por un tercero, como los documentos de identidad, pruebas de registros civiles, licencia de conducir, matrícula para trabajar, historial financiero, etc.
- Cómo interactuamos con nuestra identidad: Qué información proveemos al interactuar en diferentes dominios como el gobierno, transacciones comerciales, trabajo [16].

Para adoptar una perspectiva funcional la comunidad de 'Rebooting the Web of Trust' (Joe Andrieu, 2019) definió a la identidad como *"La identidad es cómo reconocemos, recordamos y, en última instancia, respondemos a personas y cosas específicas"* [17].

Es interesante notar la idea de "*cosas específicas*", ya que las personas también utilizamos el concepto de identidad en otros seres vivos y objetos para distinguirlos individualmente como animales, empresas, organizaciones.

3.2 Identidad Digital

La identidad digital es un conjunto de información y credenciales asociadas a un individuo o entidad que nos permite crear y presentar una versión de nosotros mismos en el mundo digital a través de Internet. Esto puede incluir nuestros datos personales como nombre, dirección de correo electrónico, número de teléfono y fecha de nacimiento, así como información de autenticación, como contraseñas y tokens de acceso que represente nuestro "ser digital". Esto puede ser visto como una ampliación o incluso como una distorsión de nuestra verdadera identidad y plantea cuestiones sobre la autenticidad y la integridad de la identidad digital, y sobre cómo esta identidad se relaciona con nuestra identidad en el mundo real.

En su diseño Internet no contempló una capa integrada de identidad, lo que dio lugar al desarrollo de múltiples protocolos y estándares de identidad en la capa de aplicación y que cada proveedor de servicios adopte el que crea conveniente, dando como resultado que un individuo pueda tener múltiples identidades digitales.

En su paper, "The laws of Identity", Kim Cameron [18] describe siete leyes sobre cómo se podría crear una capa de identidad en internet y no perder la confianza entre los usuarios conectados. Se nombran a continuación:

1. Control y consentimiento del usuario: Los sistemas de identidad técnica solo deben revelar información que identifique a un usuario con el propio consentimiento del usuario.
2. Mínima información para uso restringido: La solución que revele la mínima cantidad de información identificatoria y mejor limite su uso es la más estable a largo plazo.
3. Peticiones justificables: La solución debe garantizar que el usuario sepa en todo momento con qué entidades interactúa y qué información le solicitan. También debe tener conocimiento de qué se hará con la información solicitada.
4. Direccionalidad en la identidad: La solución de identidad universal debe admitir tanto identificadores "omnidireccionales" para uso de entidades públicas, como identificadores "unidireccionales" para uso de entidades privadas. Esto facilita el descubrimiento, evita la liberación innecesaria de identificadores de correlación y garantiza que se envíe información en un solo sentido.

5. Pluralidad de tecnologías y operaciones: Un sistema de identidad universal debe canalizar y permitir el interfuncionamiento de múltiples tecnologías de identidad ejecutadas por múltiples proveedores de identidad.
6. Integración humana: El metasistema de identidad debe definir al usuario humano como un componente del sistema distribuido integrado a través de mecanismos inequívocos de comunicación hombre-máquina que ofrecen protección contra ataques de identidad.
7. Experiencia consistente en todos los contextos: El metasistema de identidad debe garantizar a los usuarios una experiencia simple y consistente, y a su vez permita la separación de contextos a través de múltiples operadores y tecnologías.

3.3 Modelos de Identidad

A lo largo de los años se han desarrollado varios modelos para intentar identificar a las personas de manera digital mediante diferentes estrategias dentro de Internet. A estos modelos los podemos clasificar en tres según la estrategia en cómo manejan la identidad de los usuarios [19].

3.3.1 Modelo Centralizado

En el modelo de identidad centralizado un usuario para poder autenticarse dentro de un sistema debe poseer una identidad provista por el mismo sistema. Este clásico modelo, muy utilizado en los servicios web, la estrategia es que el usuario "se registre" generando un usuario y contraseña que sólo él va a saber pero que va a almacenar el propio proveedor del servicio. En este modelo la identidad es la cuenta que el propio usuario crea dentro del sistema la que se utiliza para poder identificarse. Esto plantea una serie de inconvenientes [20]:

- Los datos se almacenan de forma centralizada, cuya seguridad y confidencialidad va a depender de la organización que brinda el servicio.
- Al encontrase los datos de los usuarios centralizados, se vuelve un punto tentador para ser atacado.
- Los usuarios deben crearse cuentas para cada servicio que quieran utilizar de forma identificada.
- Es responsabilidad del usuario recordar sus credenciales.
- Normalmente para un mismo servicio, si una persona lo desea, puede crear múltiples cuentas.
- La identidad no es portable para utilizarse en otro servicio.

Ilustración 3 - Modelo Centralizado

Fuente: Timothy Ruff (2018) [20]

3.3.2 Modelo Federado

La propuesta del modelo federado es la de colocar un Proveedor de Identidad (IDP) como intermediario de identidad entre los usuarios y los sistemas que confíen en ese proveedor de identidad. Con esto se logra que el usuario sólo necesite una cuenta, y en algunos casos otorgando una experiencia de Autenticación Única (SSO – Single Sign On) entre estos servicios. En este modelo el IDP es el que emite y almacena de manera centralizada las credenciales digitales de los usuarios, pero se reduce la cantidad de credenciales separadas que un usuario necesita.

Ilustración 4 - Modelo Federado [20]

Fuente: Timothy Ruff (2018) [20]

En el modelo federado pueden existir múltiples IDPs que confíen entre sí, dando a los usuarios la capacidad de identificarse con las mismas credenciales y compartir datos de identidad entre sitios, servicios o aplicaciones que confíen en ese IDP.

Existen distintos protocolos y estándares abiertos que nos permiten implementar el modelo de autenticación federado, entre los más famosos se encuentras Identificadores Abiertos (OpenID) [21], Autorización Abierta (OAtuh) [22] o Lenguaje de Marcado para Confirmaciones de Seguridad conocido como (SAML) [23].

A pesar de la ventaja de permitir identificarnos con una sola cuenta en varios sistemas, este modelo tiene algunos inconvenientes:

- Permite a los usuarios tener más de una credencial, pudiendo tener varios perfiles para una misma persona.
- Cada IDP es un almacenamiento centralizado de credenciales, lo que también puede ser un punto crítico de falla o ataque.

- El usuario necesita manejar menos cantidad de cuentas, pero no una única, ya que necesita una cuenta por federación.
- Al igual que en el modelo centralizado, las credenciales provistas por este modelo también carecen de portabilidad.
- Los IDPs determinan el esquema de datos para identificar a los usuarios.
- Para funcionar es necesario disponer de conexiones directas con todos los participantes de la red, inhibiendo la flexibilidad y la escalabilidad.

3.3.3 Modelo Distribuido

El modelo distribuido está inspirado en las tecnologías DLT, blockchain y su modelo descentralizado de almacenamiento de datos que promovió el desarrollo de estándares como los Identificadores Distribuidos, las Credenciales Verificables, Billeteras Digitales y nuevos estándares en criptografía entre otros desarrollos que se abordaran más adelante en la tesis.

En este modelo ambas entidades comparten una conexión punto a punto y ninguno de los dos es dueño absoluto de la conexión. Mientras ambos lo deseen, la conexión persistirá.

La diferencia fundamental de éste modelo con los otros es que no se basa en cuentas sino, de manera similar al mundo real, en relaciones directas uno a uno entre pares en la que ninguno de los dos “provee”, “controla” o “posee” la relación con el otro [20], y la confianza en el otro se deposita en las credenciales que se puedan proveer y validar el uno al otro. En parte esto se basa en criptografía de claves públicas/privadas que está en poder de cada parte y la gestión de identidades la utiliza para la infraestructura de clave pública descentralizada (DPKI).

Lo que plantea este modelo es que los pares intercambien claves públicas directamente para formar conexiones privadas y seguras, almacenar estas claves públicas en cadenas de bloques públicas como blockchain y verificar las firmas en las credenciales compartidas contra ellas.

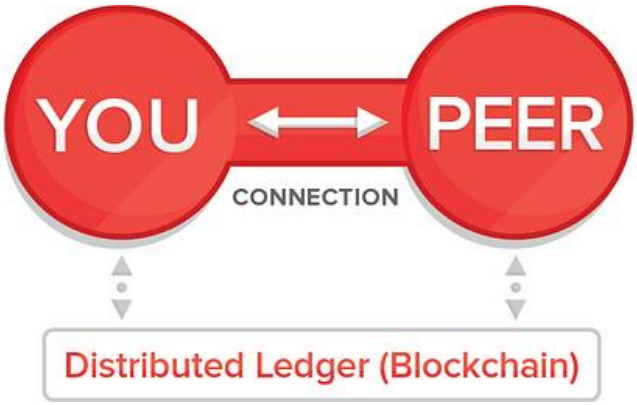

Ilustración 5 - Modelo Distribuido [20]

Fuente: Timothy Ruff (2018) [20]

Sobre este modelo distribuido de identificación nace el concepto de Identidad Auto-Soberana, que como veremos a continuación es más que un modelo de identificación.

3.4 Identidad Auto-Soberana

Identidad Auto-Soberana es un concepto que propone cómo debemos pensar y construir la próxima generación de Internet, centrada en la identidad de los usuarios y la privacidad de sus datos.

Es un nuevo paradigma de identidad descentralizada que otorga a los usuarios la capacidad de administrar sus identidades, poder pedir y recibir credenciales de gobiernos, instituciones educativas u organizaciones empresariales y almacenarlas y compartirlas de manera segura. Se basa en un conjunto de estándares y protocolos abiertos de comunicación que utilizan la tecnología blockchain para almacenar registros de validación de manera inmutable, permitiendo la posibilidad de compartir información de identificación de manera segura. También permite utilizar las credenciales para superar pruebas de validación manteniendo el anonimato de las mismas, por ejemplo que queramos demostrar si somos mayores de edad sin necesidad de revelar la edad actual o fecha de nacimiento.

Christopher Allen la define como:

> *...el siguiente paso más allá de la identidad centrada en el usuario y eso significa que comienza en el mismo lugar: el usuario debe ser el centro de la administración de la identidad. Eso requiere no solo la interoperabilidad de la identidad de un usuario en múltiples ubicaciones, con el consentimiento del usuario, sino también el verdadero control del usuario de esa identidad digital, creando autonomía para el usuario. Para lograr esto, una identidad auto-soberana debe ser transportable; no se puede bloquear en un sitio o lugar* [1].

En su capa técnica el modelo IAS requiere el desarrollo de nuevos estándares y protocolos de comunicación que amplíen el modelo OSI y permitan a las personas el control de su identidad digital, produciendo una Capa 8 independiente al resto [24].

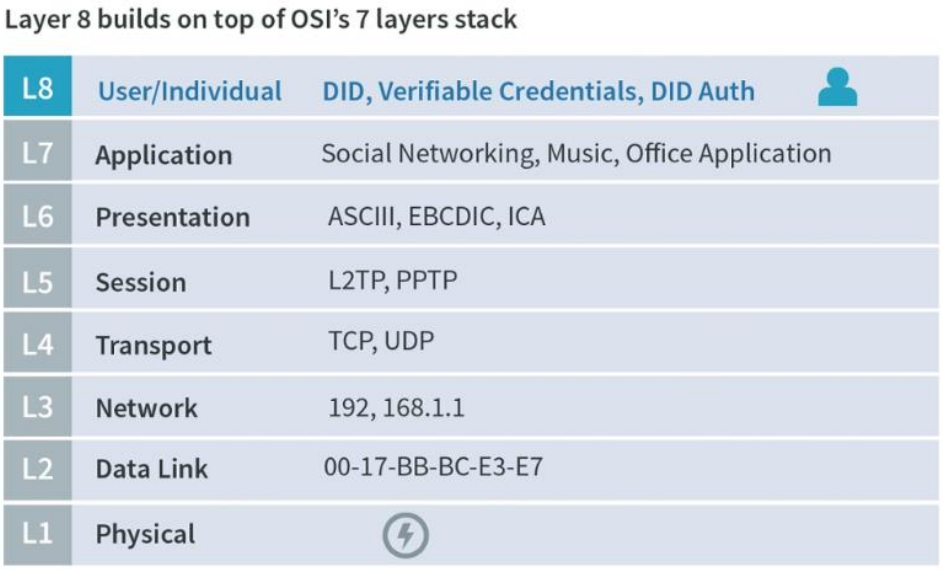

Ilustración 6 - Tecnologías de Capa 8

Fuente: Heather Vescent y Kaliya Young (2018) [24]

Algunos de los avances tecnológicos y estándares que posibilitan el desarrollo de IAS, y que posteriormente se analizarán en profundidad en esta tesis son:

- **Estructuras de datos inmutables:** Como las tecnologías DLT y Blockchain en donde la información almacenada debe poder ser accesible por cualquiera.
- **Identificadores Descentralizados (DID):** Un identificador único que está asociado con una persona o entidad, y no está controlado por ninguna autoridad u organización centralizada.
- **Credenciales Verificables:** Son representaciones digitales de información o afirmaciones que han sido emitidas al usuario por una fuente confiable, como una agencia gubernamental, una institución educativa o una organización. La misma entidad emisora resguarda una validación criptográfica en la DLT.
- **Teléfonos inteligentes, billeteras virtuales y cómputo en la nube personalizado:** IAS utiliza una combinación de teléfonos inteligentes, nubes personales para almacenar las Credenciales Verificables en agentes individuales y billeteras virtuales para manejarlos.

Además de los avances tecnológicos, para que una implementación de Identidad Auto-Soberana tenga éxito debe estar regulada mediante leyes que la validen y respalden legalmente, y en esta materia es en dónde se encuentran mayores diferencias entre países y las legislaciones que tienen sobre leyes de protección de datos y firmas digitales. Estas leyes ayudan a definir las reglas y procesos sobre cómo se gobierna, administra y opera en estos sistemas y poder armar modelos de gobernanza en base a ellas.

Un modelo de gobierno generalmente incluye un conjunto de políticas, procedimientos y estándares que están diseñados para garantizar que los sistemas IAS sean seguros, confiables e interoperables. Hay varios modelos de gobierno diferentes que se pueden usar en los sistemas IAS, según las necesidades y los requisitos específicos del sistema y sus usuarios. Algunos ejemplos son:

- **Gobernanza basada en consorcios:** en este modelo, un consorcio de organizaciones o partes interesadas es responsable de gobernar el sistema SSI. Los miembros del consorcio colaboran para definir las políticas, estándares y procedimientos del sistema, y también pueden ser responsables del desarrollo y mantenimiento de la infraestructura tecnológica.
- **Gobierno descentralizado:** en este modelo, el gobierno se distribuye entre los usuarios del sistema SSI, quienes colectivamente toman decisiones sobre cómo debe operar el sistema. Esto se puede lograr a través de varios mecanismos, como la votación, la creación de consenso o la toma de decisiones comunitaria.
- **Gobernanza híbrida:** este modelo combina elementos de la gobernanza descentralizada y basada en consorcios, donde un grupo central de partes interesadas es responsable de definir políticas y estándares, pero la comunidad más amplia de usuarios tiene voz en la toma de decisiones y la gobernanza.
- **Gobierno abierto:** En este modelo, el gobierno es abierto y transparente, con todas las decisiones y procesos documentados y disponibles públicamente. Esto ayuda a garantizar la rendición de cuentas y la confianza en el sistema.

Los modelos de gobierno pueden tener un impacto significativo en la usabilidad, la seguridad y la interoperabilidad de los sistemas IAS, y deben diseñarse cuidadosamente para satisfacer las necesidades de todas las partes interesadas, incluidos los usuarios, los desarrolladores y otros participantes.

3.4.1 Libro Mayor Distribuido y Blockchain

Tecnología de Libro Mayor Distribuido

Las Tecnología de Libro Mayor Distribuido o DLT (Distributed Ledger Technologies) son esencialmente bases de datos que permiten el almacenamiento y consenso de datos replicados, compartidos y sincronizados que se encuentran distribuidos geográficamente en nodos interconectados. A diferencia de una base de datos centralizada, las tecnologías DLT no requieren un administrador central y, por consecuencia, no tiene un único punto de falla. Cada nodo dentro de DLT funciona como un servidor independiente con la capacidad de sumar datos a la red, sincronizando la información con el resto de los nodos [25].

Si bien las cadenas de bloques o blockchains, como Bitcoin, son el tipo de DLT más famoso en la actualidad, en la práctica las DLT las podemos clasificar según cómo se pueden incorporar nodos a la red y cómo los usuarios puede hacer uso de ellas [26]:

- **Públicas sin permiso**: Son blockchains en las que cualquiera puede participar realizando transacciones, leyendo información de las transacciones almacenadas en ella. No existen barreras de entrada, por lo que también se pueden sumar nodos libremente.
- **Privada con permiso**: Para poder interactuar, ya sea escribiendo o leyendo sobre la cadena, primero se deben otorgar permisos al usuario. Estos permisos se administran por separado, y por ejemplo, la visualización podría estar abierta para algunos usuarios, pero no la escritura.
- **Híbridas**: Como su nombre sugiere es una combinaciones de los formatos anteriores. La red podría ser permisionada para la escritura de datos pero libre para la lectura.
- **Basadas en Gráficos Acíclicos Dirigidos**: Transmiten y confirmar transacciones de forma asíncrona en lugar de "encadenada". Un ejemplo es la plataforma IOTA, la DLT más grande de Europa, conformada para dispositivos IoT, los cuales para transmitir una nueva transacción a la red deben realizar los cálculos computacionales necesarios para confirmar otras dos transacciones como condición previa para que se confirme su propia transacción.

Blockchain

La tecnología Blockchain es un tipo de DLT en el cual los nodos forman una red peer-to-peer, capaces de generar nuevos registros de información, conocidos como bloques, encadenados de forma cronológica, y aceptados a través de algoritmos de consenso, de modo de que todos los nodos pertenecientes a la red dispongan de la misma información. Los usuarios pueden interactuar directamente con los datos almacenados en la cadena sin la necesidad de un intermediario o distribuidor [26].

Las blockchain eliminan la necesidad de una autoridad central y, al mismo tiempo, mantener una confianza en la integridad de los datos. Esto lo logran mediante las siguientes características:

- Cada transacción (la escritura de un nuevo registro) en una cadena de bloques está firmada digitalmente. Así es como el control de la base de datos distribuida se reparte entre todos los pares: cada integrante gestiona sus claves privadas y firma digitalmente sus transacciones con la cadena de bloques.

- Un bloque se refiere a un conjunto de transacciones que se cifran criptográficamente y se vinculan al bloque anterior. Cada bloque tiene una marca de tiempo, y cada bloque nuevo hace referencia al bloque anterior. Combinada con hashes criptográficos, esta cadena de bloques con sello de tiempo proporciona un registro inmutable de todas las transacciones en la red, desde el primer bloque, conocido como génesis.

- Cada bloque nuevo se replica en todos los nodos de la red de la cadena de bloques gracias a un algoritmo de consenso e independientemente del protocolo o algoritmo utilizado en la blockchain para el consenso, una vez alcanzado cada nodo en la red termina con una copia del último bloque y todos están de acuerdo con esa copia.

- Los bloques incorporan el hash de Merkle, que es una estructura de datos compuesta por hashes que resumen todas las transacciones en un bloque. También permite una verificación de contenido rápida y segura en grandes conjuntos de datos y verifica la consistencia y el contenido de los datos.

Un bloque suele contener como mínimo los siguientes atributos:

- Un hash de bloque para poder validar la información.
- Alguna referencia al bloque anterior, comúnmente el hash anterior.
- Datos de transacciones realizadas.
- Hash de Merkle.
- Etiqueta de tiempo (timestamp).
- Nonce o id (número que solo puede usarse una vez).

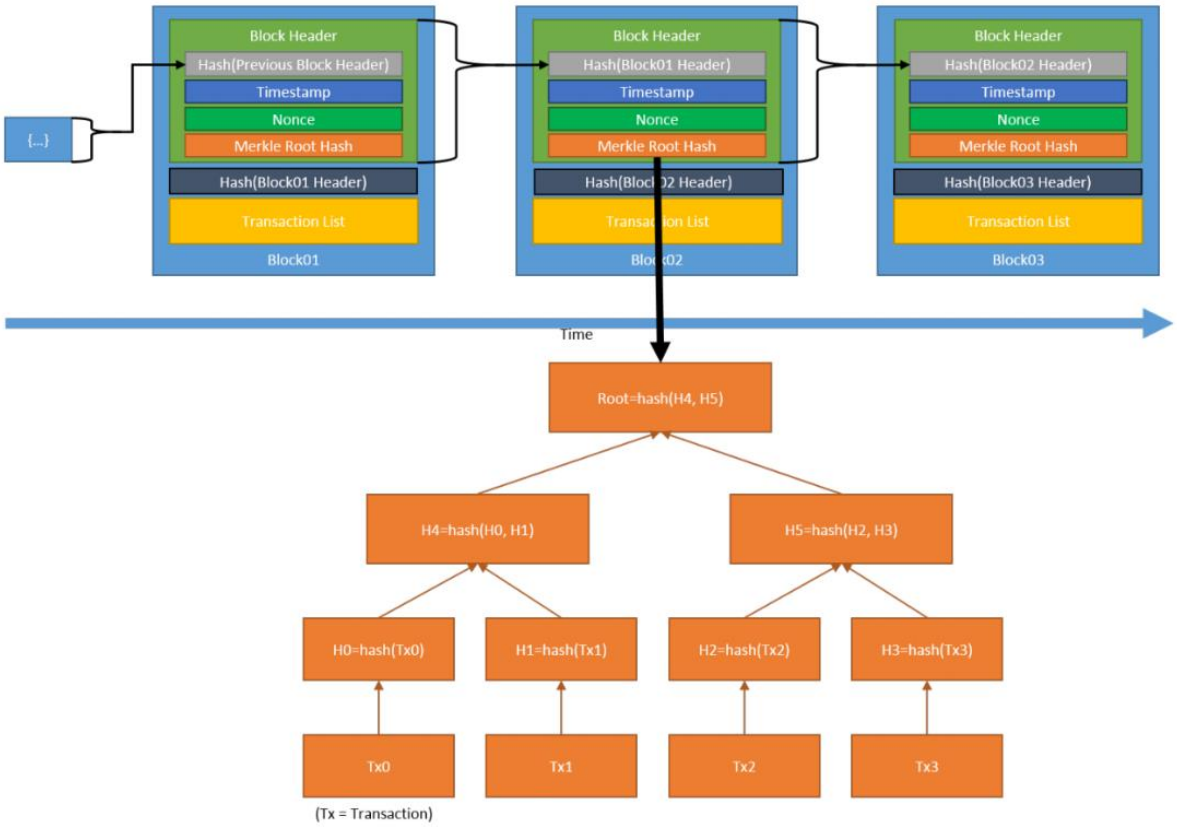

Ilustración 7 - Lista de bloques encadenada

Fuente: NIST (2021) [27]

3.4.2 Identificadores Descentralizados

El 19 de Julio del año 2022 el Consorcio World Wide Web (W3C) anunció la oficialización del nuevo estándar web Decentralized Identifiers (DIDs) v1.0 [28]. Los Identificadores Descentralizados o DIDs son un tipo de identificador global que puede ser utilizado para identificar personas, organizaciones, dispositivos, productos, lugares, o conceptos abstractos. Son una cadena de texto dividida en 3 partes:

- Un Esquema DID: Es un esquema URI conforme al RFC3986 que comienza siempre con el prefijo **did:**
- Un Método DID: Define cómo se implementa un esquema de método DID específico
- Un Identificador específico de Método: Identifica un método en particular

Ilustración 8 - Ejemplo de un DID y sus estructura resaltada

Fuente: M. Sporny, A. Guy... (Julio 2022) [29]

Para poder ser públicamente descubiertos, un DID se puede codificar en un código QR que sea accesibles desde la web o incluso imprimirlos.

Este DID podría resolver un Documento DID que contenga información asociada al DID, como formas de autenticar criptográficamente un Controlador DID.

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

Ilustración 9 - Ejemplo de un Documento DID

Fuente: M. Sporny, A. Guy... (Julio 2022) [29]

Los DIDs son un componente de un sistema mayor que es el ecosistema de las Credenciales Verificables [29], el cual influenció en los objetivos de su diseño, los cuales pueden resumirse en:

- **Descentralización**: Eliminar el requisito de autoridades centralizadas o puntos de fallas único en la gestión de identificadores.
- **Control**: Otorgar a las entidades, humanas o no humanas, el poder de controlar directamente sus identificadores digitales sin la necesidad de depender de autoridades externas.
- **Privacidad**: Permitir que las entidades controlen la privacidad de su información, incluida la divulgación mínima, selectiva y progresiva de atributos u otros datos.
- **Seguridad**: Disponer de seguridad suficiente para que las partes solicitantes dependan de los documentos DID para su nivel de seguridad requerido.
- **Basado en pruebas**: Permitir que los controladores DID proporcionen pruebas criptográficas al interactuar con otras entidades.

- **Visibilidad**: Permitir que las entidades descubran los DID de otras entidades, para obtener más información o poder interactuar con ellas.
- **Interoperabilidad**: Utilizar estándares interoperables para que la infraestructura DID pueda hacer uso de software existente y diseñado para la interoperabilidad.
- **Portabilidad**: Que sea independiente del sistema y de la red y permita que las entidades utilicen sus identificadores con cualquier sistema que admita DID y métodos DID.
- **Simplicidad**: Favorecer un conjunto reducido de funciones simples para que la tecnología sea más fácil de entender, implementar y desplegar.
- **Extensibilidad**: Siempre que sea posible, habilitar la extensibilidad sin obstaculizar la interoperabilidad, la portabilidad o la simplicidad.

A continuación un diagrama de su arquitectura y una descripción de sus componentes:

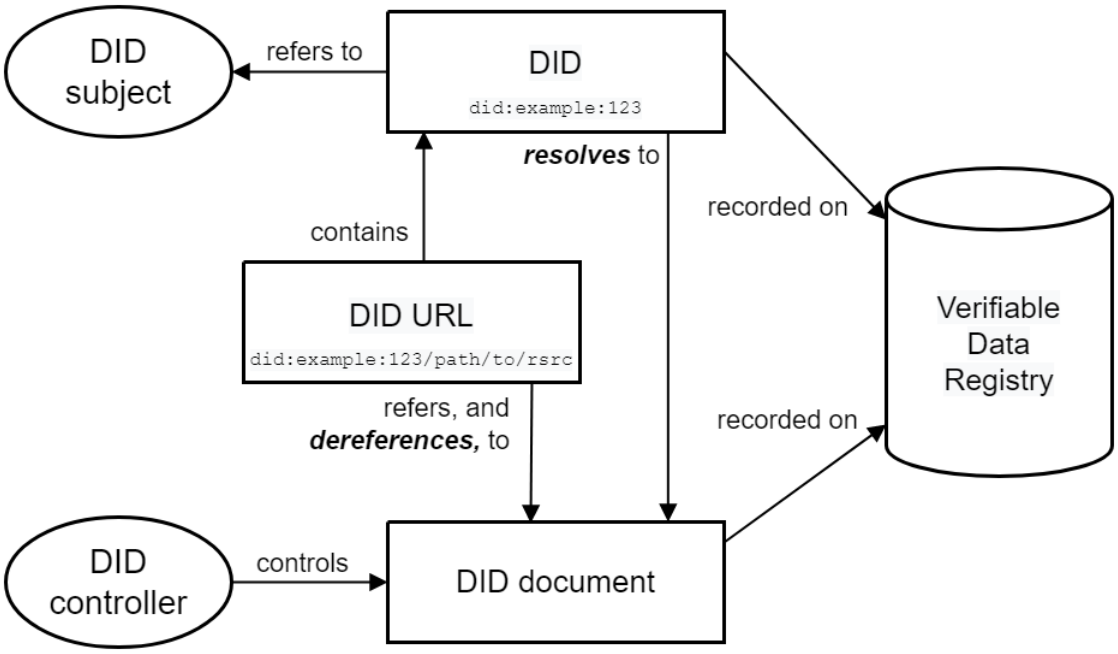

Ilustración 10 - Arquitectura DID

Fuente: M. Sporny, A. Guy... (Julio 2022) [29]

Sujeto DID

Es la entidad identificada por el DID. Cualquier cosa puede ser objeto de un DID, por ejemplo una persona, un grupo, una organización, o incluso un concepto. A su vez, el Sujeto DID también podría ser el Controlador DID.

El Sujeto DID debe estar expresado utilizando la propiedad **id** dentro del Documento DID.

```
{
  "id": "did:example:123456789abcdefghijk"
}
```

Ilustración 11 - Ejemplo de un id definido en un Documento DID

Fuente: M. Sporny, A. Guy... (Julio 2022) [29]

DIDs

Fueron diseñados para que se puedan utilizar sin necesidad de utilizar registros centralizados, proveedores de identidad o certificados autoritativos. Los DID son Identificadores uniformes de recursos (URIs) que asocian un Sujeto DID con un Documento DID permitiendo interacciones confiables. Se almacenan en un Registro de Datos Verificables, como una blockchain.

DID URL

Una URL DID es un identificador de ubicación de red para un recurso específico. Se pueden utilizar para recuperar información como representaciones de Sujetos DID, métodos de verificación aceptados, servicios ofrecidos, o partes específicas de un Documento DID.

Su sintaxis sigue la definición del formato Backus-Naur aumentado (Augmented BNF for Syntax Specifications) [30], el cual permite, por ejemplo:

- Realizar querys: *did:example:123456**?versionId=1***
- Enviar un path para especificar la consulta: *did:example:123456**/path***
- Obtener información fragmentada: *did:example:123456**#agent***

Documento DID

Cada Documento DID puede contener material criptográfico, métodos de verificación, servicios y sus propiedades, que proporcionen un conjunto de mecanismos que permitan a un Controlador DID demostrar el control del DID. Los Documentos DID pueden ser actualizados por un Controlador de DID utilizando un Método DID. Un Documento DID puede tener más de un controlador, y a su vez un Sujeto DID podría ser un Controlador del DID. Se almacenan en un Registro de Datos Verificables.

```
{
  "id": "did:example:123",
  "verificationMethod": [
    {
      "id": "did:example:123#key-1",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:example:123",
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    },
    {
      "id": "did:example:123#key-2",
      "type": "JsonWebKey2020",
      "controller": "did:example:123",
      "publicKeyJwk": {
        "kty": "OKP",
        "crv": "Ed25519",
        "x": "r7V8qmdFbwqSlj26eupPew1Lb22vVG5vnjhn3vwEA1Y"
      },
    }
  ]
  "service": [{
    "id": "did:example:123#edv",
    "type": "EncryptedDataVault",
    "serviceEndpoint": "https://edv.example.com/"
  }]
}
```

Ilustración 12 - Ejemplo de un Documento DID

Fuente: M. Sporny, A. Guy... (Julio 2022) [29]

Controlador DID

Es una entidad que está autorizada para realizar cambios en un Documento DID. El proceso de autorización de un Controlador DID está definido por el Método DID.

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "controller": "did:example:bcehfew7h32f32h7af3",
}
```

Ilustración 13 - Ejemplo de un controlador definido en un Documento DID

Fuente: M. Sporny, A. Guy... (Julio 2022) [29]

Registro de Datos Verificables

Independientemente de la tecnología utilizada, al sistema que admite el registro de DIDs y la consulta y devolución de los datos necesarios para producir Documentos DIDs se lo denomina Registro de Datos Verificables. En el modelo de IAS lo que se propone es que esta tecnología sea algún tipo de DLT como blockchain dada los beneficios anteriormente mencionados.

Métodos DID

Un método DID define cómo los implementadores pueden realizar las características descritas por esta especificación. Generalmente los métodos DID se asocian con un Registro de Datos Verificable en particular. Los nuevos métodos DID se definen en sus propias especificaciones para permitir la interoperabilidad entre diferentes implementaciones del mismo método DID. A la fecha de escribir esta tesis existen 166 especificaciones de Métodos DIDs publicados, definidos para trabajar con distintos tipos de DLTs [31].

DID Method	Registry	Contact
3	Ceramic Network	Joel Thorstensson (email)
abt	ABT Network	ArcBlock
aergo	Aergo	Blocko (website)
ala	Alastria	Alastria National Blockchain Ecosystem
amo	AMO blockchain mainnet	AMO Labs (website)
art	Artwork ID Method	Ming-lam Ng (RealMatter) (email) (website)
asset	Ledger-independent generative DID method based on CAIP-19 identifiers	BOTLabs GmbH (email) (website)
bba	Ardor	Attila Aldemir (email)
bee	Ledger agnostic	mesur.io (email) (website)
bid	bif	teleinfo caict

Ilustración 14 - Algunos de los 166 métodos DIDs

Fuente: M. Sporny, A. Guy... (Julio 2022) [29]

Cada método DID al ser específico para una red en particular debe especificar como se llevan a cabo las tareas de lectura, creación, actualización y revocación de Documentos DID, incluyendo las especificaciones de seguridad y privacidad. A continuación un ejemplo de un método de la especificación Sovrin [32], especificación que se utilizará en la prueba de concepto de esta tesis, en el que se consulta por los atributos relacionados a un DID:

```
{
    "submitterId": <Optional; DID of the author of this query>,
    "reqId": <Optional; a nonce for this query>,
    "identifier": <Required; The DID being read/resolved>,
    "operation": {
      "raw": "{\"endpoint\":{\"endpoint\":\"https://example.com\"}}" <Required; the value must be en
    }
}
```

Ilustración 15 - Ejemplo de consulta de atributos en la especificación Sovrin

Fuente: Sovrin (Abril 2024) [32]

Resolución DID

Resolución DID es el proceso para obtener el Documento DID asociado a un DID, y esto permite que las aplicaciones puedan obtener datos del Sujeto DID a partir del Documento DID y poder interactuar con él. Existen distintos escenarios en los que se puede aplicar:

- Validar firmas digitales que se encuentran en las Credenciales Verificables en base a la clave pública definida en el Documento DID.
- Autenticar a un Controlador DID en sitios web o aplicaciones.
- Para descubrir y acceder a un servicio asociado al Controlador DID, como un sitio web, una red social, servicios o autoridades verificadoras.
- Para solicitar una conexión DID a DID con el Controlador DID.

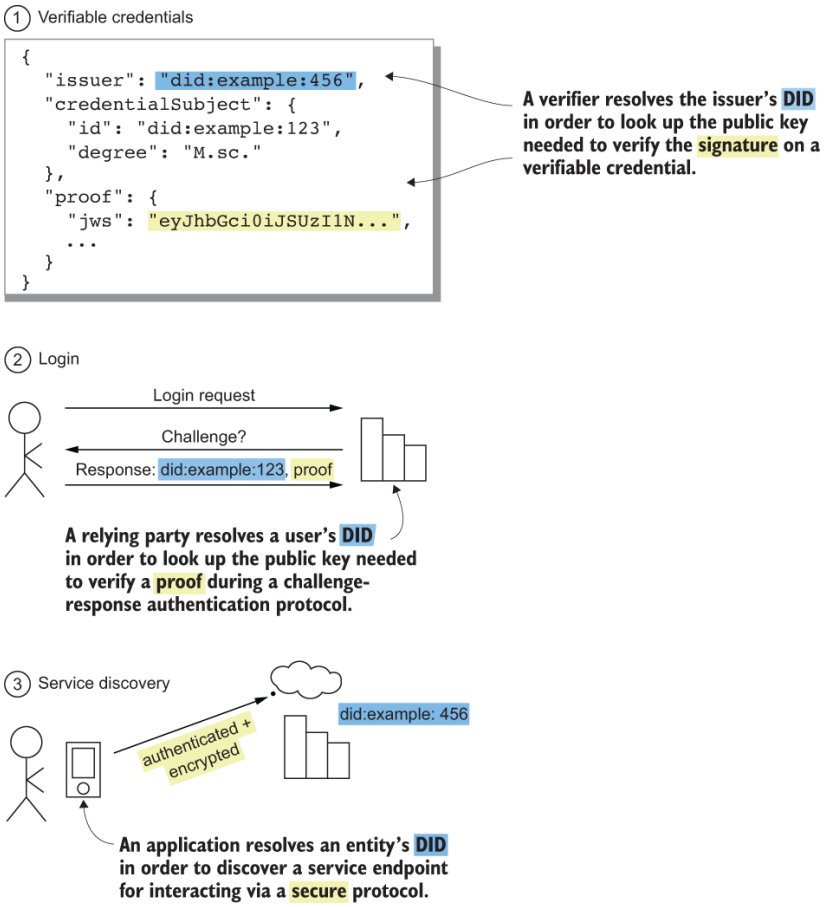

Ilustración 16 - Distintos escenarios donde aplicar Resolución de DIDs

Fuente: Alex Preukschat y Drummond Reed (2021) [4]

Autenticación DID

Como se vio anteriormente en la definición de Documento DID, en este es donde se definen las claves públicas, los métodos de verificación aceptados, y endpoint de autenticación, y es esta información la utilizada para enviar desafíos y pruebas de autenticidad. El proceso por el cual se establecen conexiones confiables entre los agentes en base a la información de los Documentos DID no forma parte del estándar de la W3C, pero a este se lo denomina Autenticación DID o DIDAuth.

Por ejemplo, en base a el modelo que propone la W3C, una clave pública criptográfica se puede utilizar como método de verificación con respecto a una firma digital, enviando una prueba en formato JWT (JSON Web Token) o JSON-LD (JSON Linked Data), cuya respuesta verifica que el firmante poseía la clave privada criptográfica asociada [33].

3.4.3 Credenciales y Presentaciones Verificables

En nuestra vida cotidiana utilizamos todo tipo de credenciales, ya sea para poder identificarnos con un documento de identidad o pasaporte, o para demostrar una aptitud como el carnet de conducir o un título profesional. Estas credenciales son necesarias tanto en el mundo físico como en el digital, pero en el digital todavía sigue siendo un desafío poder generar un equivalente a las credenciales físicas en cuanto a su control y seguridad para los usuarios. La W3C se encuentra trabajando en la recomendación del Modelo de Datos para Credenciales Verificables v1.1 [34] en el afán de crear un equivalente para el mundo digital. El modelo se basa en tres conceptos: las Aserciones (Claims), las Credenciales Verificables (Verifiable Credentials) y las Presentaciones Verificables (Verifiable Presentations).

Claims

Los Claims son afirmaciones sobre una entidad, que se expresan mediante relaciones clave-valor. Este modelo sirve para expresar los atributos que puede tener una entidad, como por ejemplo, que una persona es alumno de una universidad. A su vez, los Claims pueden combinarse formando un grafo de información sobre la entidad.

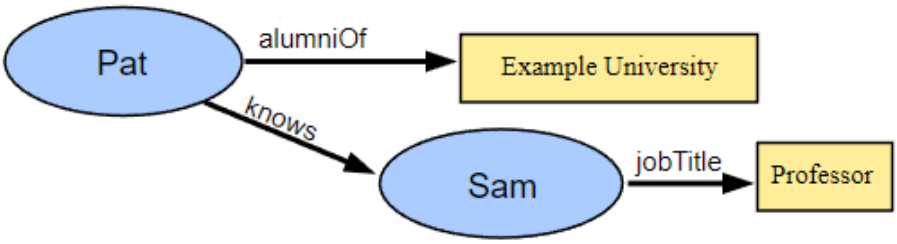

Ilustración 17 - Grafo de Claims de una entidad

Fuente: M. Sporny, D. Longley, D. Chadwick. (2022) [34]

Credenciales Verificables

Una Credencial Verificable es un conjunto de Claims realizados por una misma entidad. Estos se pueden agrupar en tres secciones:

- Metadatos: Sirven para describir las propiedades de la credencial, como el emisor, la fecha y hora de vencimiento, el mecanismo de revocación.
- Claims: Los atributos que se quieren expresar sobre el portador de la credencial.
- Prueba: Contiene una firma digital, como la RsaSignature2018, una marca de tiempo de la fecha y hora de creación, el nonce y la clave pública del emisor. Esta información es importante para terceros con el fin de verificar los datos presentados.

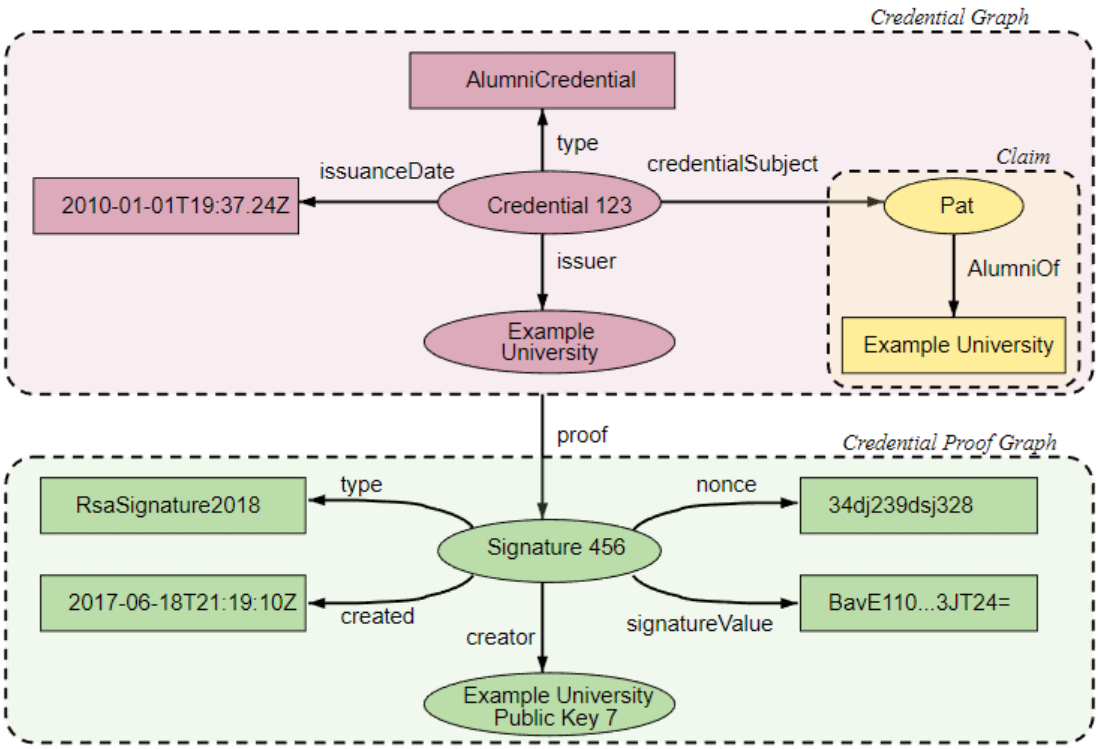

Ilustración 18 - Gafo de los componentes de una Credencial Verificable

Fuente: M. Sporny, D. Longley, D. Chadwick. (2022) [34]

La figura anterior muestra cómo se relacionan y están organizados los Claims dentro de una Credencial Verificable.

Presentaciones Verificables

Una de las claves del diseño del modelo de Credenciales Verificables es el de la privacidad. Imaginémonos en una situación en la que debemos demostrar que somos mayores de edad, información que puede estar en una credencial emitida por un gobierno como un documento de identidad, o que pertenecemos a una determinada organización, información que puede estar en una credencial emitida por la organización como un carnet. Es importante entender que para lo que se quiere demostrar no hace falta revelar todos los datos que pueden contener las credenciales como haríamos en el mundo real al entregar una credencial. Las Presentaciones Verificables están diseñadas para solucionar esto, son una encapsulación de datos contenidos en una o más Credenciales Verificables que pertenecen a una misma entidad pero que pueden haber sido emitidas por diferentes emisores.

Una Presentación Verificable está compuesta por cuatro campos de datos:

- Metadata de la Presentación: Contiene referencia sobre la o las Credenciales a presentar.
- Credenciales Verificables: Metadata de las Credenciales y Claims a presentar. No necesariamente se presentan todos los Claims de las Credenciales.
- Prueba de las Credenciales: Firmas Digitales de las Credenciales presentadas.
- Prueba de la Presentación: Firma Digital de la Presentación.

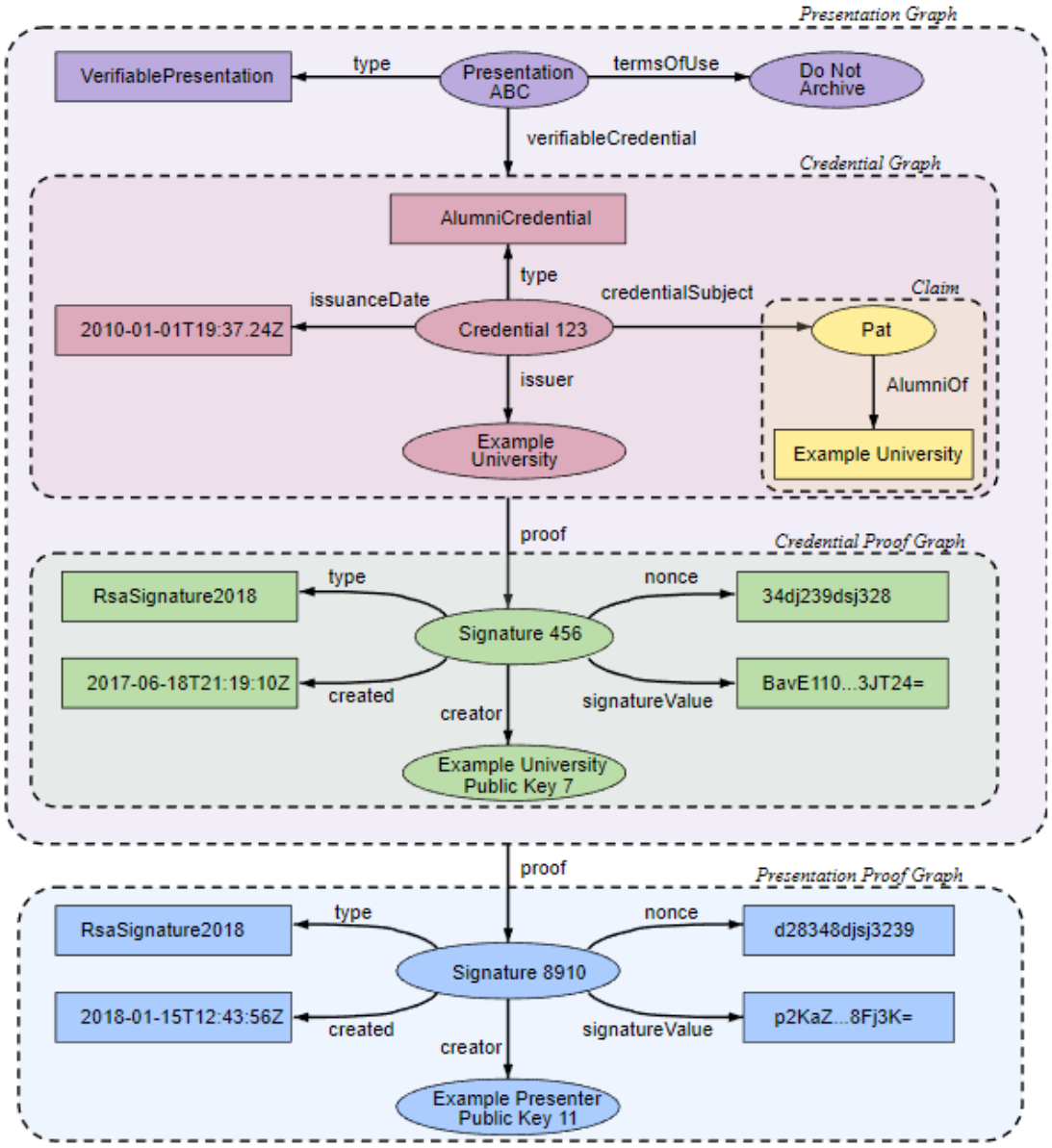

Ilustración 19 - Grafo de una Presentación Verificable

Fuente: M. Sporny, D. Longley, D. Chadwick. (2022) [34]

Las Presentaciones Verificables pueden contener información sintetizada de una credencial, sin contener el Claim en sí, por ejemplo si queremos demostrar solamente que somos mayores de edad sin revelar la edad o fecha de nacimiento. Esto se logra gracias a las pruebas de conocimiento cero (zero-knowledge proofs).

Las pruebas de conocimiento cero pueden ser de 6 tipos [35]:

- Declaración de Igualdad: Si un valor es igual o no a un valor dado.
- Declaración de Desigualdad: Si un valor es mayor o menor a un valor dado.

- Declaración de Membresía: Si el valor está contenido en una lista.
- Declaración de Rango: Si un valor está dentro de un intervalo dado [a, b] o no lo está.
- Hash de pre-imagen: Probar que se conoce un valor secreto X que genera un hash H conocido.
- Declaración de prueba de Merkle: Probar que se conoce un miembro de un árbol de Merkle en base a una raíz R conocida.

Los formatos propuestos por la W3C para las Pruebas Verificables son JWT o JSON-LD, aunque existen otros como OpenID4VC, que incluye OpenID4VCI (OpenID para emisión de credenciales verificables) y OpenID4VP (OpenID para presentaciones verificables) o el formato mDL, acrónimo en inglés de licencia de conducir móvil, estandarizado por la ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional).

Ecosistema

Dentro del ecosistema de las Credenciales Verificables podemos identificar los siguientes roles y entidades:

- Emisor: Es la entidad que puede emitir y revocar las credenciales a los usuarios.
- Sujeto: Es la entidad de cuyas propiedades se almacenan en la credencial, pudiendo ser una persona, una organización, un objeto, etc. y presenta la información que contiene a otros.
- Titular: Es la entidad que posee la credencial, en el caso de las personas normalmente también es el Sujeto.
- Verificador: Es la entidad que verifica las credenciales o presentaciones verificables presentadas por el Sujeto con el fin de acceder a algún recurso o beneficio contra los registros de datos. En algunos casos, en el que las credenciales tengan estado (por ejemplo una licencia de conducir) también debe verificar contra el emisor que las credenciales no se encuentren revocadas.
- Billetera: Es la entidad que en donde el Sujeto almacena las credenciales.

- Agente: Es el software que interactúa con el ecosistema de VC en nombre del Titular, Emisor o Verificador, por ejemplo ser una aplicación que se carga en el teléfono celular de una persona.

- Registro de datos verificables: Como de definió en capítulos anteriores, es un registro accesible por Internet donde se almacenan datos como los DID públicos y registros de revocación.

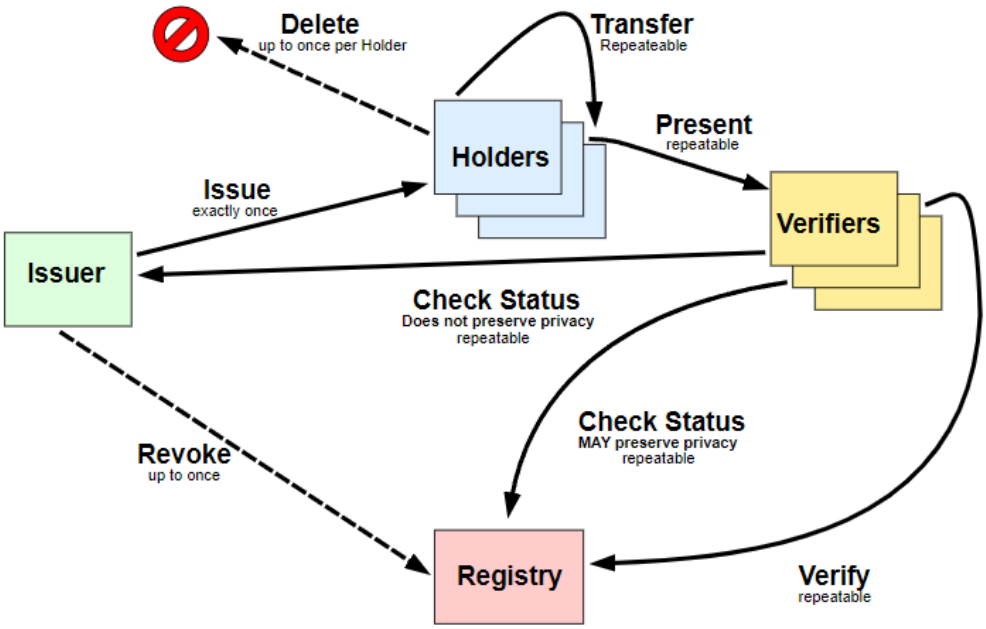

Ilustración 20 - Relación entre los actores en el ecosistema de Credenciales Verificables

Fuente: L. Lesavre, P. Varin… (2020)

3.4.4 Billeteras Digitales y Agentes

Billeteras Digitales

Los instrumentos de software que utilizan las personas para almacenar y administrar de manera segura las Credenciales Verificables, y poder realizar Presentaciones Verificables a distintas entidades en el modelo de Identidad Auto-Soberana son las Billeteras Digitales [36]. Estas billeteras se pueden encontrar en aplicaciones para celulares, navegadores web, servicios en la nube, e inclusive en dispositivos hardware como los dispositivos HSM (Hardware Security Modules).

El Sistema de Administración de Claves (KMS – Key Management System), es el corazón de las Billeteras Digitales, ya que es el responsable de la generación, rotación, revocación, almacenamiento, firma y protección de las llaves criptográficas utilizadas y de todos los secretos asociados como la protección de la dirección de los enlaces utilizados en las pruebas de conocimiento cero.

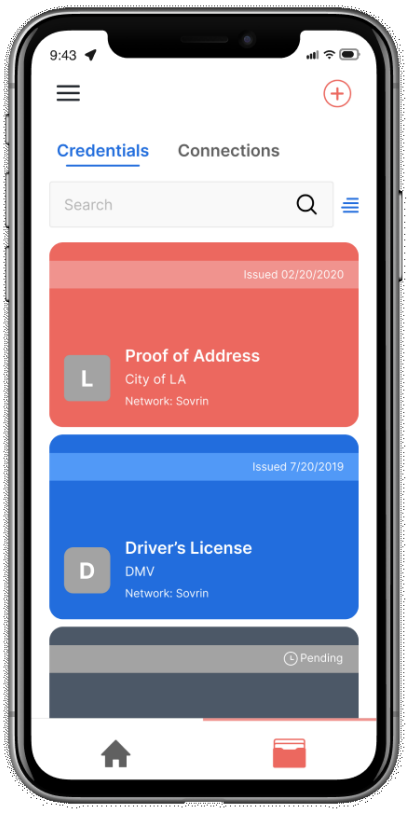

Ilustración 21 - Imagen de una Billetera Digital para celulares y sus credenciales

Fuente: Anna Johnson (2020) [36]

Agentes

Por otro lado a un Agente se le llama al software que da la capacidad a una entidad de asumir uno o más roles dentro del modelo de credenciales verificables y comunicarse con otros agentes. Estos roles pueden ser los nombrados anteriormente de Titular, Emisor o Verificador.

Normalmente los agentes con el rol de Titular almacenan las credenciales en las Billeteras Virtuales para poder interactuar con otras entidades. Se encarga de enviar y recibir mensajes estructurados, información, notificaciones de los controladores, a través de protocolos de comunicación DID.

Los agentes deben ofrecer la posibilidad de realizar copias de seguridad y restauración de los datos almacenados en la Billetera Virtual, esto se debe a la importancia de los datos almacenados y al hecho de que si se utiliza algún dispositivo móvil como un celular, estos se pueden perder, robar o estropear físicamente. Esto se puede lograr con los métodos de recuperación que ofrece el protocolo DID.

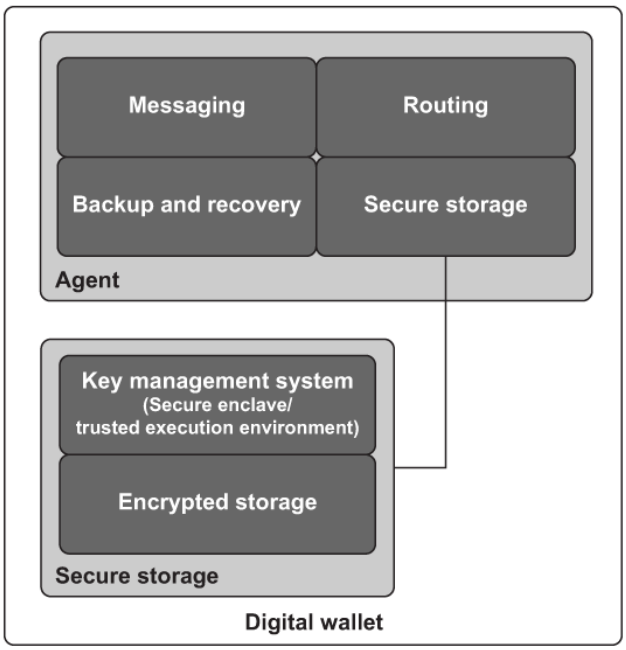

Ilustración 22 - Arquitectura conceptual de una Billetera Digital y un Agente

Fuente: Alex Preukschat y Drummond Reed (2021) [4]

Los protocolos de comunicación utilizados en la comunicación entre Agentes se pueden agrupar en dos:

- Protocolos Web securizados con TLS (Capa de Transporte Segura)
- Protocolo basado en mensajes DIDComm

Los protocolos Web como HTTP (Protocolo de Transferencia de Hipertexto) son prácticos en el sentido de que ya se encuentran desarrollados y correctamente utilizados se muestran seguros, pero presentan una serie de inconvenientes en el modelo de Identidad Auto-Soberana al estar diseñados para una arquitectura cliente-servidor, con un servidor pasivo, y no una descentralizada o que se requiera que ambas partes se encuentren activas para poder comunicarse. La mayoría de los protocolos web se basa en registros clave, proveedores de identidad, autoridades de certificación, proveedores de navegadores o aplicaciones, o centralizaciones similares.

DIDComm

DIDComm [37] es un protocolo desarrollado dentro del proyecto de código abierto Hyperledger de la Fundación Linux y donado en el año 2019 al Grupo de Trabajo DIDComm Working Group de la Fundación de Identidad Descentralizada.

Es un protocolo orientado a mensajes, con algunas similitudes a la mensajería de correo electrónico, ya que permite mensajes asíncronos, mensajes destinados a más de un receptor, y las respuestas pueden llegar por un canal distinto. Está desarrollado para comunicaciones peer-to-peer y presenta las siguientes características:

- Descentralizado: Los destinatarios se identifican mediante un DID.
- Seguro: Toda la comunicación está protegida (encriptada, firmada o ambas) por las claves asociadas con los DID.
- Privado: Debe dar al remitente la opción de permanecer anónimo para el destinatario.
- Independiente del transporte: Los mensajes se pueden enviar a través de cualquier medio de transporte como HTTP, Bluetooth, notificaciones push móviles, códigos QR, etc.
- Interoperable: Funciona con distintos lenguajes de programación, cadenas de bloques, proveedores, sistemas operativos/plataformas, redes, evitando el bloqueo de proveedores.
- Extensible: Permite que protocolos de nivel superior hereden las garantías de DIDComm.
- Permite un caso particular de Agentes que actúan como intermediarios en las comunicaciones, los Agentes de Ruteo que se utilizan para poder generar comunicaciones asíncronas y que las entidades reciban los mensajes cuando se encuentren preparadas. Está diseñado para que ningún intermediario conozca el origen o el destino final de un mensaje, sólo el siguiente salto.

Admite tres diferentes tipos de mensajes en formato JSON Web Message (JWM):

1. **Texto plano**: Sólo contiene metadata e información para llegar al destinatario.

```
{
  "id": "1234567890",
  "type": "<message-type-uri>",
  "from": "did:example:alice",
  "to": ["did:example:bob"],
  "created_time": 1516269022,
  "expires_time": 1516385931,
  "body": {
    "message_type_specific_attribute": "and its value",
    "another_attribute": "and its value"
  }
}
```

Ilustración 23 - Ejemplo de un mensaje DIDComm en formato de texto plano

Fuente: DIDComm Working Group (2023) [37]

2. **Mensajes Firmados**: Al mensaje de texto plano se le agrega una firma del tipo JSON Web Signature (JWS) para garantizar en no repudio.

3. **Mensajes Encriptados**: Al mensaje en texto plano (firmado o no) se lo encripta con el formato JSON Web Encryption para garantizar la confidencialidad.

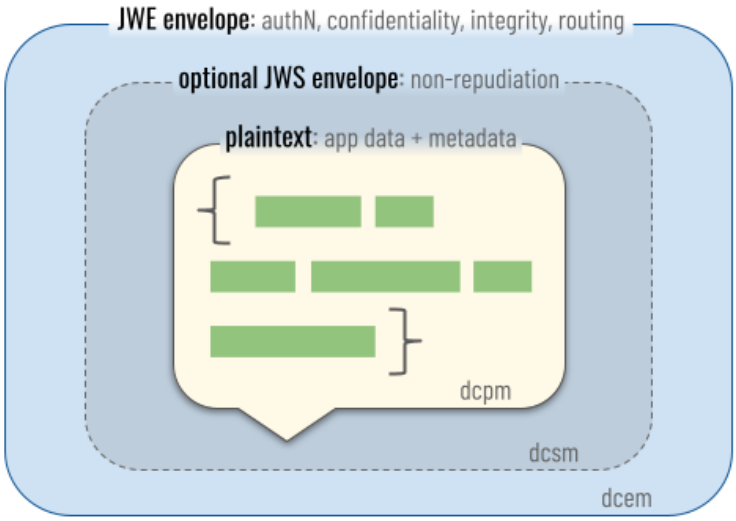

Ilustración 24 - Encapsulamiento de mensajes DIDComm

Fuente: DIDComm Working Group (2023) [37]

3.4.5 Sistema de Administración de Claves Descentralizado

Previamente se remarcó la importancia del Sistema de Administración de Claves (KMS) dentro de las Billeteras Digitales. En el modelo de Identidad Auto-Soberana el sistema que mejor se adapta es el Sistemas de Administración de Claves Descentralizado (DKMS) que es un nuevo paradigma desarrollado en el año 2018 por la empresa Evernym especializada en Identidad Auto-Soberana, a pedido del Departamento de Seguridad Nacional de Estados Unidos, para la gestión de claves criptográficas, diseñado para su uso en tecnologías DLT, y en donde no haya una autoridad centralizada [38], con la idea de crear un estándar abierto e independiente de cualquier proveedor y permita la portabilidad de credenciales entre proveedores de billeteras, dispositivos, sistemas y redes.

A diferencia de la clásica Infraestructura de Clave Púbica (PKI – Public Key Infraestructure) ampliamente utilizada en Internet, en donde la confianza de las claves se deposita en entidades centralizadas que registran, autorizan y validan los certificados, en el modelo DKMS se propone en enfoque distinto mediante una gestión descentralizada, en donde la confianza se encuentra en algoritmos y certificados auto generados por las mismas entidades aprovechando las propiedades de seguridad, inmutabilidad, disponibilidad y resiliencia de los sistemas de registros distribuidos como Blockchain para proporcionar distribución, verificación y recuperación de claves de forma altamente escalable [39]. Gracias a DKMS la responsabilidad de la gestión de sus propias claves ahora recae directamente sobre los individuos y la confianza se otorga gracias a las tecnologías DLT que soportan el almacenamiento de registros inmutables.

El desarrollo de DKMS busca los siguientes beneficios:

- **Evitar puntos de falla únicos:** al no depender de una entidad central.
- **Interoperabilidad:** permitiendo que dos entidades realicen el intercambio de claves y creando conexiones seguras peer-to-peer independientemente del software utilizado.
- **Portabilidad:** permite el traspaso de credenciales y secretos a otra billetera.
- **Resiliencia:** los datos se persisten sobre una tecnología DLT y encima de ella se crea una red de confianza distribuida donde cualquier par puede intercambiar

claves, formar conexiones y emitir o aceptar credenciales verificables de cualquier otro par.

- **Desacoplar la verificación de Identidad de la verificación de Clave Pública:** Los certificados utilizados en PKI como X.509 suelen tener todos los datos de la entidad, DKMS los DIDs se generan a partir de un par de claves públicas/privadas utilizando un certificado auto emitido, con lo que un Controlador puede demostrar control sobre el DID firmando un Documento DID con su clave privada.

En el año 2021 el Phd. Samuel Smith [40] presentó un proyecto llamado Infraestructura de Recepción de Eventos Clave (KERI por sus siglas en inglés). Este ofrece un enfoque para desarrollar una solución de IAS en el que plantea que la demostración de las propiedades de la clave privada y la rotación de claves no dependa de la utilización de DLT.

Su enfoque propone el uso de un identificador autogenerado que demuestre que solo ese identificador se encuentra vinculado a una clave pública sin necesidad de usar DLT, basándose en la confianza criptográfica en lugar de un algoritmo de consenso de una blockchain. Se utiliza la entropía para generar primero un par de claves en donde la clave privada se almacena de forma segura, mientras que la clave pública se ofrece a quien la necesite. La clave pública se utiliza para generar un identificador único.

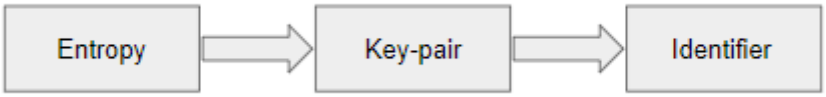

Ilustración 25 - Generación del Identificador único en KERI

Fuente: Smith Samuel (2021) [40]

En resumen, KERI puede proporcionar la infraestructura subyacente para respaldar un sistema de gestión de claves descentralizado universal para IAS. Aunque se encuentra todavía en desarrollo, ésta solución es útil para alcanzar los objetivos de interoperabilidad en IAS.

4. TRABAJO EXPERIMENTAL

En esta sección se describirá el trabajo realizado en la implementación de una prueba de concepto de Identidad Auto Soberana dentro de la Prosecretaría TICs de la Universidad Nacional del Noroeste de la Provincia de Buenos Aires.

Primero se comenzará describiendo las herramientas, versiones, y características a tener en cuenta de los proyectos de software utilizados en el despliegue del agente emisor de credenciales por parte de la universidad, el DLT público utilizado y la billetera virtual utilizada para almacenar las credenciales de los alumnos.

Luego se describirá el diseño de arquitectura alcanzado y el caso de uso desarrollado en la prueba de concepto. Se describirá la experiencia de la emisión de credenciales, evaluación de presentaciones realizadas con las mismas y consideraciones a tener en cuenta en los resultados obtenidos.

4.1 Tecnologías utilizadas

4.1.1 Hyperledger Indy

El proyecto Indy [41] fue desarrollado en un comienzo dentro de la Fundación Sovrin, que en el año 2017 delegó a la Fundación Linux, siendo actualmente parte de su proyecto Hyperledger el cual engloba múltiples proyectos de código abierto que hacen uso de ledgers distribuidos basados en cadenas de bloques. En particular Indy es un DLT especialmente diseñado para soluciones de identidad descentralizada que incluye características como:

- Soporte de credenciales verificables basadas en tecnología de prueba de conocimiento cero.
- Soporte de Identificadores descentralizados o DIDs.
- Un Kit de Desarrollo de Software (SDK) para la construcción de agentes.
- Una implementación de un DLT público autorizado.

Indy es una cadena de bloques diseñada para ser utilizada únicamente en soluciones IAS por lo que no soporta el intercambio de activos ni tampoco contratos inteligentes, aunque existen extensiones para otorgar diferentes características como el uso de tokens para obtener permiso de escritura en la cadena, que buscan evitar, por ejemplo, ataques de denegación de servicios con operaciones gratuitas de escritura.

Indy es un tipo de DLT público-permisionada, diseñada con un enfoque de acceso público a los datos en los bloques pero en la que sólo los participantes aprobados, los administradores, pueden participar en el proceso de validación. El algoritmo de consenso para decidir el contenido del siguiente bloque agregado a la cadena es una implementación del algoritmo de Tolerancia a Fallas Bizantinas (TFB) llamado Plenum, diseñado para lograr consenso aun cuando muchos de los nodos no están operativos o accesibles. El número de nodos defectuosos *(f)* en una red TFB que funciona correctamente es $f = (N-1)/3$, donde N es el número total de nodos en la red.

British Columbia VON Network

El gobierno de la provincia canadiense British Columbia [42] desarrolla diferentes proyectos para promover el aprendizaje y prueba del uso de soluciones de Identidad Auto Soberana. Entre estos proyectos destaca el de la Red de Organizaciones Verificables o Verifiable Organizations Network (VON por sus siglas en inglés) [43], el cual es una implementación de Hyperledger Indy portable en contenedores bajo la tecnología Docker [44] e incluye un servicio web de consulta para analizar el estado de los nodos y buscar información sobre las transacciones realizadas, entre otras características. Este proyecto no está pensado para su uso en producción y su principal objetivo es el de simplificar al usuario el despliegue de una red DLT con Hyerledger Indy, pero además ofrece una implementación pública de pruebas que corre en el dominio *https://test.bcovrin.vonx.io/,* con las características de que cualquier agente puede escribir sin previa autorización y de que cada 15 días reinicia sus datos. Esta DLT fue la utilizada en esta tesis principalmente por:

- La dificultad de encontrar una Billetera Digital que permita la configuración manual de una DLT customizada.
- Por venir pre configurada en la mayoría de las Billeteras Digitales desarrolladas para el uso de Identidad Auto Soberana.
- Por poder utilizarla sin incurrir en gastos económicos ni necesitar solicitar autorización previa para su uso.
- Por disponer de interfaces públicas donde poder analizar el estado del DLT y sus transacciones, en las cuales poder validar fácilmente los registros almacenados en ella.

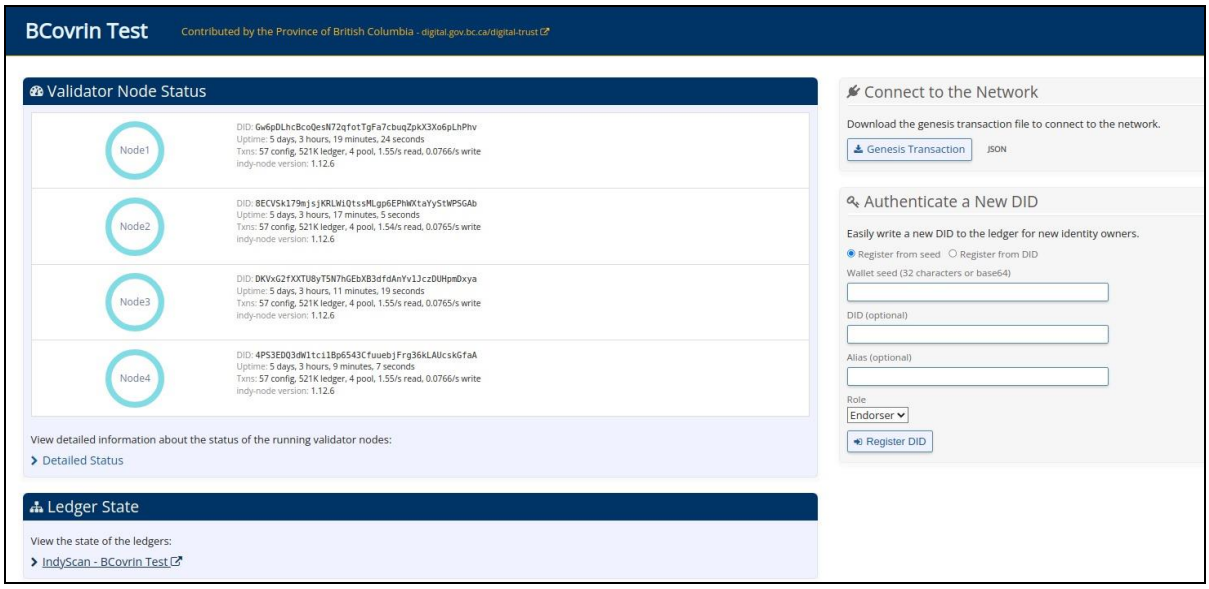

Ilustración 26 - Interfaz pública del estado de la DLT BCovrin Test

Fuente: autor

Actualmente la versión del proyecto Indy utilizada en el despliegue de los nodos de la cadena BCrovrin es la versión 1.12.6, publicada 2 de Septiembre del 2022 [45]. Está versión utiliza los métodos de la especificación Sovrin [32], pero se espera que el proyecto migre en versiones futuras a los métodos de la especificación Indy que actualmente se encuentra en borrador [46], y el cual presenta una serie de cambios en los métodos en los datos y objetos que la DLT acepta. En esta tesis se detallan los cambios en los métodos y objetos utilizados durante la prueba de concepto a fin de analizar los mismos.

4.1.2 Hyperledger Aries

Para el despliegue del agente utilizado por la universidad para la emisión de Credenciales Verificables se utilizó como base una implementación del proyecto Aries [47] que al igual que Indy, pertenece a la Fundación Linux la cual ofrece dentro de su proyecto Hyperledger. El proyecto Aries ofrece un conjunto de herramientas y librerías que permiten desarrollar agentes en diferentes lenguajes de programación con soporte para múltiples DLTs, tipos de credenciales, y protocolos. En particular en esta tesis se utilizó el desarrollado en Python, llamado Aries Cloud Agent Python, conocido como ACA-Py [48].

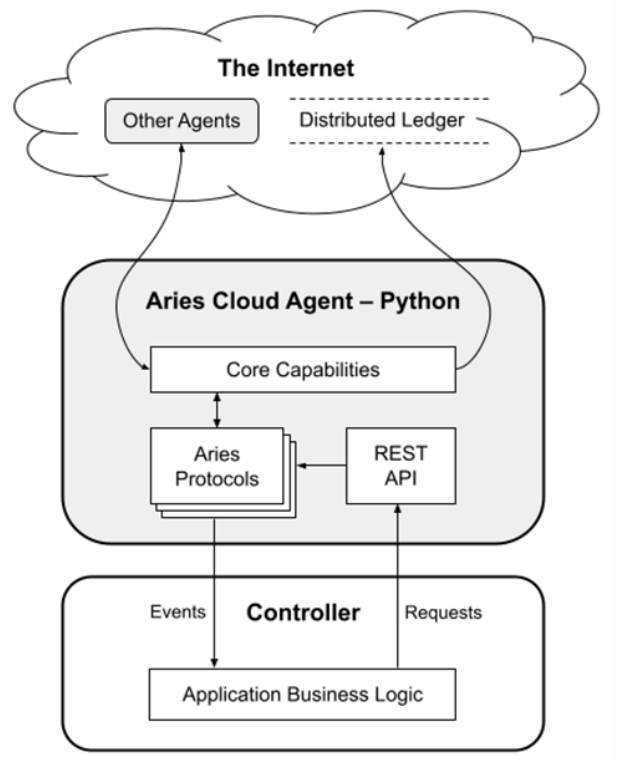

Ilustración 27 - Descripción general de la arquitectura propuesta por ACA-Py

Fuente: Hyperledger Aries (2024) [48]

Además se desarrolló un controlador web para interactuar con el agente, orientado al caso de uso de la tesis, permitiendo la gestión de emisión de credenciales por usuarios sin conocimientos técnicos.

Despliegue del Agente

Actualmente ACA-Py es un proyecto que está en constante desarrollo, y durante el tiempo que llevo el desarrollo de esta tesis fueron publicándose distintas actualizaciones. La versión utilizada y a la que se hace referencia en este apartado es la versión 0.12.1, publicada el primero de Mayo de 2024, la última versión disponible a la fecha de publicar esta tesis.

Como herramienta de integración y comunicación en distintos entornos, el proyecto ACA-Py implementa una interfaz de programación de aplicaciones REST (transferencia de estado representacional) sobre el protocolo HTTP (protocolo de transferencia de hipertexto), basada en las especificaciones OpenAPI/Swagger [49] con la que ofrece distintos métodos para interactuar con el agente y dar diferentes instrucciones como la de invitar a conectar a otro agente o emitir credenciales, por nombrar algunas.

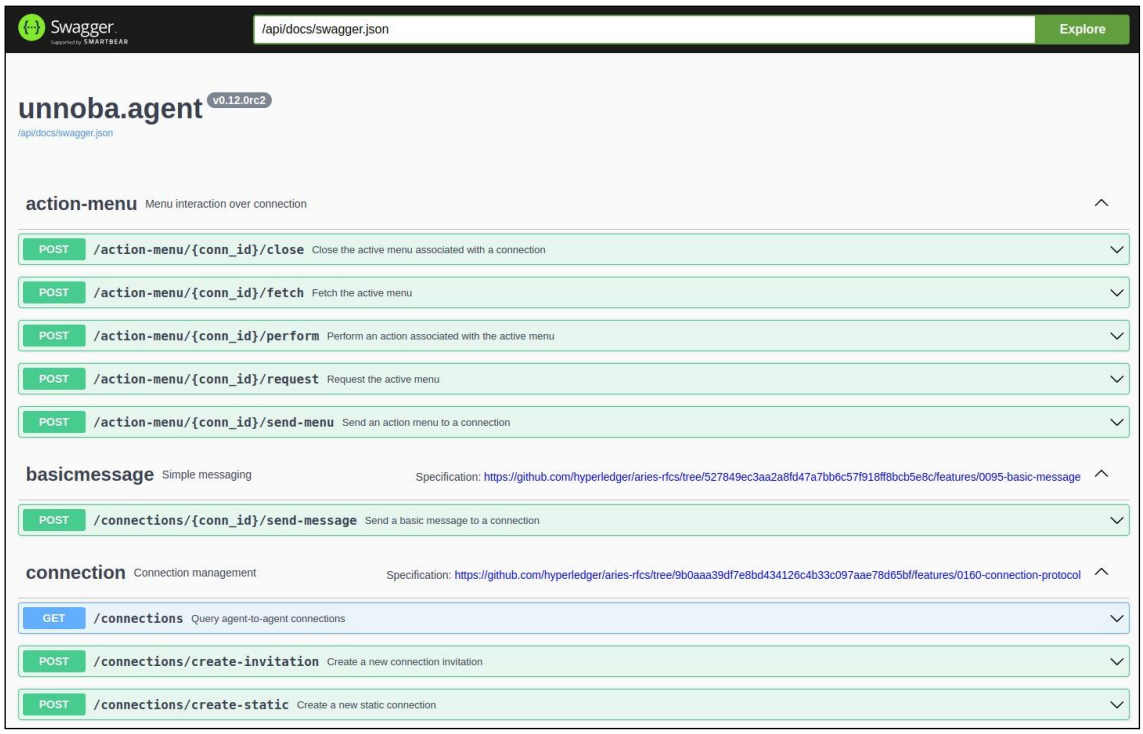

Ilustración 28 - Interfaz de comunicación del agente ACA-Py

Fuente: autor

Para poder manejar el agente haciendo uso de esta interfaz se desarrolló una controladora web la cual ofrece las opciones de crear un esquema de credenciales a utilizar con el formato deseado, invitar a conectar a otros agente, emitir credenciales verificables y emitir pruebas para validar si las credenciales son capaces de cumplirlas.

Ilustración 29 - Controladora desarrollada para comunicarse con el agente

Fuente: autor

Los métodos que invoca a la interfaz del agente son:

- **wallet/did/public:** Obtener el DID público actual.
- **connections:** Ver todas las conexiones.
- **connections/id_mensaje/send-message:** Enviar mensaje de texto a una conexión.
- **connections/create-invitation:** Crear una nueva invitación de conexión.
- **connections/id_conexion_eliminar:** Eliminar un registro de conexión existente.
- **present-proof/send-request:** Enviar prueba a un agente.
- **issue-credential/send-offer:** Emitir una credencial.
- **schemas:** Envía un esquema a la DLT.
- **credential-definitions:** Envía una Credential Definition a la DLT.

Vale aclarar que como los protocolos relacionados a IAS están en desarrollo y por ende los proyectos que los implementan, es importante prestar atención en los cambios de versiones ya que pueden cambiar el funcionamiento de estos, agregar o eliminar nuevas características.

El proyecto ACA-Py no es ajeno a esto y define un Perfil de interoperabilidad de Aries [50] que proporciona un conjunto definido de versiones de RFC para que los proyectos que apunten a la implementación de su agente, en el cual nos advierte de estos cambios a futuro que podrían llevar a incompatibilidades con la comunicación entre agentes, siendo los más relevantes:

- Se abandona el protocolo de conexión de agentes a través de invitaciones a favor del Intercambio de DIDs.
- Nuevo Protocolo de Emisión de Credenciales 2.0
- Nuevo Mecanismo de Presentación de Pruebas 2.0
- Nuevo Protocolo de Descubrimiento de Características 2.0

4.1.3 Lissi ID-Wallet

Para el uso de una billetera digital en dónde guardar las Credenciales Verificables se utilizó Lissi ID-Wallet [51], aplicación de la empresa alemana Lissi GmbH, y la cual se caracteriza por ser una EUDI-Wallet al cumplir con los requisitos de la regulación europea eIDAS 2.0 [52]. La versión utilizada en esta tesis fue la última disponible, siendo la 1.10.6, y entre sus características más interesantes encontramos:

- Soporte de protocolos de comunicación DIDComm y OpenID4VC.
- Soportar almacenar Credenciales Verificables en formato recomendado por la W3C, JSON, mDL o AnonCreds, entre otros.
- Soportar realizar Presentaciones Verificables en formato JWT, JSON-LD, y OpenID4VP.

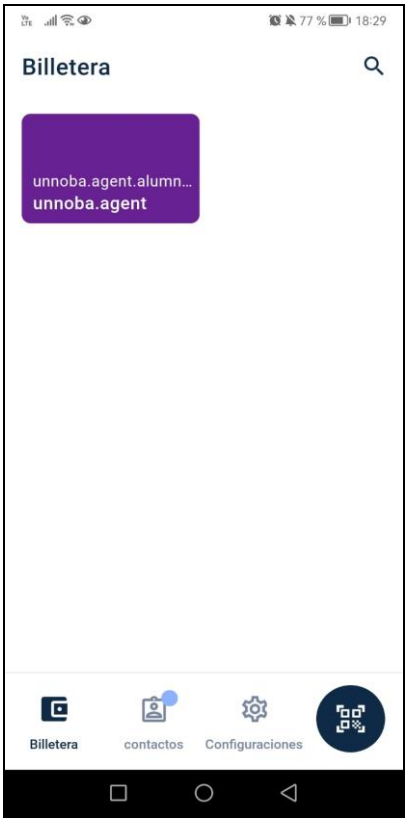

Ilustración 30 - Billetera Lissi ID-Wallet ejecutándose en un celular

Fuente: autor

Cabe aclarar que no todas las billeteras digitales son compatibles para comunicarse con todas las DLTs, esto se debe principalmente a que deben implementar los métodos de comunicación y objetos de datos que cada DLT defina.

4.2 Diseño de Arquitectura IAS

Con las herramientas descriptas anteriormente se buscó implementar y analizar un prototipo funcional de identidad digital auto soberana para alumnos de la universidad Nacional del Noroeste de la Provincia de Buenos Aires, ambiente académico universitario que es donde se desarrolla profesionalmente el tesista, que garantice los siguientes puntos:

- Que las credenciales emitidas por las organizaciones sean de confianza, pudiéndose validar contra alguna tecnología del tipo Libro Mayor Distribuido (DLT) como blockchain.
- Que los individuos tengan control sobre las mismas pudiéndolas administrar desde una billetera virtual.
- Que los usuarios puedan realizar Presentaciones Verificables con las credenciales que disponen en sus billeteras.

Arquitectura propuesta implementada:

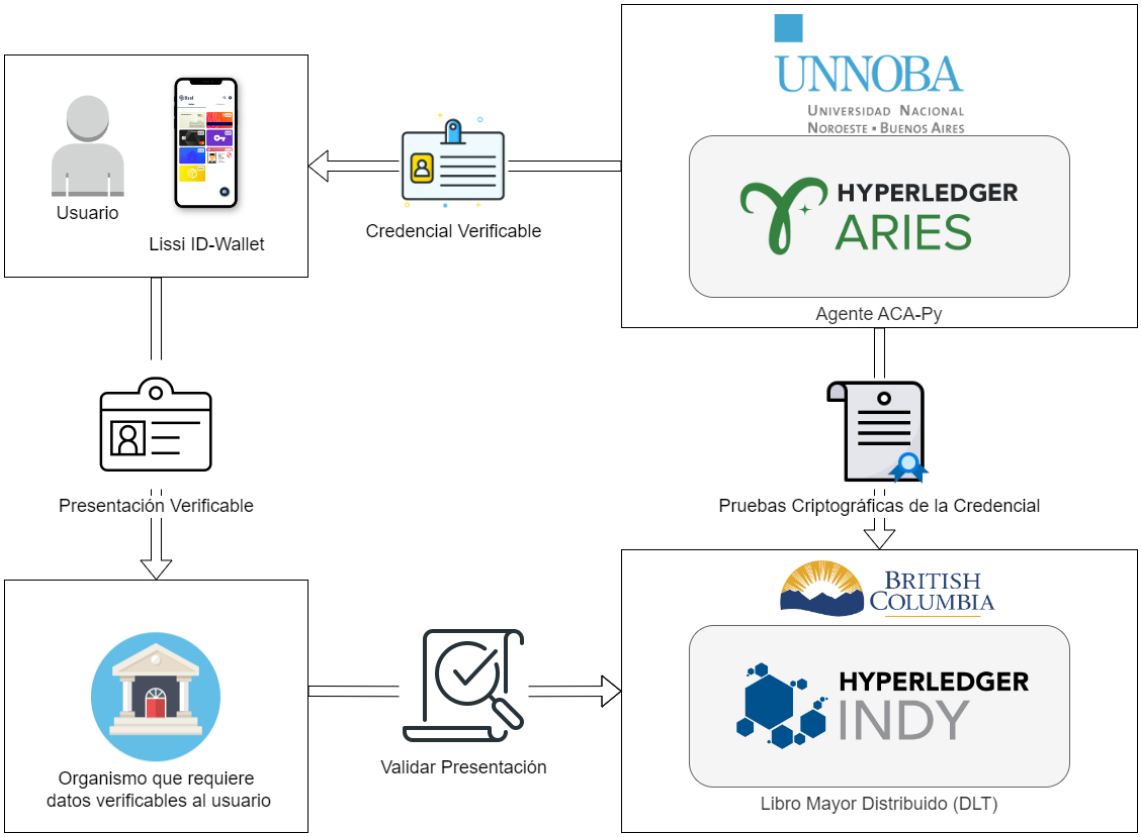

Ilustración 31 - Diseño de Arquitectura propuesta y sus componentes

Fuente: autor

4.2.1 Prueba de concepto

Esta prueba de concepto se desarrolló dentro de la Prosecretaria TICs de la Universidad Nacional del Noroeste de la Provincia de Buenos Aires. Para realizar la prueba se definió un caso de uso en el que la universidad emite credenciales que contienen datos académicos e identificatorios a sus alumnos y una prueba en la que deben realizar una presentación conteniendo información parcial de sus credenciales y en la que además se evalúa con una prueba de conocimiento cero una si un atributo cumple una condición aritmética.

Para llevar a cabo esta prueba de concepto fue necesario desplegar un agente emisor de credenciales para la universidad y desarrollar una controladora para un manejo sencillo de la misma pensada en usuarios administrativos de perfil no técnico.

Durante esta prueba de concepto se buscó de evaluar el grado de madurez de las herramientas utilizadas y la viabilidad de poder llevarlas en un futuro a un ambiente productivo.

Excede el objetivo de esta tesis, pero es esencial aclarar que para poder llevar a la práctica el uso de IAS dentro de cualquier ámbito no sólo hacen falta las herramientas tecnológicas, sino además definir un marco de confianza y regulaciones necesarias para darle valides jurídica en donde se desea comenzar a utilizar y que estas cumplan con las leyes de protección de datos vigentes.

4.2.2 Registro del DID y Documento DID

Una vez inicializado el agente de la universidad podemos analizar los datos registrados en la DLT tanto del DID como del Documento DID a utilizar. En este último podemos ver la información del DID autorizado para modificarlos y sus datos de autenticación. En este caso el agente que maneja la universidad va a actuar como emisor y controlador del documento. También podemos controlar valores como URL y clave pública para conectar y validar el agente:


```
{
  "results": [
    {
      "did": "F8dfSB7zEqubx6iXCofWDY",
      "verkey": "8hjBqvzM9cbweE5Efkp37C8cR55dCcX5Waofgz4JvQ7D",
      "posture": "posted",
      "key_type": "ed25519",
      "method": "sov"
    }
  ]
}
```


Ilustración 32 - Consulta de DID del agente

Fuente: autor

En particular Hyperledget Indy almacena en la DLT distintos objetos para clasificar los registros almacenados. Para poder registrar un DID se utiliza el objeto de datos llamado NYM (abreviatura de Verinym) que se asocia con la identidad legal de un propietario de identidad. Un objeto NYM no es un DID en sí mismo, pero contiene todos los datos de la especificación de este, por lo tanto escribir un objeto NYM en Indy es el equivalente a publicar un DID en una DLT.

En la página web de la DLT de BCovrin utilizada podemos corroborar los registros creados en la cadena de bloques y datos de la transacción realizada:

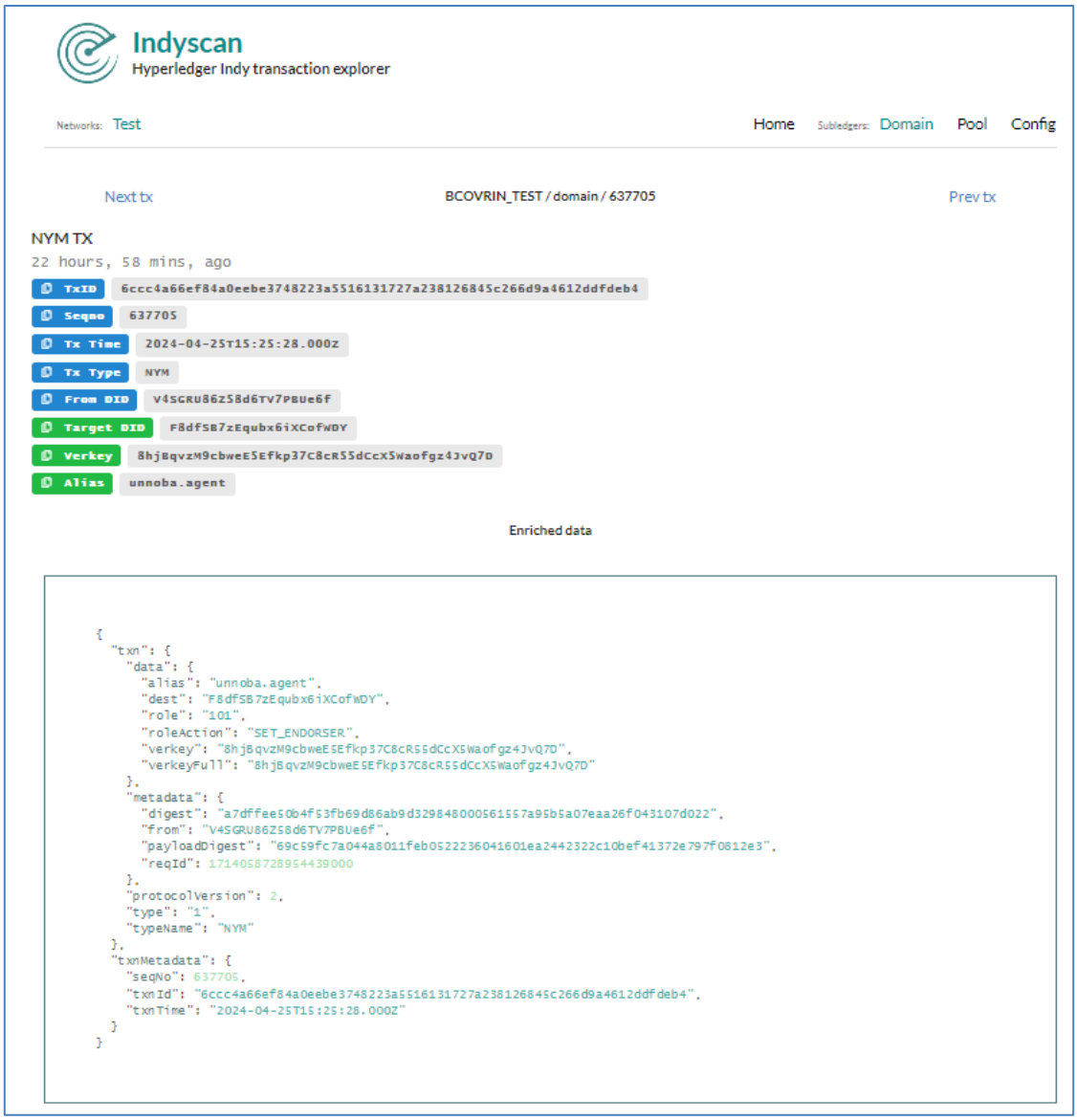

Ilustración 33 - Registro del DID en la DLT

Fuente: autor

En Indy un objeto del tipo ATTRIB (abreviatura de atributo) extiende la cantidad de información que podemos obtener sobre un DID y es utilizado para almacenar datos sobre los Documentos DID y así poder resolverlos, en particular se utiliza para almacenar el atributo endpoint que contiene una URL o dirección IP asociada al agente.

Como se comentó anteriormente, dentro del proyecto Indy se está desarrollando un borrador con nuevas especificaciones sobre los métodos Indy y tipos objetos a almacenar en futuras versiones en detrimento de los métodos Sovrin y en este se desaconseja el uso del objeto ATTRIB para almacenar esta información y en su

reemplazo propone agregar el atributo llamado diddocContent con el mismo propósito al objeto NYM [46].

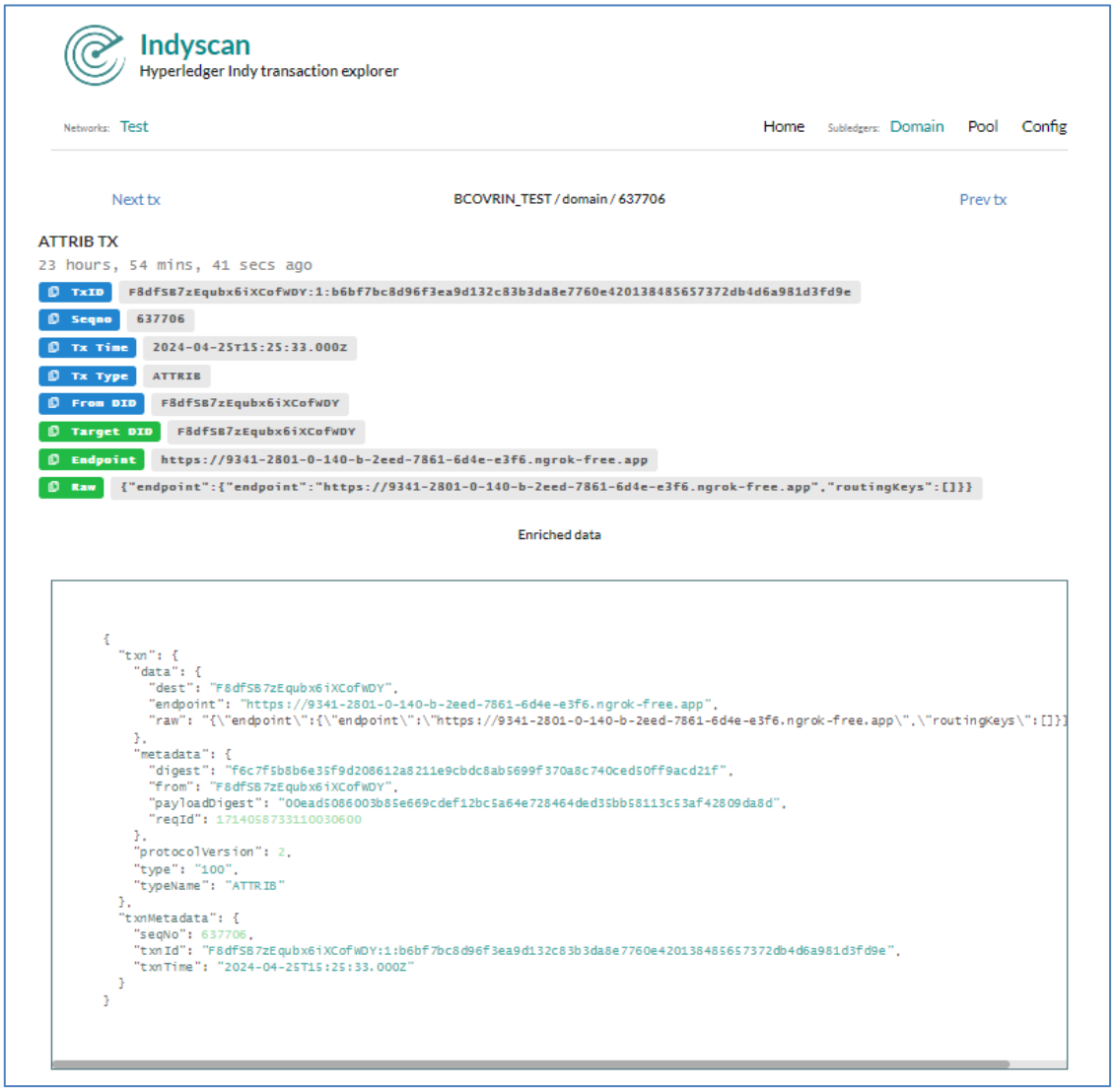

Ilustración 34 - Objeto ATTRIB

Fuente: autor

4.2.3 Definición del esquema a utilizar

El siguiente paso es definir y publicar un esquema de credenciales a utilizar, es decir qué datos va a contener la credencial emitida por la universidad. En este caso los datos que se eligieron para la prueba fueron:

- Apellido
- Nombre
- DNI
- Fecha de nacimiento
- Número de legajo
- Carrera
- Escuela
- Fecha de inscripción

Desde la controladora web podemos realizar esta acción corroborando que el esquema y sus atributos a utilizar es el deseado. Publicar el esquema nos devolverá los valores del ID del Esquema y el ID de la Definición de Credenciales dentro de la cadena de bloques. Vale aclarar que el esquema es la estructura de la credencial y la definición de credenciales son los emisores autorizados a emitir credenciales utilizando el esquema.

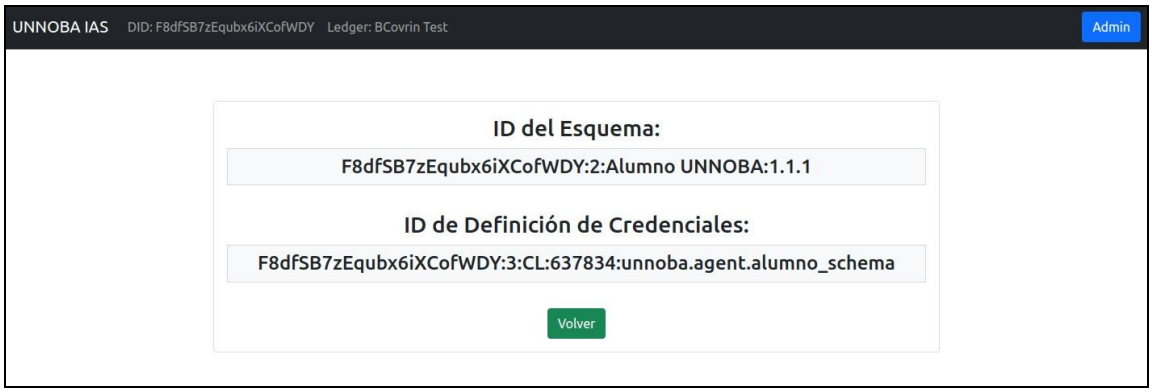

Ilustración 35 - ID del Esquema y Definición de Credenciales a utilizar

Fuente: autor

Estos valores también los podemos corroborar en la DLT. El esquema se almacena en un objeto del tipo SCHEMA y su consulta nos devolverá una respuesta como la siguiente:

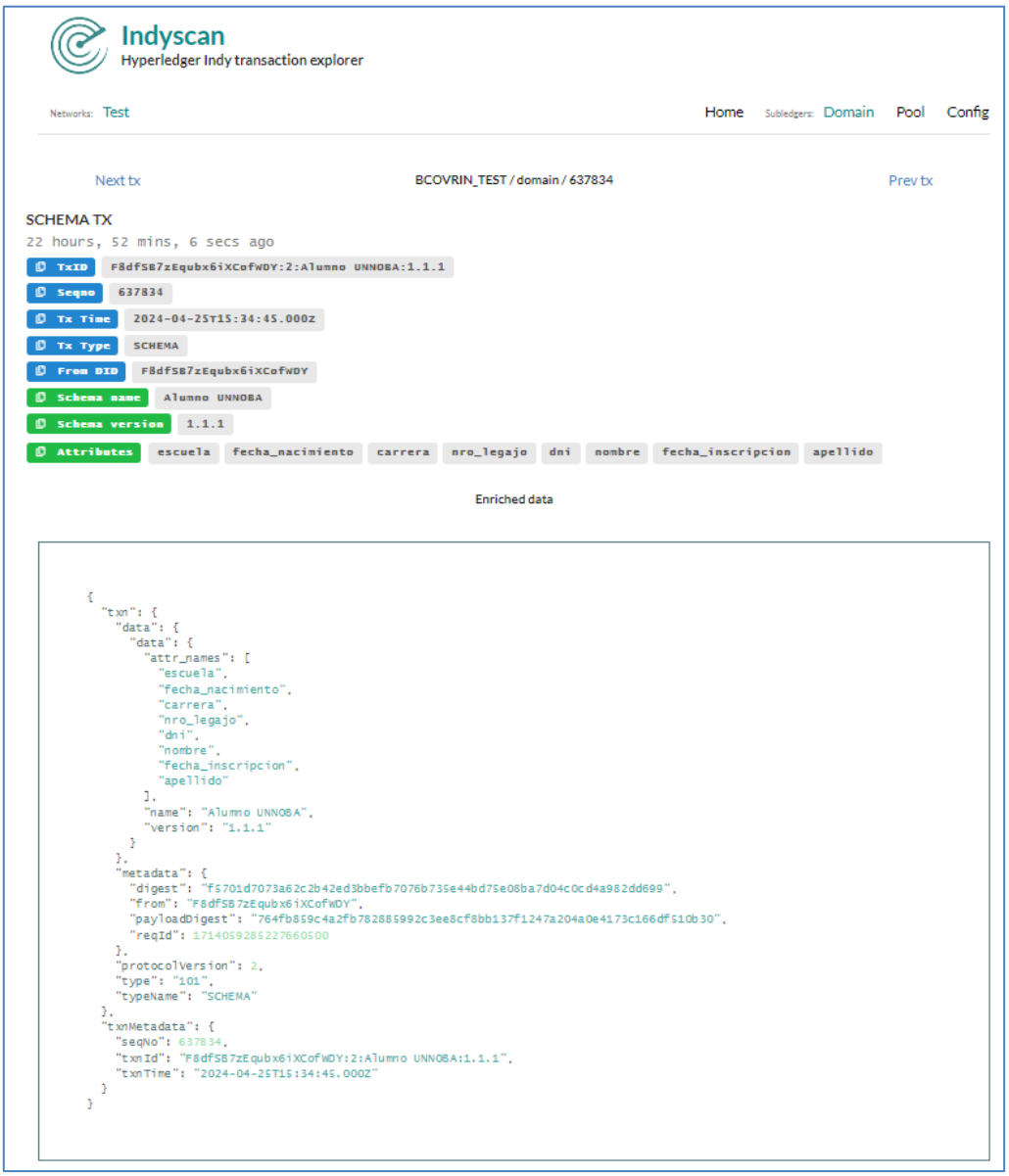

Ilustración 36 - Registro del Esquema en la DLT

Fuente: autor

La definición de credenciales se almacenan en objetos del tipo CLAIM_DEF y su consulta nos devolverá una respuesta como la siguiente:

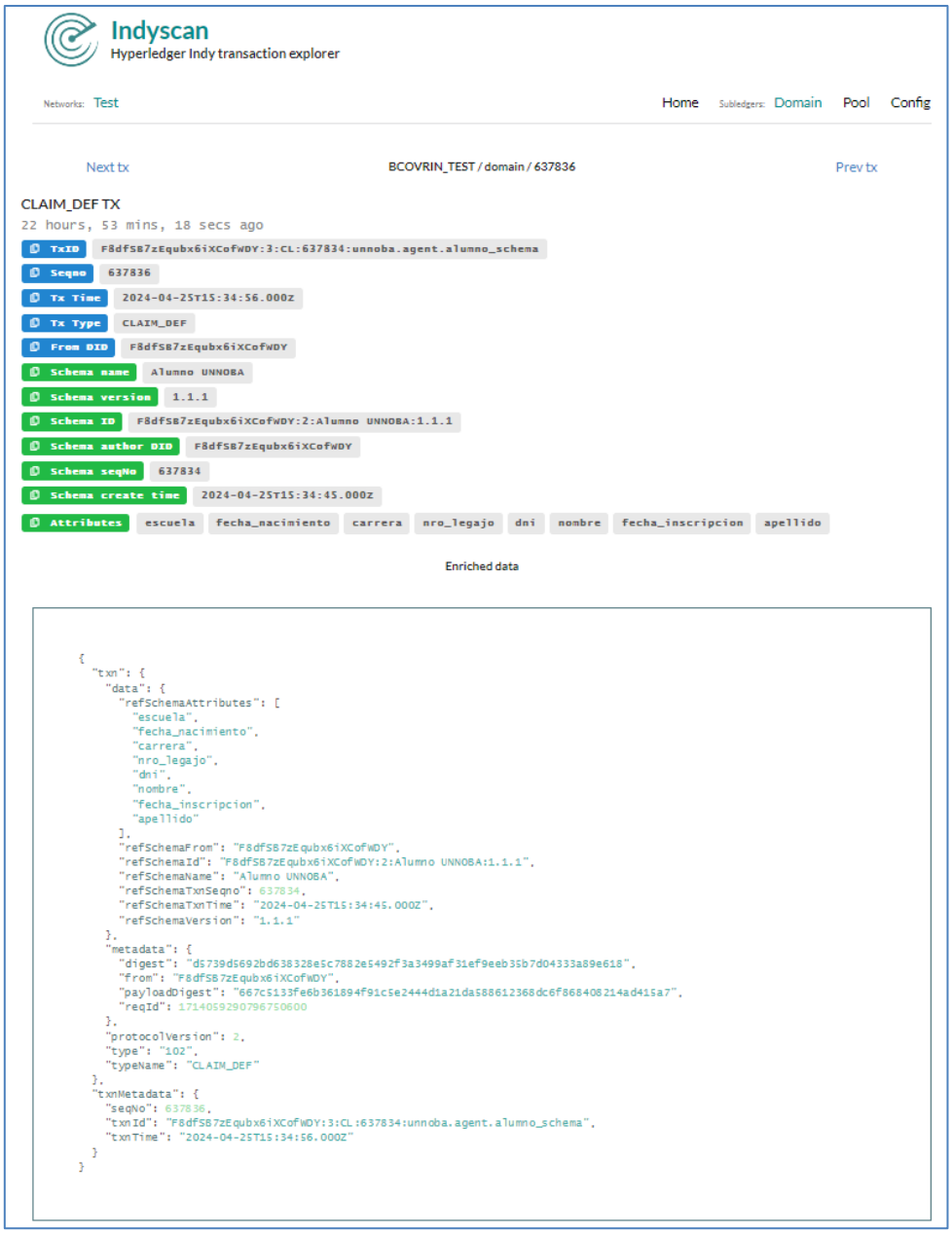

Ilustración 37 - Registro del Claim Definiton en la DLT

Fuente: autor

Al igual que como se mencionó antes con el tipo de objeto ATTRIB, en los borradores de las especificaciones sobre los futuros métodos Indy, se deja obsoleto el tipo CLAIM_DEF y se reemplazará por uno llamado CRED_DEF [46].

4.2.4 Invitar a los usuarios a conectar

Una vez definido el esquema a utilizar en la DLT el agente emisor ya puede empezar a invitar a conectar a los usuarios a fin de poder emitirles las credenciales. La forma más práctica de realizar esto es que el emisor genere un código QR con la información necesaria para que el agente que va a recibir la credencial pueda conectarse:

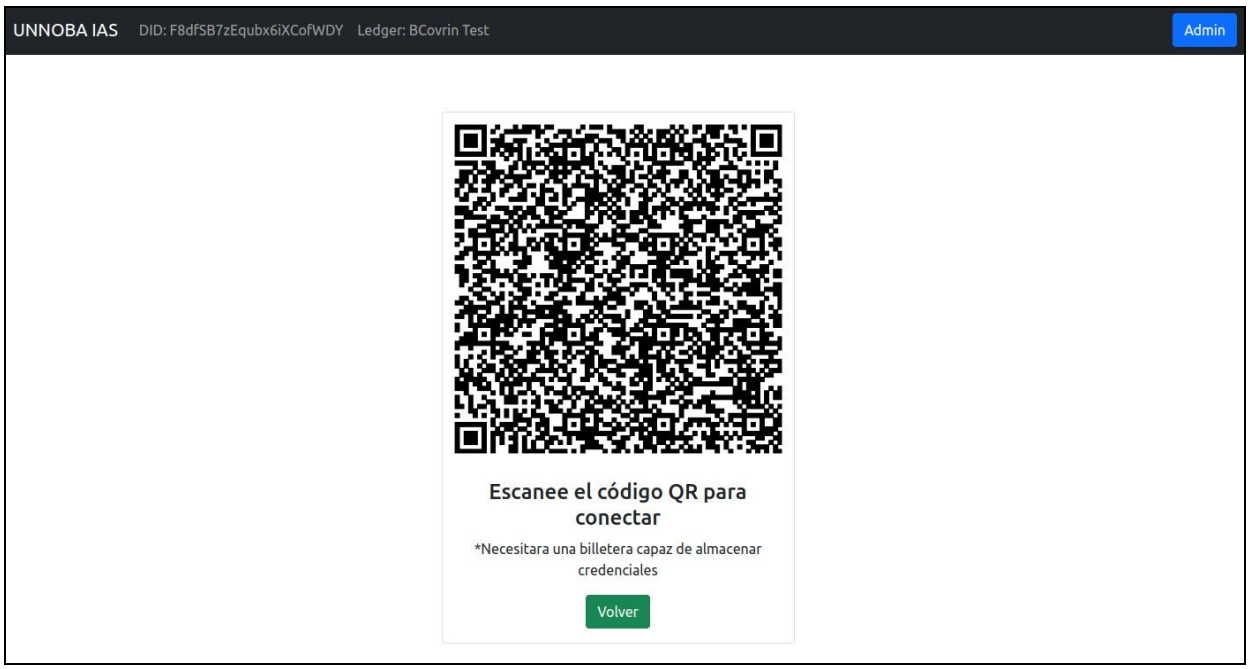

Ilustración 38 - Código QR para invitar al usuario a conectar

Fuente: autor

El usuario debe leer el código QR con su billetera y esta mostrará al usuario un mensaje preguntando si desea aceptar o no la conexión, aquí el usuario puede leer los datos del agente de la universidad con el que va a conectar. Aceptar el canal de comunicación es un requisito necesario para que el emisor pueda enviar la credencial al usuario.

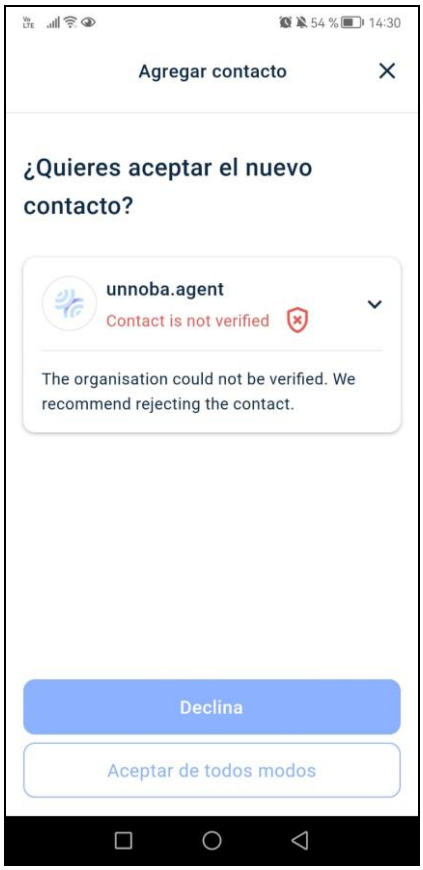

Ilustración 39 - Mensaje de conexión

Fuente: autor

En la controladora web también podemos ver el estado de las invitaciones generadas, si las conexiones fueron aceptadas y establecidas por el usuario con su billetera virtual y el estado en que se encuentran. Dentro de esta sección tenemos la posibilidad de eliminar las conexiones y de enviarles un mensaje de texto a las conexiones activas:

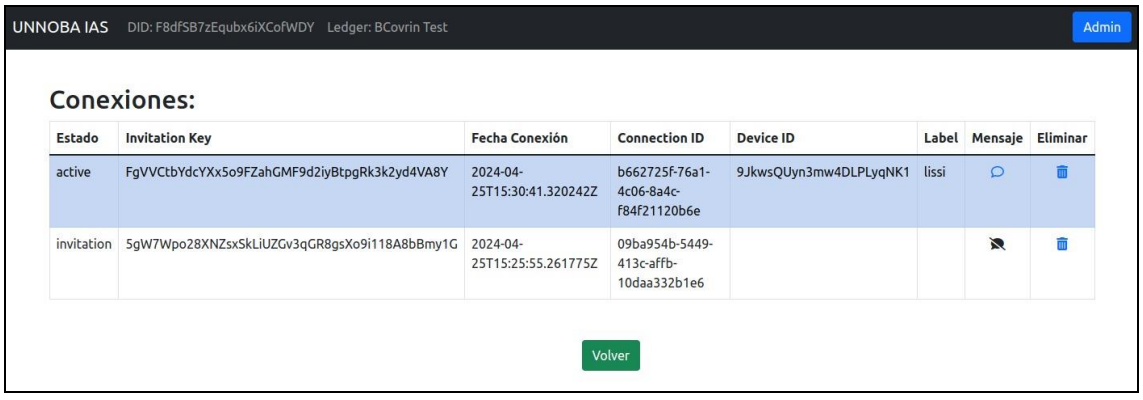

Ilustración 40 - Conexiones y sus estados

Fuente: autor

A continuación un mensaje de texto emitido por el agente de la universidad y recibido en la billetera:

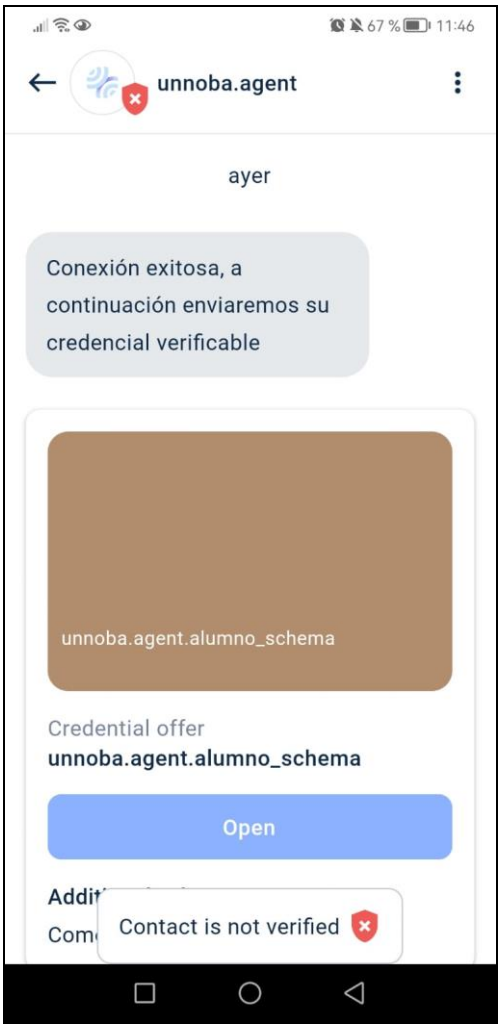

Ilustración 41 - Mensaje de texto recibido

Fuente: autor

4.2.5 Emitir Credencial Verificable

Una vez aceptada la conexión, el agente emisor ya es técnicamente capaz de emitir una Credencial Verificable al usuario. Para lograr esto podremos utilizar la controladora, la cual pedirá la carga de datos de los campos definidos en el esquema de la credencial y la conexión del usuario a la cual se enviará la misma.

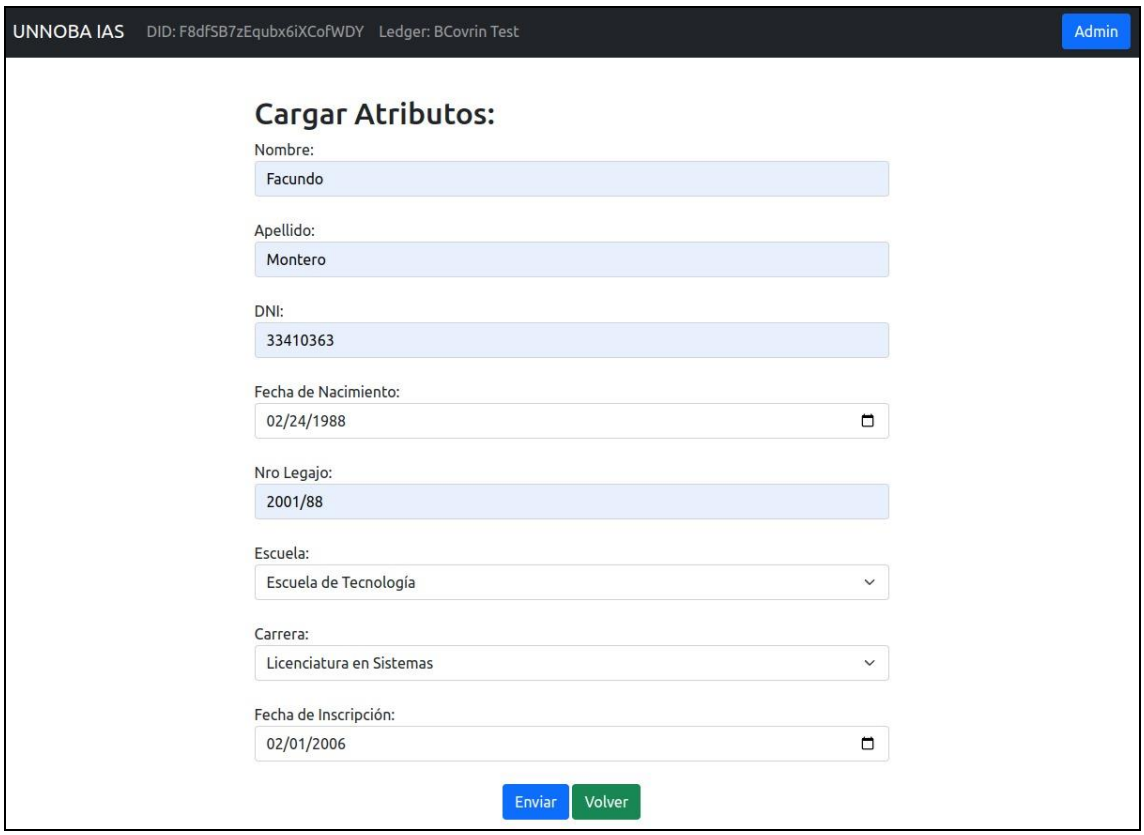

Ilustración 42 - Carga de datos de la Credencial Verificable

Fuente: autor

Posteriormente la Billetera Digital preguntará al usuario si desea aceptar la credencial, mostrando los datos contenidos en la misma. En caso de aceptarla la billetera procederá a almacenarla de manera segura.

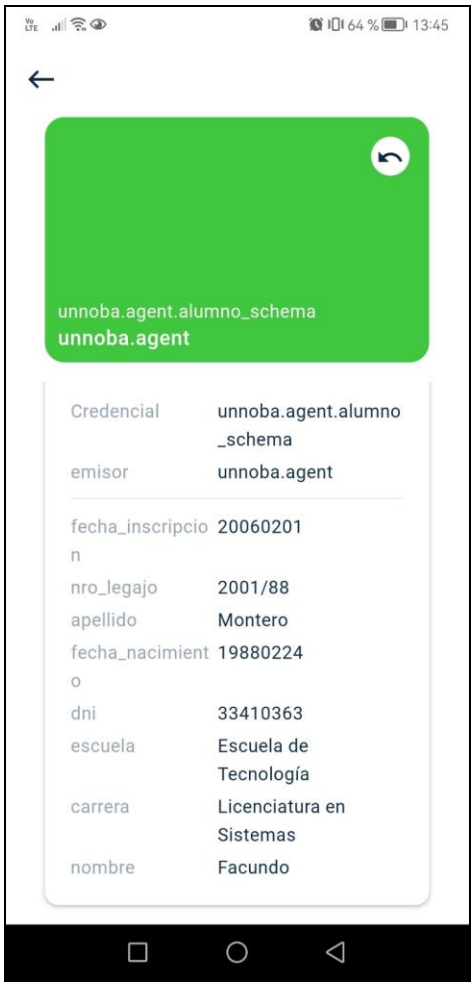

Ilustración 43 - Credencial ofrecida al usuario

Fuente: autor

Una vez finalizado el proceso de entrega de la credencial el usuario ya se encuentra en condiciones hacer uso de la misma emitiendo Presentaciones Verificables.

4.2.6 Realizar una prueba de Presentación Verificable

Para probar la credencial emitida se creó una Solicitud de Prueba con el agente emisor la cual consulta por los datos del esquema Nombre, Apellido, Carrera y Fecha de Inscripción, pero en relación a la fecha de inscripción sólo evalúa que la Presentación Verificable cumpla la condición de que la persona se haya inscripto hace más de 3 años.

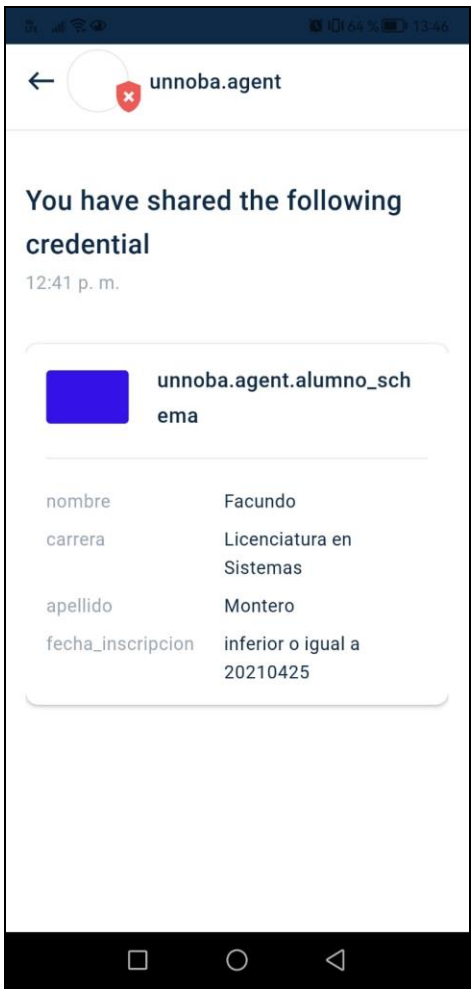

Ilustración 44 - Presentación Verificable emitida

Fuente: autor

Una vez recibida la Presentación Verificable el agente que envió la prueba puede, en caso satisfactorio, dar por superada la misma. En este caso la controladora mostrará el siguiente mensaje.

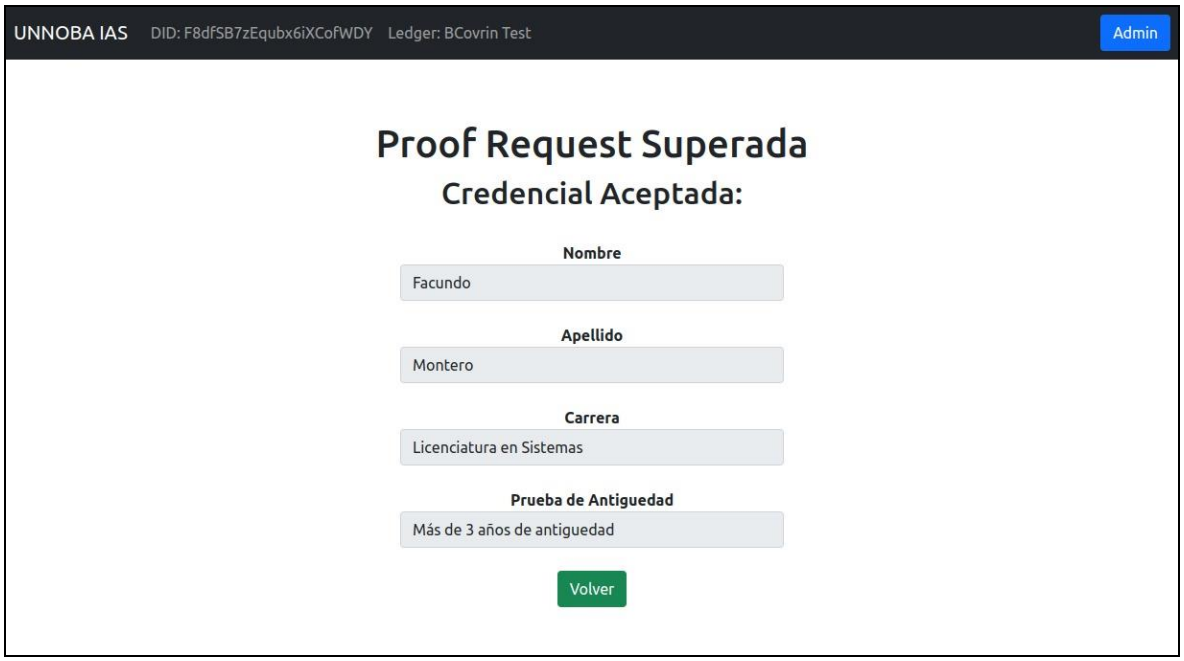

Ilustración 45 - Proof Request superada

Fuente: autor

4.2.7 Revocar una Credencial Verificable

Actualmente la especificación de Credenciales Verificables de la W3C no tiene una normativa de cómo debería llevarse a cabo la revocación de Credenciales Verificables [29]. Existen diferentes estrategias para llevar a cabo una revocación con diferentes ventajas y desventajas cada una, siendo la más sencilla la de generar listas de revocación pública y accesible desde internet. Sin embargo, esta técnica no preserva la privacidad, ya que las credenciales deben presentarse de manera que puedan correlacionarse con la lista de revocación y al hacerlo, las credenciales también pueden correlacionarse con su presentador, lo que anula todas las características de preservación de la privacidad en la tecnología ZKP.

Es por esto que dentro del proyecto Hyperledger Indy la solución que ofrecen para llevar a cabo una revocación es la de generar un archivo de colas asociado con un acumulador y sus factores [53]. Este archivo contiene una serie de factores generados aleatoriamente para un acumulador y a cada credencial potencial o real emitida por un emisor en particular se le asigna un índice de un factor acumulador del archivo de colas.

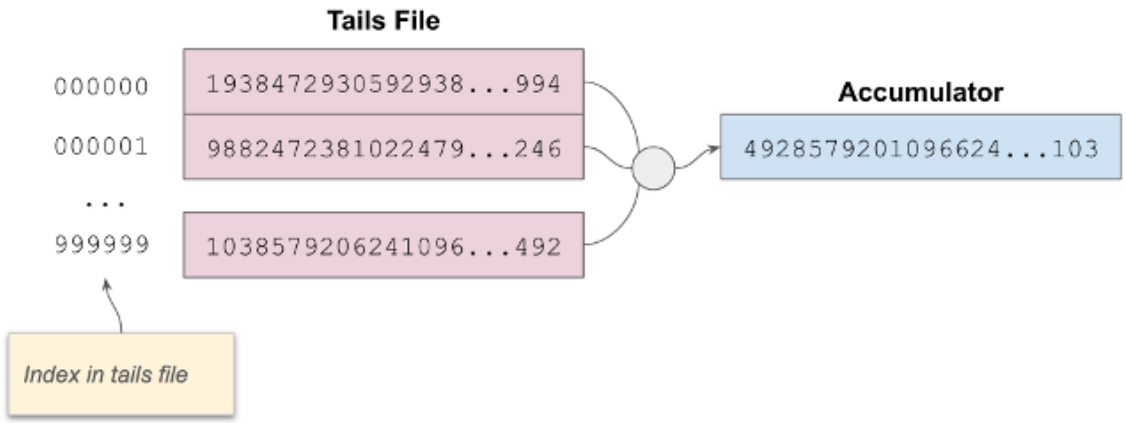

Ilustración 46 - Índice del Archivo de Colas y cálculo del Acumulador

Fuente: Daniel Hardman (2018) [54]

Cada agente emisor debe publicar en la DLT en un Registro de Revocación, en el que se refleja el estado de revocación de todas las credenciales. Este acumulador debe actualizarse periódicamente en la DLT, dando como resultado que los factores enumerados en el archivo de colas para los índices asociados ya no se multiplican en el acumulador [54]., dando como resultado que los factores enumerados en el archivo de colas para los índices asociados ya no se multiplican en el acumulador [54].

Los metadatos del Registro de Revocación publicado deben hacer referencia a una Definición de Credencial en particular y especificar cómo se manejará la revocación. El registro de revocación indica qué acumulador criptográfico utilizar para probar la revocación y proporcioná el URI y el hash del archivo de colas asociado.

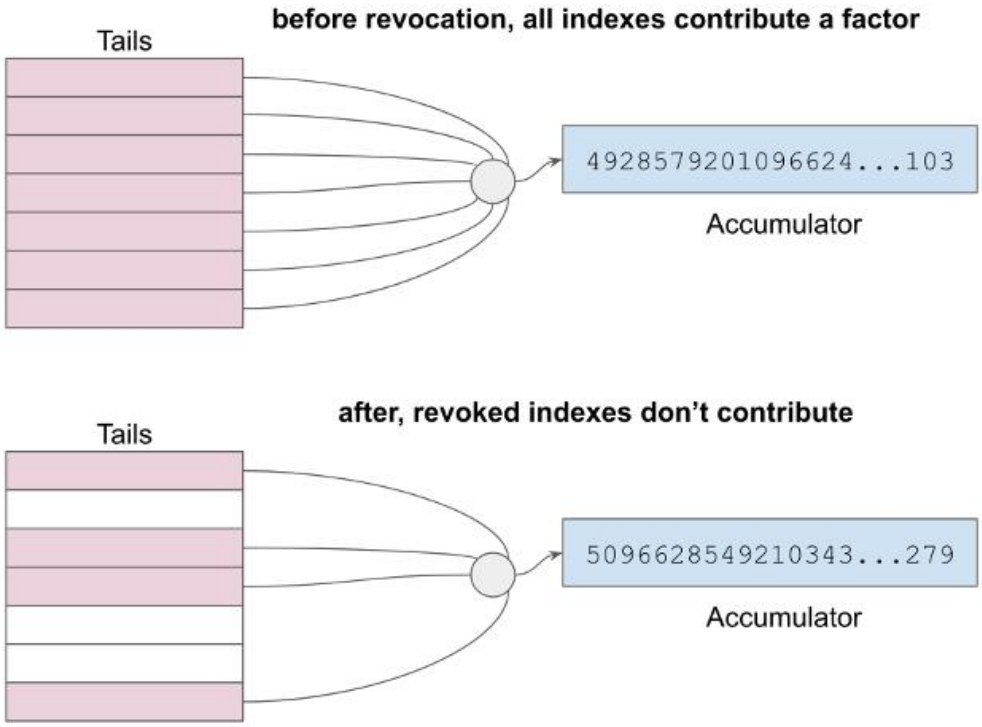

Ilustración 47 - Cambio del valor del acumulador luego de revocar credenciales

Fuente: Daniel Hardman (2018) [54]

La estrategia adoptada en el proyecto Hyperledger Indy no está exenta de problemas y presenta los siguientes inconvenientes:

- Plantea el interrogante del momento en el que debe publicarse y actualizar el acumulador.
- La revocación es reversible, ya que la validación se hace contra un número que técnicamente no impide que el emisor publique el acumulador que desee.
- La revocación añade complejidad a la emisión, prueba y verificación:
    - La URL pública del servidor de colas debe estar disponible en todo momento.

    - Por parte de los agentes emisores que deben mantener un servicio para los acumuladores, el cual si se corrompe o pierde se pierde la capacidad de revocar.
    - Por parte de los verificadores que deben realizar el cálculo de validez de la credenciales y presentaciones.
- Gestionar el tamaño de archivos de colas para que no sea un problema por parte de los agentes emisores.
- Problema de ofrecer un punto de correlación temporal en el archivo de colas.

Escapa el alcance de la prueba de concepto de esta tesis la adopción de un mecanismo de revocación, pero se intentó describir el estado actual y los desafíos que conlleva la solución propuesta por el proyecto Hyperledger Indy.

5. CONCLUSIONES

Durante el desarrollo de esta tesis se estudiaron los distintos modelos de identidad desarrollados hasta el momento y se presentó el concepto de Identidad Auto Soberana, un nuevo paradigma de identidad basado en tecnología descentralizada que otorga al propio usuario la capacidad y responsabilidad de controlar y almacenar sus credenciales identificatorias, y la capacidad de realizar presentaciones verificables con las mismas sin necesidad de develar información innecesaria como sucede con las credenciales físicas.

Se procedió a analizar el estado del arte de distintas soluciones y propuestas de IAS de iniciativa pública y privada, encargadas de promover su desarrollo a lo largo del mundo, tanto de los componentes técnicos tecnológicos como regulaciones y marcos de confianza que den validez a su utilización. En este apartado se describieron distintas iniciativas que actualmente se están desarrollando en todo el mundo y en particular Latinoamérica, que intentan buscar soluciones a distintas problemáticas sociales promoviendo el uso de herramientas basadas en este paradigma de identidad.

Luego se describieron sobre cuáles son los componentes tecnológicos, estándares y protocolos utilizados y en algunos casos desarrollados específicamente para su uso en implementaciones de IAS, como las tecnologías DLT y blockchain que permite realizar transacciones de manera segura, la promoción del uso del estándar de identificadores distribuidos que permiten una identificación global, los estándares de credenciales y presentaciones verificables y los conceptos de billetera digital y agentes. Como se detalló, en su mayoría continúan en proceso de desarrollo y estandarización y en otros casos se están desarrollando activamente nuevas versiones superadoras de las primeras versiones publicadas.

Se realizó un trabajo experimental en el que primero se describieron las herramientas Indy y Aries pertenecientes al proyecto Hyperledger de la fundación Linux, dos proyectos de software libre con el objetivo de ayudar a desplegar un ecosistema de Identidad Auto Soberana. La utilización de la cadena de bloques de test British Columbia VON Network basada en el proyecto Indy. Se describió la billetera digital Lissi ID-Wallet para uso por parte de los usuarios, compatible con las tecnologías

anteriormente descriptas. Estas herramientas se utilizaron para realizar una prueba de concepto dentro del ambiente académico de la Universidad Nacional del Noroeste de la Provincia de Buenos Aires, que constó en el despliegue de un agente emisor de credenciales de parte de la universidad pasado den el proyecto Aries, el desarrollo de una controladora para un fácil manejo, la emisión de credenciales a billeteras virtuales y validación de las mismas contra información almacenada en la cadena de bloques. Durante todos estos pasos se intentó mostrar el grado de madurez de las herramientas utilizadas para su despliegue, las cuales en su mayoría se consideran aún en etapas tempranas al no encontrarse en versiones estables, se detallaron problemas y limitaciones encontradas y posibles cambios a futuros tanto en las herramientas como protocolos utilizados.

6. TRABAJOS A FUTURO

A partir del trabajo realizado en esta tesis las siguientes líneas de investigación se sugieren de interés teniendo en cuenta el auge que está teniendo esta tecnología a nivel global:

- Desarrollar marcos de confianza para su implementación con validez legal según las leyes y normativas vigentes.
- Desarrollar mecanismos de interoperabilidad de DIDs entre distintos DLTs.
- Una solución superadora a los mecanismos actuales de revocación de Credenciales Verificables.
- Comparativa de uso y capacidad de interacción entre distintos protocolos de comunicación como DIDComm y OpenID.
- Analizar las distintas consideraciones de accesibilidad necesarias para que esta tecnología pueda ser de uso y encontrarse al alcance de todos los usuarios.

7. REFERENCIAS

[1] Christopher Allen (2016). The Path to Self-Sovereign Identity. Life With Alacrity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[2] Andrew Tobin y Drummond Reed (2018). The Inevitable Rise of Self-Sovereign Identity. Sovrin Foundation. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

[3] Paul Dunphy y Fabien A. P. Petitcolas (2018). A First Look at Identity Management Schemes on the Blockchain. VASCO Data Security. https://arxiv.org/ftp/arxiv/papers/1801/1801.03294.pdf

[4] Alex Preukschat y Drummond Reed (Junio 2021), «Self-Sovereign Identity: Decentralized digital identity and verifiable credentials», MANNING.

[5] Microsoft (2023) Microsoft Entra. Microsoft. https://www.microsoft.com/entra

[6] Hyperledger (2022). Hyperledger: Building Better Together. The Linux Fundation. https://www.hyperledger.org/

[7] Parlamento Europeo (2014). Reglamento (UE) n ° 910/2014. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32014R0910

[8] Parlamento Europeo (2016). RGPD. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

[9] EU Blockchain (2018). EU Blockchain. Comisión Europea. https://www.eublockchainforum.eu/

[10] Parlamento Europeo (2019). European Self Sovereign Identity Framework Laboratory. CORDIS. https://cordis.europa.eu/project/id/871932/es

[11] AlastriaID (2020). ALASTRIA IDENTITY 1.0. Alastria. https://github.com/alastria/alastria-identity

[12] Marcos Allende Lopez (2020). El futuro de la identidad digital: auto-gestión, billeteras digitales y blockchain. BID.

[13] LACNet (2021). LacChain. BID Lab. https://lacnet.lacchain.net/lacnet-soluciones/

[14] Sovrin Foundation (2024). Global public registry for DIDs and Verifiable Credentials. Sovrin. https://sovrin.org/

[15] Dan Gisolfi, Milan Patel y Rachel Radulovich (2018). Decentralized Identity Introduction. IBM. https://www.ibm.com/downloads/cas/OPEQYEL7

[16] Kaliya Young (2020). The Domains of Identity - A Framework for Understanding Identity Systems in Contemporary Society. Anthem Impact.

[17] Joe Andrieu (2019). Rebooting Web of Trust. Web of Trust. https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/functional-identity-primer.md

[18] Kim Cameron (2005). The Laws if Identity. Kim Cameron's Identity Weblog. https://www.identityblog.com/?p=352

[19] Nishant Bhajaria (Diciembre 2021). Exploring Security, Privacy, and Trust. Manning.

[20] Timothy Ruff (2018). The Three Models of Digital Identity Relationships. Evernym.

[21] OpenID (2023). OpenID Foundation. https://openid.net/

[22] OAuth 2.0 (2023). OAuth. https://oauth.net/

[23] OASIS (2023). SAML V2.0 Standard. https://wiki.oasis-open.org/security

[24] Heather Vescent y Kaliya Young (2018). A Comprehensive Guide to Self Sovereign Identity. Purple Tornado.

[25] Government Office for Science (2016). Distributed Ledger Technology: beyond block chain. Reino Unido. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[26] Julie Maupin, Jonas Kahlert, Franz v. Weizsäcker... (2019). Blockchain: A World Without Middlemen?. GIZ.

[27] NIST (2021). Blockchain. https://www.nist.gov/blockchain

[28] World Wide Web Consortium (2022). Decentralized Identifiers (DIDs) v1.0 becomes a W3C Recommendation. https://www.w3.org/press-releases/2022/did-rec/

[29] M. Sporny, A. Guy, M. Sabadello, D. Reed. (Julio 2022). Decentralized Identifiers (DIDs) v1.0 - Core architecture, data model, and representations. W3C. https://www.w3.org/TR/2022/REC-did-core-20220719

[30] D. Crocker, P. Overell (2008). Augmented BNF for Syntax Specifications: ABNF. RFC INTERNET STANDARD. https://www.rfc-editor.org/rfc/rfc5234

[31] O. Steele, M. Sporny (Mayo 2024). The interoperability registry for Decentralized Identifiers. W3C Group Note. https://www.w3.org/TR/did-spec-registries/

[32] Sovrin (Abril 2024). Sovrin DID Method Specification. W3C. https://sovrin-foundation.github.io/sovrin/spec/did-method-spec-template.html

[33] Markus Sabadello, Kyle Den Hartog, Christian Lundkvist... (2018). Introduction to DID Auth. Paper público. https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/draft-documents/did_auth_draft.md

[34] M. Sporny, D. Longley, D. Chadwick. (Marzo 2022). Verifiable Credentials Data Model v1.1. W3C Recommendation. https://www.w3.org/TR/vc-data-model/

[35] L. Lesavre, P. Varin, P. Mell, M. Davidson, J. Shook. (Enero 2020). A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. NIST cybersecurity white paper. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01142020.pdf

[36] Anna Johnson (Agosto 2020). What Are SSI Digital Wallets?. Trinsic Id. https://trinsic.id/what-are-ssi-digital-wallets/

[37] DIDComm Working Group (2023). DIDComm Messaging v2.x Editor's Draft. Decentralized Identity Foundation. https://identity.foundation/didcomm-messaging/spec/

[38] John Verrico (Julio 20217). DHS S&T Awards $749K to Evernym for Decentralized Key Management Research and Development. DHS S&T Press Office. https://www.dhs.gov/science-and-technology/news/2017/07/20/news-release-dhs-st-awards-749k-evernym-decentralized-key

[39] Hyperledger (2018). Decentralized Key Management. The Linux Foundation. https://hyperledger-indy.readthedocs.io/projects/sdk/en/latest/docs/design/005-dkms/README.html

[40] Smith Samuel (2021). Key event receipt infrastructure (KERI) design. Paper público. https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

[41] Hyperledger Indy (2023). Hyperledger Indy. https://hyperledger-indy.readthedocs.io/en/latest/index.html

[42] Government of British Columbia (2023). Digital Credential Services. https://digital.gov.bc.ca/digital-trust/

[43] Government of British Columbia (2023). VON Network. https://github.com/bcgov/von-network

[44] Docker Inc. (2023). Manuals. https://docs.docker.com/manuals/

[45] Hyperledger Indy (2022). Indy Node. https://github.com/hyperledger/indy-node/tree/release-1.12.6

[46] S. Curran, P. Bastian, D. Hardman… (2024). Indy DID Method. Hyperledger Indy. https://hyperledger.github.io/indy-did-method/

[47] Hyperledger Aries (2023). Hyperledger Aries. https://www.hyperledger.org/projects/aries

[48] Hyperledger Aries (2024). Aries Cloud Agent Python. https://aca-py.org/v0.12.1/

[49] Hyperledger Aries (2024). ACA-Py Administration API. https://aca-py.org/v0.12.1/features/AdminAPI/

[50] Hyperledger Aries (2024). Aries AIP and RFCs Supported in Aries Cloud Agent Python. https://aca-py.org/v0.12.1/features/SupportedRFCs/

[51] Lissi GmbH (2023). Lissi ID-Wallet . https://www.lissi.id/for-users

[52] European Digital Identity (Diciembre 2023). Lissi ID-Wallet: Towards eIDAS2 and EUDI-Wallet compatibility. Medium. https://lissi-id.medium.com/lissi-id-wallet-towards-eidas2-and-eudi-wallet-compatibility-0eec47d0b468

[53] J. Camenisch, M. Kohlweiss, C. Soriente (2008). An Accumulator Based on Bilinear Maps and Efficient Revocation for Anonymous Credentials. Cryptology ePrint Archive. https://eprint.iacr.org/2008/539.pdf

[54] Daniel Hardman (Febrero 2018). 0011: Credential Revocation. Hyperledger Indy Project Enhancements. https://github.com/hyperledger/indy-hipe/tree/master/text/0011-cred-revocation