tesis doctoral

FRANCISCO JOSÉ DE CALDAS

FACULTAD DE INGENIERÍA

MODELO PARA LA GESTIÓN DE UNA IDENTIDAD DIGITAL DESCENTRALIZADA Y AUTOGOBERNADA BAJO TECNOLOGÍA DE REGISTRO DISTRIBUIDO

M.eng. Roberto Albeiro Pava Díaz

Énfasis en Ciencia de la información y el conocimiento

Doctorado en Ingeniería

http://doctoradoingenieria.udistrital.edu.co

Modelo para la gestión de una identidad digital descentralizada y autogobernada bajo tecnología de registro distribuido

M.eng. Roberto Albeiro Pava Díaz

Universidad Distrital "Francisco José de Caldas"

Facultad de Ingeniería

Doctorado en Ingeniería

Bogotá D.C - Colombia

20 de diciembre de 2024

Modelo para la gestión de una identidad digital descentralizada y autogobernada bajo tecnología de registro distribuido

M.eng. Roberto Albeiro Pava Díaz

Tesis presentada como requisito parcial para optar al título de:

Doctor en Ingeniería

Director:
Ing. Danilo Alfonso López Sarmiento
Doctor en Ingeniería

Co-Director:
Ing. Luis Fernando Niño Vásquez
Ph. D. in Computer Science

Grupo de investigación
LIDER - Laboratorio de Investigación y Desarrollo en Electrónica y Redes
LISI - Laboratorio de Investigación en Sistemas Inteligentes

Universidad Distrital "Francisco José de Caldas"

Facultad de Ingeniería

Doctorado en Ingeniería

Énfasis en Ciencia de la información y el conocimiento

20 de diciembre de 2024

© Derechos de autor 2024 de M.eng. Roberto Albeiro Pava Díaz.

Todos los derechos reservados.

Resumen

La identidad digital es concebida como un derecho humano fundamental, por lo tanto debe facilitarle a un individuo el acceso oportuno a bienes y servicios, el control de su privacidad y la mitigación de riesgos de suplantación, además, de ser fundamental para el desarrollo económico, político y social de un país, y de sus ciudadanos. Toda persona debería estar en capacidad de probar, administrar y preservar su identidad digital, sin barreras de acceso y con la autonomía para gestionar sus atributos de identidad personal. Por otro lado, la Internet ha evolucionado sin una capa de identidad digital por lo que cada servicio web o aplicación ha tenido que implementar un esquema para identificación, generalmente basado en credenciales de acceso tipo usuario - contraseña, lo que obliga a los usuarios a recordar y administrar múltiples contraseñas y utilizar diferentes métodos de validación. Bajo este contexto la gestión de la identidad digital es uno de los grandes retos asociados a infraestructuras digitales a gran escala en la sociedad actual. Es un problema complejo, puesto que actualmente la información de los individuos esta almacenada de forma dispersa, con almacenamiento y custodia por parte de terceros y atributos de autenticación asociados a datos personales o biométricos públicos.

La identidad digital autogobernada (SSI) soportada en tecnología de registro distribuido provee la capa de identidad digital necesaria en la web actual y posibilita a una entidad crear, poseer y controlar una identidad verificable y persistente en un ecosistema de datos centrado en el usuario.

Este proyecto de investigación propone un modelo SSI denominado *Aletheia*, que proporciona una representación verificable de la identidad digital y resistente a manipulación gracias a la disponibilidad de un registro distribuido. Este modelo preserva la privacidad del usuario y el control de los atributos de identificación personal gracias a la implementación de identificadores descentralizados y credenciales verificables, junto con la integración de un sistema de almacenamiento descentralizado con un método adicional de cifrado de documentos. *Aletheia* fue comparado con un conjunto de *frameworks* SSI analizando su adherencia a los principios de identidad digital, y por su naturaleza presentó un cumplimiento notable en persistencia, protección, acceso, portabilidad e interoperabilidad. Además, se implementó una prueba de concepto que permite la creación de identidades descentralizadas con un almacenamiento seguro y protegido de credenciales verificables, bajo el control del titular de los derechos de identidad. Esta prueba permite al usuario gestionar sus credenciales y realizar presentaciones verificables, en un entorno que la preservación la privacidad. La prueba de concepto facilita el análisis completo del flujo de información en el modelo, desde la creación de la billetera digital, la solicitud y emisión de una credencial, su almacenamiento correspondiente, hasta la presentación de la credencial a un verificador, culminando con la verificación criptográfica por parte de este.

Palabras clave

Blockchain, Identidad digital autogobernada, SSI, Identificadores descentralizados, DID, Credenciales verificables, VC, Triángulo de la confianza.

Abstract

Digital identity is conceived as a fundamental human right; therefore, it should facilitate an individual's timely access to goods and services, control over their privacy, and mitigation of impersonation risks. Moreover, it is crucial for the economic, political, and social development of a country and its citizens. Every person should be capable of proving, managing, and preserving their digital identity without access barriers and with the autonomy to manage their personal identity attributes.

On the other hand, the Internet has evolved without a digital identity layer, compelling each web service or application to implement an identification scheme, generally based on username-password access credentials. This obliges users to remember and manage multiple passwords and utilize various validation methods. Within this context, digital identity management is one of the significant challenges associated with large-scale digital infrastructures in contemporary society. It is a complex problem, as individuals' information is currently stored in a dispersed manner, with storage and custody by third parties and authentication attributes associated with public personal or biometric data.

Self-Sovereign Identity (SSI) supported by distributed ledger technology provides the necessary digital identity layer in the current web and enables an entity to create, own, and control a verifiable and persistent identity in a user-centric data ecosystem.

This research project proposes an SSI model called Aletheia, which provides a verifiable representation of digital identity resistant to manipulation due to the availability of a distributed ledger. This model preserves user privacy and control of personal identification attributes through the implementation of decentralized identifiers and verifiable credentials, along with the integration of a decentralized storage system with an additional document encryption method. Aletheia was compared with a set of SSI frameworks by analyzing its adherence to digital identity principles, and due to its nature, it demonstrated notable compliance in persistence, protection, access, portability, and interoperability. Additionally, a proof of concept was implemented to enable the creation of decentralized identities with secure and protected storage of verifiable credentials, fully under the control of the identity rights holder. This proof of concept allows users to manage their credentials and perform verifiable presentations within an environment that ensures privacy preservation. It facilitates a comprehensive analysis of the information flow within the model, encompassing the entire process from the creation of the digital wallet, the request and issuance of a credential, and its subsequent storage, to the presentation of the credential to a verifier, culminating in cryptographic verification by this.

Keywords

Blockchain, Decentralized identifiers, DID, Self-sovereign digital identity, SSI, Verifiable credentials, VC, Trust triangle.

Agradecimientos

En primer lugar agradezco al Dios de la vida por acompañarme en este camino y sostenerme en todas las dificultades vividas.

Seguidamente, es menester expresar mi más profundo reconocimiento a todos los directores que me han guiado y aportado a lo largo de este interesante pero a su vez intrincado camino académico. En primer lugar, quiero destacar la invaluable contribución del profesor Luis Fernando Niño Vásquez[1] Ph.D de la Universidad Nacional de Colombia, cuyo acompañamiento constante ha sido fundamental para el desarrollo de esta disertación doctoral, y en toda mi formación profesional; su orientación y sabiduría han sido pilares esenciales.

Asimismo, extiendo mi sincera gratitud a los profesores de la universidad Distrital "Francisco José de Caldas". Agradezco al Dr. Sandro Javier Bolaños Castro[2], por su acompañamiento en el proceso de admisión y guía inicial durante el período 2018-I. Con profundo respeto, rindo homenaje a la memoria del Dr. José Nelson Perez Castillo[3] (Q.E.P.D.), cuya tutoría de 2018-II a 2020-II dejó una huella indeleble en mi formación. Al Dr. Roberto Ferro Escobar[4] por su dedicación y colaboración durante el período 2021-II. Un reconocimiento especial al Dr. Danilo Alfonso López Sarmiento[5], quien me acompañó en dos etapas cruciales: de 2022-I a 2022-II, y posteriormente desde 2024-I hasta el presente. Igualmente, al Dr. César Augusto Hernández Suárez[6] por su instrucción durante los períodos académicos 2023-I y 2023-II.

De igual manera, al Dr. Rafael Vicente Páez Méndez[7] de la Pontificia Universidad Javeriana, cuyo asesoría durante mi pasantia de investigación doctoral enriqueció significativamente mi trabajo.

Cada uno de estos maestros ha dejado una huella imborrable en mi formación académica y en el desarrollo de esta investigación, contribuyendo de manera significativa a mi crecimiento profesional y personal.

[1] http://www.hermes.unal.edu.co/pages/Docentes/Docente.jsf?u=lfninov
[2] https://doctoradoingenieria.udistrital.edu.co/bolanos-castro-sandro-javier/
[3] https://facingenieria.udistrital.edu.co/maestria-ciencias-informacion/index.php/docentes/jose-nelson-perez-qepd
[4] https://doctoradoingenieria.udistrital.edu.co/ferro-escobar-roberto/
[5] https://doctoradoingenieria.udistrital.edu.co/lopez-sarmiento-danilo-alfonso/
[6] https://doctoradoingenieria.udistrital.edu.co/hernandez-suarez-cesar-augusto/
[7] https://orcid.org/0000-0003-1721-0883

Dedicatoria

A mis padres.

Tabla de contenido

Resumen v

Abstract v

Agradecimientos vi

Dedicatoria vii

Lista de tablas xii

Lista de figuras xiv

1 Identidad digital autogobernada 1

1.1 Introducción . . . 1

1.2 Contexto del problema de investigación . . . 3

1.2.1 Objetivos . . . 7

1.2.1.1 Objetivo General . . . 7

1.2.1.2 Objetivos Específicos . . . 7

1.2.2 Hipótesis . . . 7

2 Caracterización de la identidad digital autogobernada 8

2.1 Metodología para revisión de la literatura . . . 8

2.1.1 Preguntas de investigación . . . 8

2.1.2 Identificación . . . 9

2.1.3 Filtro . . . 10

2.1.4 Selección . . . 11

2.1.5 Inclusión . . . 13

2.2 Análisis crítico de la literatura . . . 15

2.2.1 Atributos esenciales de una identidad autogobernada . . . 15

2.2.1.1 Conceptos fundamentales en identidad digital autogobernada . . . 16

2.2.1.2 Principios de diseño para la identidad autogobernada 17
2.2.1.3 Patrones de diseño de una identidad autogobernada basados en *blockchain* 18
2.2.1.4 Identificadores Descentralizados 19
2.2.1.5 Autenticación 23
2.2.1.6 Credenciales Verificables 24
2.2.1.7 Almacenamiento 26
2.2.2 Arquitecturas propuestas para *SSI* 26
2.2.2.1 Principios y componentes básicos a nivel de arquitectura 27
2.2.2.2 Casos de uso que implementan gestión de identidad digital basada en *blockchain* 28

3 Meta-sistemas para el despliegue de una identidad digital autogobernada 36
3.1 *Sovrin Network* 36
3.2 *uPort* 38
3.3 *Jolocom* 39
3.4 *ShoCard* 40
3.5 *Litentry* 41
3.6 *Civic* 41
3.7 *Kilt* 42
3.8 *Identity Overlay Network* 43
3.9 *Idena* 43
3.10 Nivel de cumplimiento de los principios de *SSI* 44
3.10.1 Principio de Existencia 45
3.10.2 Principio de Control 46
3.10.3 Principio de Consentimiento 47
3.10.4 Principio de Minimización 48
3.10.5 Principio de Persistencia 49
3.10.6 Principio de Protección 50
3.10.7 Principio de Acceso 52
3.10.8 Principio de Transparencia 53
3.10.9 Principio de Portabilidad 54
3.10.10 Principio de Interoperabilidad 55
3.10.11 Conclusiones de la evaluación del nivel de cumplimiento de los principios SSI 57

4 Aletheia: Un modelo de identidad digital autogobernada 60
4.1 Marco de referencia 61

4.1.1 Modelo de confianza para la Internet . . . 61
4.2 Requerimientos de Aletheia . . . 63
4.2.1 Descripción de entidades . . . 64
4.2.2 Aletheia *Wallet* . . . 65
4.2.3 Aletheia-Dapp . . . 65
4.2.4 Requerimientos por capa *ToIP* . . . 65
4.2.4.1 Requerimientos en la capa 1: utilidad pública . . . 65
4.2.4.2 Requerimientos en la capa 2: Infraestructura técnica de confianza . 67
4.2.4.3 Requerimientos en la capa 3: Diamante de la confianza . . . 67
4.2.4.4 Requerimientos en la capa 4: Nivel de aplicación . . . 68
4.2.5 Requerimientos tecnológicos . . . 69
4.3 Aletheia: Modelo de identidad digital autogobernada . . . 70
4.3.1 Descripción general . . . 70
4.3.2 Descripción de la arquitectura . . . 70
4.3.3 Diagramas de flujo para credenciales verificables . . . 71

5 Escenario de validación de Aletheia 79
5.1 Marco de gobernanza . . . 79
5.1.1 Capa 1: Utilidad pública . . . 79
5.1.2 Capa 2: Infraestructura técnica de confianza . . . 80
5.1.3 Capa 3: Diamante de la confianza . . . 81
5.1.4 Capa 4: Nivel de aplicación . . . 83
5.2 Adherencia a los principios de identidad digital autogobernada . . . 84
5.3 Análisis del escenario de validación . . . 85
5.3.1 Aspectos generales de la implementación . . . 86
5.3.2 Contexto del escenario de validación . . . 87
5.3.2.1 Generación de una credencial verificable . . . 89
5.3.2.2 Realización de una presentación verificable . . . 98
5.4 Verificación de la presentación . . . 104

Conclusiones 106

Trabajo futuro 108

Principales contribuciones 109
5.5 Socialización de resultados . . . 111
5.5.1 Ponencias en congresos internacionales . . . 111

5.5.2 Artículos realizados 112
5.5.3 Estancia de pasantia 112
5.5.3.1 Proyecto de investigación institucionalizado 112
5.5.4 Trabajos de grado dirigidos 112
5.5.5 Conferencista/Panelista invitado 113

Referencias **114**

Lista de tablas

2.1 Filtro de inclusión de publicaciones por criterios bibliométricos 11
2.2 Criterios de exclusión para la selección de artículos. 11
2.3 Criterios de inclusión de publicaciones basados en el contenido. 12
2.4 Información general de los *frameworks* para SSI. 12
2.5 Descripción del conjunto de datos analizado. 14
2.6 Definición de los conceptos clave en una *SSI*. 17
2.7 Objetivos de diseño para *DID*. 20
2.8 Componentes de arquitectura aplicados en los casos de uso. 35

3.1 Nivel de cumplimiento del principio de existencia. 45
3.2 Nivel de cumplimiento del principio de control. 47
3.3 Nivel de cumplimiento del principio de consentimiento. 48
3.4 Nivel de cumplimiento del principio de minimización. 49
3.5 Nivel de cumplimiento del principio de persistencia. 50
3.6 Nivel de cumplimiento del principio de protección. 51
3.7 Nivel de cumplimiento del principio de acceso. 52
3.8 Nivel de cumplimiento del principio de transparencia. 54
3.9 Nivel de cumplimiento del principio de portabilidad. 55
3.10 Nivel de cumplimiento del principio de interoperabilidad. 56
3.11 Consolidado del nivel de cumplimiento de los *frameworks* analizados. 58

4.1 Requerimientos para la implementación de *DID*. 66
4.2 Requerimientos para el registro y autenticación de una entidad. 66
4.3 Requerimientos en la capa 2 para *ToIP*. 67
4.4 Requerimientos en la capa 3 para *ToIP*. 68
4.5 Requerimientos en la capa 4 para *ToIP*. 69
4.6 Requerimientos tecnológicos. 69

5.1 Nivel de cumplimiento de Aletheia 85

5.2 Configuración de *ethereum* simulada con *Ganache*. 88
5.3 Entidades creadas en Aletheia *Wallet* 88
5.4 Datos incluidos en la solicitud de emisión de VC. 92
5.5 Datos asociados a la presentación verificable realizada por estudiante.1-Dapp 103
5.6 Trabajos de grado dirigidos a nivel de Maestría 113
5.7 Trabajos de grado dirigidos a nivel de Pregrado 113

Lista de figuras

1.1 Mapa conceptual de la identidad digital. 3
1.2 Esquema para la administración de una SSI. 4

2.1 Diagrama del proceso de revisión de literatura. 9
2.2 Estructura de la cadena de búsqueda. 10
2.3 Relación entre palabras claves propuestas por los autores 14
2.4 Arquitectura y componentes de un *DID*. 21
2.5 Autenticación y confidencialidad mediante criptografía asimétrica 23
2.6 Actores y componentes para la implementación de *VC*. 25
2.7 Arquitectura de alto nivel en 7 capas para *SSI* 27

3.1 Arquitectura de los *frameworks* para SSI. 37
3.2 Nivel de cumplimiento de los principios SSI 57

4.1 Aletheia: diosa de la verdad, la sinceridad y la revelación 60
4.2 Arquitectura en capas propuesta por *ToIP*. 62
4.3 Vista de alto nivel de Aletheia. 64
4.4 Requerimientos para la creación de un *DID*. 65
4.5 Diagrama de componentes para Aletheia-Dapp. 71
4.6 Generación de una credencial verificable 72
4.7 Visualización de una credencial verificable. 73
4.8 Almacenamiento de una VC en Aletheia *wallet*. 74
4.9 Generación de una presentación verificable. 75
4.10 Verificación de una presentación verificable 77

5.1 Flujo de información para crear y acceder a la billetera 81
5.2 Flujo de información para crear e iniciar sesión en Aletheia-Dapp 82
5.3 Cumplimiento de los principios SSI en Aletheia 86
5.4 Inicialización Aletheia *Wallet* para estudiante.1 89

5.5 Transacciones asociadas a la creación de usuarios en Aletheia-Dapp 90
5.6 Solicitud de emisión de una credencial verificable. 91
5.7 Credencial Verificada emitida para estudiante.1-Dapp. 95
5.8 Visualización de la credencial verificable emitida. 96
5.9 Mediador para la comunicación entre Aletheia-Dapp y Aletheia *Wallet*. 97
5.10 Interface de la *Wallet* para el almacenamiento de una VC emitida. 97
5.11 Vista actualizada de Aletheia *Wallet* para estudiante.1-Dapp. 98
5.12 *Dashboard* para el estudiante.1-Dapp 99
5.13 Información requerida para la elaboración de una PV. 100
5.14 Inicio de la comunicación con la *Wallet* 101
5.15 Autenticación en Aletheia *Wallet* 101
5.16 Listado de VC propiedad del estudiante.1-Dapp. 102
5.17 Estructura final para la generación de la PV. 102
5.18 Notarización de una nueva PV. 103
5.19 *Dashboard* en Aletheia-Dapp para unidadInvestigacion.1-Dapp. 104
5.20 Listado PV remitadas a unidadInvestigacion.1-Dapp 104
5.21 Visualización de la PV y su comprobación. 105
5.22 Aprobación de la PV por parte de unidadInvestigacion.1-Dapp. 106

Capítulo 1

Identidad digital autogobernada

Este capítulo aborda el problema de la identidad digital autogobernada, también conocida como *Self-Sovereign Identity* (SSI). Se presenta un análisis del contexto de la gestión de identidad digital desde una perspectiva descentralizada. Se enfatizan los desafíos y riesgos inherentes a la administración de la identidad digital, como son la fragmentación de la información y la pérdida de control sobre los atributos personales por parte del usuario. Asimismo, se examinan los beneficios de un modelo de identidad digital sustentado en tecnología de registro distribuido, que ofrece beneficios en privacidad, seguridad y control sobre los datos personales. Por último, se presentan los objetivos e hipótesis establecidos para esta investigación.

1.1 Introducción

La definición de identidad se ajusta según el escenario de uso, por ejemplo, en psicología se abordan rasgos de la personalidad, en sociología se incluyen factores culturales y religiosos, y desde un enfoque legal la identidad se centra en diferenciar a las personas, tanto naturales como jurídicas. La identidad digital es la representación de una entidad que le permite identificarse en las transacciones e interacciones digitales [1], [2], contiene los atributos que la describen, con una orientación polifacética para permitir la existencia de los múltiples perfiles que desempeña la entidad en los diferentes dominios de aplicación. Cada uno de estos perfiles deberá tener asociado un identificador para establecer un vínculo con la entidad en el mundo real. Los identificadores presentan dos propiedades, (1) unicidad: un identificador es asignado de forma exclusiva a una entidad, sin posibilidad de reasignación; y (2) singularidad: un identificador es único en un dominio de aplicación [3].

La gestión de identidad digital es uno de los retos más importantes asociados a infraestructuras digitales a gran escala que afronta nuestra sociedad [4]. El riesgo por suplantación y falsificación genera afectaciones económicas y de seguridad tanto en el ámbito individual como corporativo o incluso nacional. Generalmente, el gobierno es responsable de administrar la identidad física de sus ciudadanos mediante la expedición de documentos oficiales de identidad, proceso que se actualiza periódicamente para mejorar la seguridad, por ejemplo en el año 2005 los *Estados Unidos de América* modificaron los estándares mínimos de seguridad para la emisión de documentos de identidad, como licencias de conducción con la expedición de la norma federal *REAL ID Act* [5], con vigencia a partir del 1 de octubre de 2021. Esta norma surgió como recomendación de seguridad nacional emitida por la comisión 9/11 con el objetivo de reducir los riesgos de identificación de personas al momento de acceder a edificios gubernamentales y aeropuertos nacionales.

Por otra parte, la administración de la identidad digital y los datos asociados debe ser delegada

por el usuario a la institución que ofrece un servicio, se basa principalmente en la utilización de credenciales de acceso como usuario y contraseña, con la posibilidad de asociar datos personales como números telefónicos o dirección de correo electrónico. Esta delegación conlleva a una identidad digital fragmentada, con procesos no fiables o inexistentes de validación de identidad, lo que representa uno de los problemas más difíciles y vigentes que enfrenta la *Internet* desde sus inicios. En [6] se planteó que la fragmentación y dispersión de los atributos de identidad personales afecta la privacidad, puesto que los usuarios no tienen control sobre su información una vez es cedida en custodia, suscitando riesgos de divulgación de información por desanonimización en procesos de *big data* sobre registros alojados en diferentes fuentes, fallas de seguridad en la protección de los datos o comercialización de los mismos [2].

La identidad es fundamental para el desarrollo económico, político y social de un país, y de sus individuos. Se estima que más de 1 billón de personas no la tienen, y aquellos que disponen de identidad digital no poseen el control de sus atributos enfrentando limitaciones de privacidad, portabilidad y persistencia [7]. En esta línea se destacan los esfuerzos realizados por la alianza para la identidad digital *-ID2020-*, quienes han elaborado un manifiesto para la identidad digital donde la conciben como un derecho humano universal que debe tener todo individuo para probar su identidad, tanto de manera física como digital, que le permita acceder de forma confiable y oportuna a servicios públicos en su carácter de ciudadano del mundo, sin obstáculos asociados a procesos de migración forzada o exclusión poblacional [8]. Además, la identidad digital ha evolucionado y prevalecido en entornos centralizados, con terceros que se presumen confiables para llevar a cabo el proceso de verificación de identidad y validación de credenciales, basados en los datos que poseen de los individuos. Este enfoque centralizado ha generado silos de información que provocan la fragmentación de la identidad, agudizada por la naturaleza polifacética de la misma, donde un individuo se identifica con un subconjunto de atributos acorde con un contexto particular, por ejemplo, en una red social se requieren atributos de identidad diferentes que en una plataforma financiera, los cuales podrían no estar asociados o confrontados con una identidad física real, favoreciendo la explotación de vulnerabilidades por suplantación, fraudes y acceso ilegal por parte de piratas informáticos [9].

Por último, en la Figura 1.1 ilustra los diversos aspectos relacionados con la identidad digital, organizados en cuatro categorías principales: Beneficios, Factores Tecnológicos, Propiedades, y Derechos Humanos [2]. Presenta una visión general de la identidad digital enfocada en cuatro características: (1) la identidad como derecho humano universal que faculta al individuo para demostrar la tenencia de su identidad digital que lo habilita para acceder a servicios públicos, sociales y financieros; en un esquema de administración autogobernado; (2) La identidad debe ser universal e interoperable, sin límites geográficos, que permita transacciones seguras en entornos confiables, con persistencia garantizada, inclusive ante desastres políticos o naturales y que preserve la privacidad; (3) El actual desarrollo tecnológico impulsa la creación de una identidad digital centrada en el usuario, cuyo despliegue se realice en ambientes descentralizados haciendo uso de credenciales verificables automáticamente y estándares de interoperabilidad, mitigando los riesgos por ataques informáticos; y (4) la importancia de la identidad digital se reflejará en beneficios hacia la sociedad como el fortalecimiento en la gestión de servicios públicos, por ejemplo, en el diseño de políticas para salud pública, uso eficiente de los recursos para la educación, vigilancia y seguridad nacional, privacidad y control en el uso de datos personales [7]. Este mapa conceptual subraya la importancia de la identidad digital y su impacto en la sociedad moderna, destacando cómo su correcta implementación traerá beneficios y fortalecerá el ejercicio de los derechos humanos fundamentales.

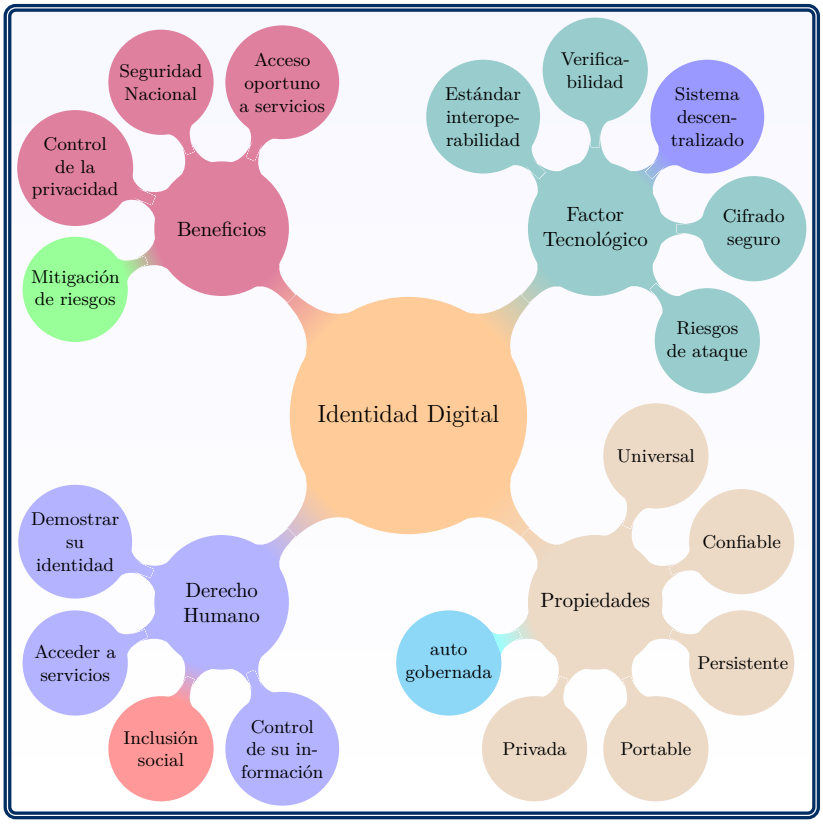


FIGURA 1.1: Mapa conceptual de la identidad digital: desafíos, beneficios, retos y propiedades. Fuente: Elaboración del autor.

1.2 Contexto del problema de investigación

La Internet ha evolucionado sin una capa de identidad digital por lo que cada servicio web o aplicación ha tenido que implementar un esquema para identificación y autenticación, generalmente basado en credenciales de acceso tipo usuario - contraseña, lo que obliga a los usuarios a recordar o administrar múltiples contraseñas y utilizar diferentes métodos de validación, generando riesgos de suplantación, privacidad y control [10]. Es por esto, que la identidad digital constituye uno de los desafíos actuales en investigación, orientado a afrontar los problemas de seguridad presentes en los sistemas de administración de identidad -*IdM*- centralizados o federados [11], [12], [13], [14], enfoque que ha generado una identidad fragmentada, con pérdida del control por parte de los individuos, y posibilidades de menoscabo a la privacidad por reidentificación o desanonimización de la información, al realizar análisis de datos entre múltiples plataformas [6], [15].

En la Figura 1.2 se presenta un esquema general para la identidad digital autogobernada [2]. La gestión de identidad es un problema complejo, puesto que actualmente la información de los individuos está almacenada de forma dispersa, con dificultades y limitaciones para una correlación entre las identidades digitales y la física, con almacenamiento y custodia por parte de terceros, atributos de autenticación asociados a datos personales y biométricos públicos, que generan riesgos de fraude y suplantación [11], interoperabilidad limitada entre las plataformas que restringe o inhabilita el uso, intercambio o validación de atributos entre diferentes dominios. Además, es reciente la concepción de identidad como un derecho humano fundamental y universal [16], que debe permitir la inclusión de los individuos sin limitar su acceso a un mercado de bienes y servicios en un mundo globalizado [3], [17]. La persona debe tener la soberanía sobre sus atributos de identidad, los cuales se acumulan

y modifican en el tiempo, y se agrupan para generar sub-identidades en múltiples contextos, cada una de ellas con un identificador único pero derivadas o relacionadas con un identificador principal [18]. Por otra parte, la tecnología de registro distribuido -*DLT*- se perfila como el soporte tecnológico para el despliegue de una identidad digital autogobernada, posibilitando la creación de una infraestructura de servicios de identidad que soporte la creación de identificadores únicos descentralizados -*DID*-, generación y validación de credenciales verificables digitalmente, asignación y revocación de permisos y consentimientos de consulta sobre los atributos y la implementación de una ley computable que automatice la aplicación de restricciones, derechos y monetización de la identidad digital [19].

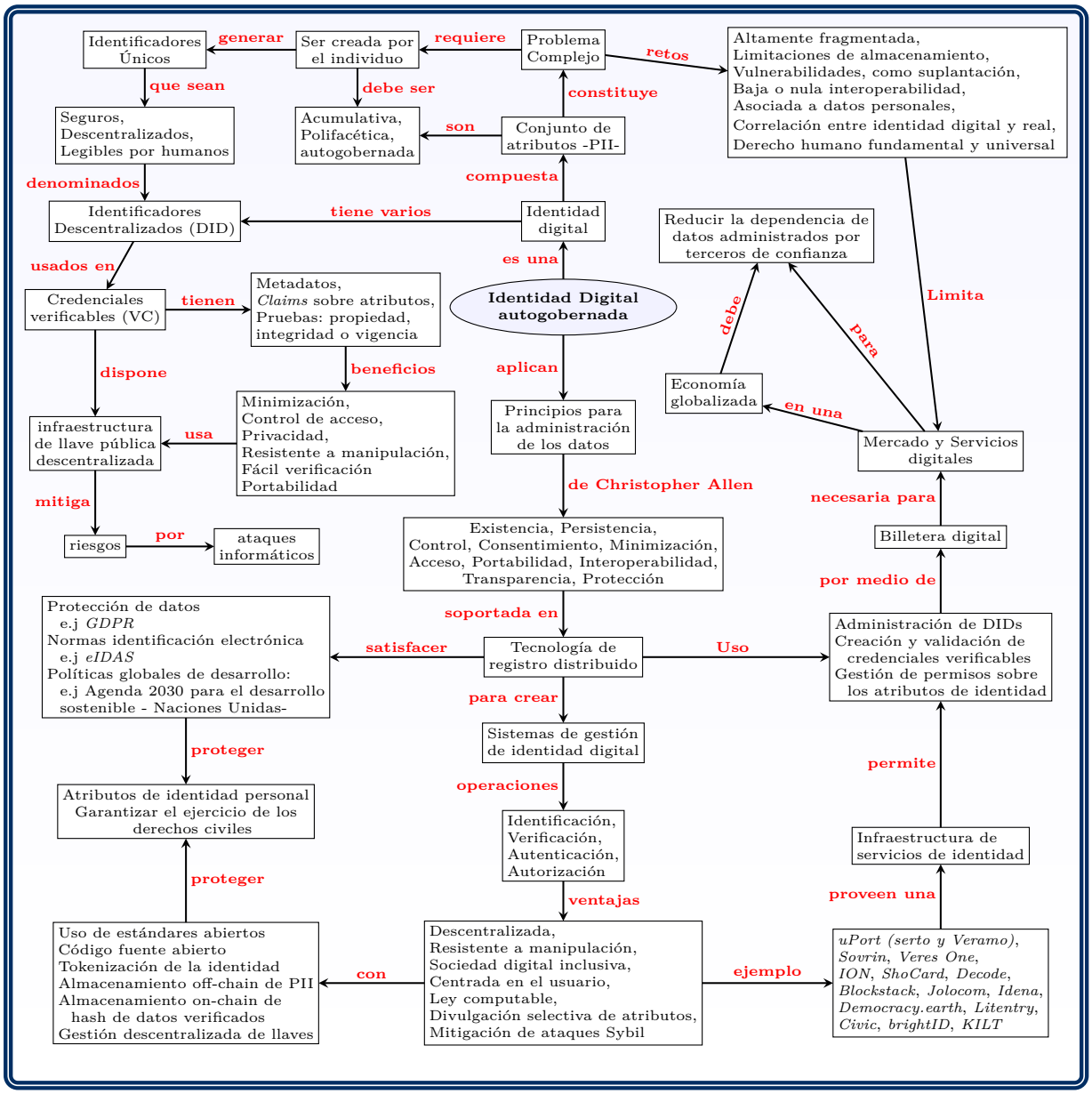


FIGURA 1.2: Esquema para la administración de una identidad autogobernada (SSI): Desafíos e implementación utilizando tecnología de registro distribuido (DLT).
Fuente: Adaptado de [2].

En este contexto, la combinación de la tecnología de registro distribuido (*DLT*) con sistemas de almacenamiento descentralizados como *IPFS* [20, 21, 22] proporciona una plataforma sobre la cual se puede diseñar una arquitectura descentralizada. Esta arquitectura es resistente a la manipulación,

inclusiva, reduce los costos de almacenamiento y mitiga los ataques informáticos [23], otorgando el control de la información al usuario en entornos de confianza, seguridad y privacidad para gestionar su identidad digital, preservando la integridad de los datos [24, 25]. Además, facilita la ejecución de procesos consensuados y autorizados de *Big Data* [26] y el intercambio de documentos [22], cumpliendo con reglamentaciones para la protección de datos personales como el *General Data Protection Regulation* (*GDPR*) [27], estándares de identificación como *Electronic IDentification, Authentication and trust Services* (*eIDAS*) [9], y la protección de datos sensibles como el *Health Insurance Portability and Accountability Act* (*HIPAA*) [28]. Esta interacción tecnológica proveerá la infraestructura de servicios para la identidad digital requerida por la Web 3.0 y deberá hacer uso de estándares abiertos, con código fuente público y auditable, implementar sistemas de almacenamiento descentralizado externo al registro distribuido, resistencia a la computación cuántica y posibilitar la tokenización [29] de los datos personales [9, 30]. En conclusión, una identidad autogobernada es una identidad digital centrada en el usuario, persistente, descentralizada, portátil y transparente, que permite al propietario el uso de un servicio digital de forma segura, privada, confiable y autónoma [1].

La creciente necesidad de una gestión de identidad digital centrada en el usuario y segura requerida por la sociedad actual, exige el diseño y despliegue de sistemas de identidad digital autogobernada (SSI) que incorporen los siguientes elementos:

- La identidad digital es concebida como un derecho humano fundamental que permite un acceso oportuno a servicios, control de la privacidad y mitigación de riesgo de suplantación, además de favorecer el ejercicio de la seguridad nacional [8],[16]. Se estima que 1 100 millones de personas carecen de una identidad oficialmente reconocida y 3 500 millones se encuentran fuera del sistema financiero o con acceso limitado [31]. En [3] se define la identidad como un conjunto de atributos o datos de una persona, los cuales pueden ser divididos en subconjuntos para disponer de perfiles de identidad que le permiten a un individuo autenticarse con diferentes roles en el mundo real, por ejemplo, jefe de un departamento, profesor, estudiante o usuario de un servicio. La identidad digital autogobernada es un tipo de identidad digital descentralizada centrada en el usuario, donde la administración de los atributos de identidad reside directamente en el propietario, ofreciendo ventajas en privacidad, seguridad y control [32]. El usuario está facultado para generar y controlar sus identificadores únicos de identidad, almacenar su información personal, y definir los atributos que desea divulgar conforme al contexto particular del servicio que requiere acceder, por ejemplo, servicios médicos, financieros o de entretenimiento [2]. En la Figura 1.2 se ilustra el contexto general para la administración de una identidad digital autogobernada, con los retos y factores técnicos asociados.
- El esquema centralizado o federado para la administración de una identidad digital requiere intermediarios de confianza, lo que permite ejercer acciones de control y censura, ya que se dispone de un repositorio centralizado en el cual reside la información catalogada como confiable. Esta situación puede producir limitaciones a los ciudadanos para un acceso eficiente y oportuno a servicios, además de posibles fallas para preservar la privacidad, o incluso amenazar la democracia de una nación como se evidenció con el caso de *Cambridge Analytica* que mediante *Big Data* creo perfiles psicológicos de los usuarios para direccionar publicidad política [33]. Por otro lado, se generan riesgos informáticos que al ser explotados por ciberdelincuentes podrían afectar a toda una comunidad, como sucedió en la república de *Estonia* donde un ataque informático de negación de servicio -*DDoS*-, realizado entre los meses de abril y mayo del año 2 007, logró una parálisis total de los servicios estatales [34], provocando disturbios en todo el país. Este incidente canalizó el interés de *Estonia* por asegurar sus sistemas informáticos mediante -*DLT*-, específicamente aplicando *blockchain* para preservar la privacidad de sus ciudadanos [35]. Adicionalmente, los gobiernos proveen marcos normativos para la protección de las privacidad de sus ciudadanos, por ejemplo *GDPR* en la unión europea, la cual es de estricto

cumplimiento a partir del año 2 018. *GDPR* en su artículo cinco establece los siete principios fundamentales para la gestión de datos personales: (1) Procesamiento y almacenamiento de datos ajustado a la ley, predecible, justo y transparente: (2) propósito claro y único para el uso y recolección de datos; (3) los datos recopilados deberán ser estrictamente los necesarios para el uso del servicio; (4) la información debe permanecer actualizada; (5) los datos se deben conservar el tiempo autorizado para su uso y se deben eliminar cuando ya no sean necesarios; (6) se debe preservar la protección y seguridad de los datos bajo custodia evitando accesos no autorizados, perdida de información y desanonimización; y (7) responsabilidad claramente delimitada de cada actor que acceda a la información. Este reglamento o similares obligan al ajuste o creación de nuevos sistemas para gestionar la identidad digital [36]

- La suplantación de identidad puede comprometer la estabilidad personal, económica y moral de los individuos, desde el momento mismo del incidente. Este flagelo produce daños económicos y sociales en los implicados, puesto que deben invertir tiempo y dinero para tratar de recuperarla, además del daño psicosocial al cual quedan expuestos. En [11] se diseñó un modelo para medir el impacto del robo de identidad basado en las experiencias recopiladas por el departamento de defensa de los *EE.UU.* en la encuesta nacional de victimización del delito, que recopiló datos de 16,7 millones de estadounidenses afectados durante el 2 017, y estimó pérdidas económicas de alrededor de 16 800 000 000USD. Además, un estudio del departamento de justicia realizado en 2 016 y publicado en 2 019 estableció que el 10 % de los residentes en Estados Unidos manifestó haber sido victima de suplantación [37]. Además, la posibilidad de eludir la responsabilidad y las inherentes sanciones a actos delictivos se relaciona directamente con la capacidad de los individuos u organizaciones para eliminar o reducir la supervisión y control social, mediante limitaciones a la individualización (identificación) en la investigación de delitos y acopio de pruebas. Por lo cual, se recomienda el diseño de sistemas de información que permitan ejercer una veeduría social, orientada a mitigar la afectación por el accionar deshonesto de individuos [38], [39], [40]. *DLT* se perfila como la tecnología subyacente para diseño de sistemas descentralizados que permiten una correcta identificación de las personas, preservando la integridad y privacidad de la información [30], [24], [41].
- La *DLT* puede generar un cambio en el paradigma de gestión de la información ya que se modificarán los procesos de administración tecnológica en las organizaciones, realizando la transición de una Internet de la información a una Internet del valor, siendo necesario adaptar prácticas para el desarrollo de plataformas tecnológicas corporativas, integrando la automatización de procedimientos legales para transferencia de valor, lo que dinamizará el sistema de registro e intercambio de bienes y servicios, con acceso democrático a la información, y un subsecuente cambio cultural, que permitirá el empoderamiento de las personas hacia el control de la información y de las instituciones, como factor clave de transparencia y eficiencia [2], [42], [43], [44]. Por ejemplo, el registro de derechos de autor basados en *blockchain* permitirá recibir una compensación ajustada al uso de la obra, ya que claramente se establece y preserva el origen de las creaciones artísticas [45]. Asimismo, movimientos sociales y activistas tecnológicos han reclamado por un sistema de contabilidad de valor y gestión de identidad, que utilice las nuevas tecnologías como *blockchain* para evitar la represión estatal y se aleje de la lógica del capitalismo que únicamente incluye en la contabilidad los aspectos que impactan las ganancias, siendo así una herramienta pragmática e intelectual de dominación social. *DLT* esta transformando el modelo de confianza en la industria ya que esta tomando fuerza la validación por *software* realizada por la ejecución de algoritmos de consenso frente a la validación por terceros confiables; y podría ser utilizada para el diseño de una nueva economía común en las que sus miembros obtengan beneficios de acuerdo con el valor que produzcan, por ejemplo, los mineros de criptomonedas [46].
- Finalmente, un factor de éxito para el diseño y despliegue de una plataforma *SSI* es la posibilidad de crear identificadores únicos descentralizados -*DID*- mediante el uso de la criptografía

asimétrica que junto con el registro y verificación bajo una infraestructura de llave pública descentralizada (*Decentralized Public Key Infrastructure -DPKI-*) que opere de forma global y pública [47] soportada en *DLT* [48]. El triángulo de *Zooko* establece las tres características para un *DID*, y se discute la dificultad de crear un identificador que satisfaga de manera simultánea los requerimientos de seguridad, descentralización y legibilidad por el humano [49]; y en el modelo de privacidad propuesto por *Nakamoto* [50] se introduce un *DID* con dos características únicamente, son seguros dada la criptografía asimétrica aplicada y se generan en la *blockchain* de forma descentralizada [51], pero el *DID* obtenido no es fácilmente leído por los humanos, como se observa en este identificador $12HSM4FRr6V6CBzhJA4Z8fxdU1eazvVW6t$ asociado a un usuario en la *blockchain* de *bitcoin*.

Considerando los retos y problemas planteados en este capítulo, y con el propósito de abordar los desafíos en la gestión de la identidad digital autogobernada, se establecen los siguientes objetivos e hipótesis. Estos elementos buscan contribuir a un modelo de administración de identidad digital que sea más seguro, autónomo y eficaz. La intención es crear un marco que potencie la capacidad de los usuarios para gestionar sus identidades de manera transparente, confiable y con control total.

1.2.1 Objetivos

1.2.1.1 Objetivo General

Proponer un modelo para la gestión de una identidad digital autogobernada soportado en la tecnología de registro distribuido.

1.2.1.2 Objetivos Específicos

1. Analizar los atributos y requisitos necesarios en un modelo de identidad digital autogobernada.
2. Diseñar la arquitectura para un sistema de administración de una identidad digital autogobernada.
3. Diseñar e implementar un escenario de experimentación que permita evaluar el modelo propuesto para la identidad digital autogobernada.

1.2.2 Hipótesis

Un modelo para la gestión de una identidad digital autogobernada soportado en la tecnología de registro distribuido permitirá preservar la privacidad e integridad de los atributos personales de identificación y su intercambio seguro.

Capítulo 2

Caracterización de la identidad digital autogobernada

El presente capítulo se enfoca en la caracterización de la identidad digital autogobernada. Se estructura en dos secciones, la primera describe la metodología utilizada para llevar a cabo una revisión sistemática de la literatura, mientras que la segunda presenta un análisis de la literatura seleccionada, con el objetivo de identificar los atributos esenciales para el diseño de una identidad digital autogobernada y las arquitecturas propuestas para su implementación. La revisión sistemática, realizada utilizando el lenguaje R y el paquete *Bibliometrix*, permitió desarrollar una visión holística y exhaustiva de los principales componentes y enfoques en el ámbito de la identidad digital descentralizada.

2.1 Metodología de revisión sistemática de la literatura

La revisión sistemática de la literatura permite construir una visión general del área de investigación [52],[53]. En este trabajo, la revisión se llevó a cabo con el objetivo de identificar los atributos y requisitos necesarios para el diseño de un modelo de identidad digital autogobernada, junto con las arquitecturas propuestas, y se realizó bajo un enfoque reproducible implementado con el lenguaje de programación *R* [54] y el paquete de análisis bibliométrico *Bibliometrix* [55]. La Figura 2.1 contiene el diagrama de flujo que ilustra el proceso sistemático de la revisión aplicado, y consolida los resultados obtenidos, en términos de las publicaciones tratadas en cada una de las etapas del protocolo de revisión. Este diagrama proporciona una vista organizada del proceso de revisión sistemática de la literatura, incluyendo las fuentes de datos, los criterios de búsqueda, los pasos de filtrado y el número final de documentos incluidos para un análisis completo.

2.1.1 Preguntas de investigación

Este estudio se ha enfocado en determinar el estado del arte sobre la aplicación de la tecnología de registro distribuido para el diseño de una identidad digital autogobernada, para lo cual se formularon las siguientes preguntas de investigación:

1. ¿Cuáles son los atributos y requisitos en un modelo de identidad digital autogobernada?
   Ésta es la principal pregunta de investigación ya que facilita identificar y comprender los requerimientos de información en la construcción de una identidad autogobernada. Además,

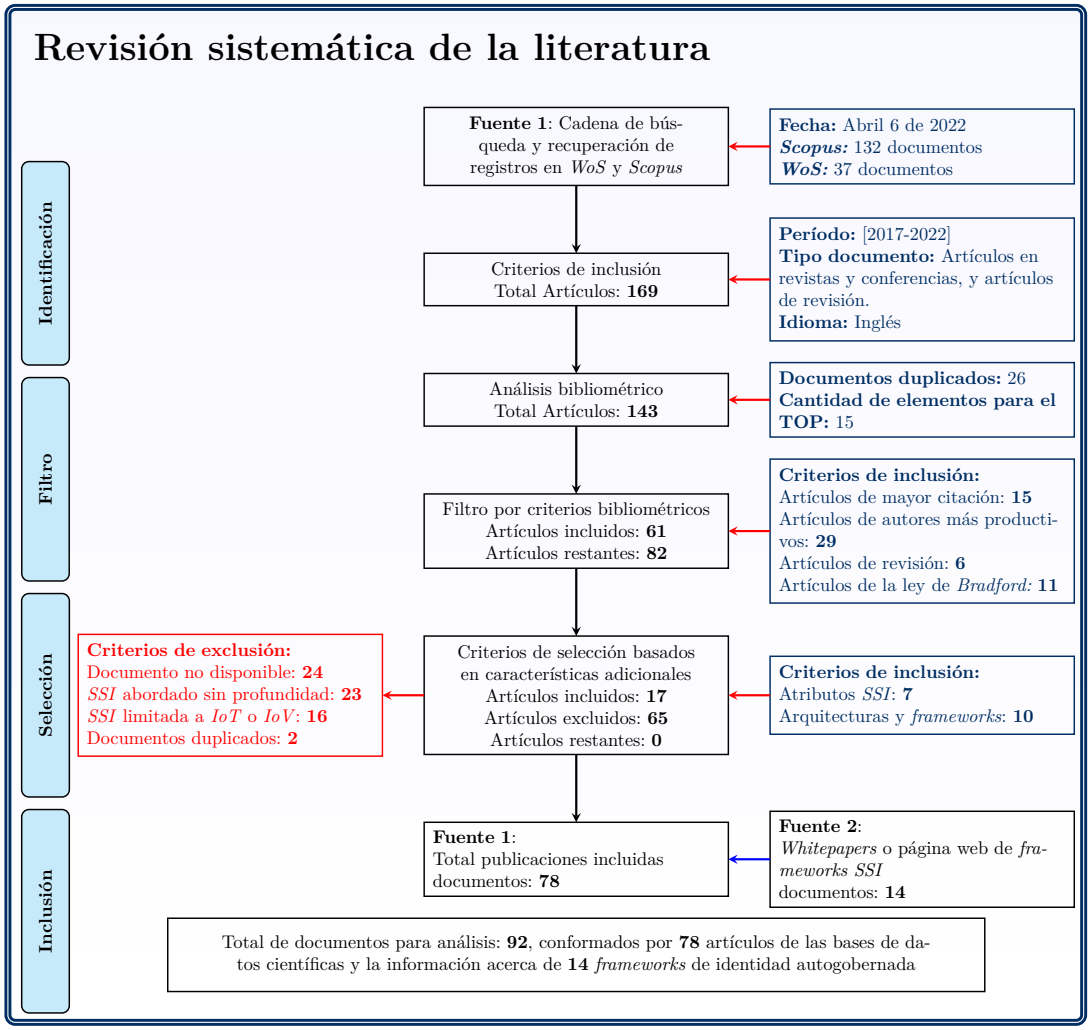


FIGURA 2.1: Diagrama del proceso de revisión sistemática de la literatura.
Fuente: Elaboración del autor.

el análisis de las publicaciones relevantes sobre *SSI* permite establecer los diferentes enfoques al problema de gestión de identidad centrada en el usuario.

2. ¿Cuáles arquitecturas se han propuesto para sistemas de administración de identidad digital autogobernada?
   Determinar y analizar las arquitecturas para *SSI* permite identificar componentes tecnológicos, y establecer el flujo de información y control de los atributos de identidad en ambientes *SSI*.

2.1.2 Identificación

La búsqueda incluyó dos bases de datos científicas, *Web of Science* [56] y *Scopus* [57], las cuales se han seleccionado por vincular artículos publicados en revistas o conferencias acreditadas, con estrictos procesos de revisión por pares.

La Figura 2.2 muestra una estructura de árbol que ilustra la construcción de la sentencia de búsqueda utilizada para recuperar publicaciones de las bases de datos seleccionadas, enfocadas en la gestión de la identidad digital, la identidad autogobernada y la tecnología blockchain. Se observa la unión de los conjuntos de referencias obtenidos sobre los títulos y las palabras claves. La sentencia

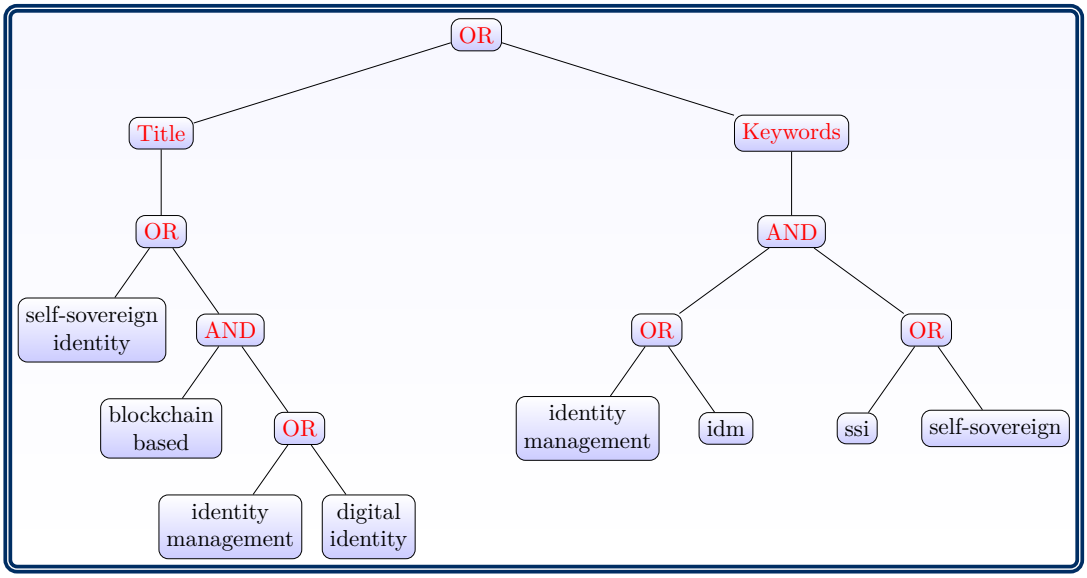


FIGURA 2.2: Estructura de la cadena de búsqueda para recuperación de documentos relacionados con identidad digital autogobernada basada en blockchain.
Fuente: Elaboración del autor.

de búsqueda se refinó mediante la realización de consultas piloto en las que se probaron términos asociados con los principios y componentes de la identidad autogobernada como: privacidad, autenticación, credenciales verificables, seguridad, identificadores descentralizados y *frameworks* de *SSI*. La consulta final en las bases de datos se realizó el día 6 de abril de 2022, y excluyó los documentos con alguna de las siguientes condiciones: fecha de publicación anterior a 2017, escritos en idioma diferente al inglés o cuyo tipo de documento no corresponda con artículo de revista, conferencia o revisión. La búsqueda extrajo 132 documentos de *Scopus* y 37 de *WoS*.

2.1.3 Filtro

El conjunto de referencias bibliográficas se procesó con el paquete *Bibliometrix* [55], eliminando 26 documentos duplicados, quedando un total de 143 publicaciones. El análisis bibliométrico recopiló datos de los documentos con la finalidad de ubicar temporalmente autores y publicaciones, definir los investigadores de mayor impacto junto con los medios de publicación con mayor preferencia, además de analizar la dinámica de las palabras claves. Los resultados del procesamiento bibliométrico se pueden consultar en [58], [59].

Los criterios bibliométricos aplicados para la inclusión son:

1. Documentos con el mayor número de citaciones: estas publicaciones han sido validadas por la comunidad científica y representan un soporte para el desarrollo del área de investigación.

2. Autores con mayor productividad: la ley de *Lotka* establece una distribución asimétrica de autores generando una concentración de artículos relevantes sobre un tema de investigación en un grupo reducido de autores [111].

3. Artículos de revisión: permiten sintetizar la producción científica y analizar los avances en un campo de investigación.

4. Artículos publicados en revistas de la zona núcleo conforme a la ley de *Bradford*: se distribuyeron las fuentes de publicación en tres conjuntos aproximadamente del mismo tamaño, una

Criterio de inclusión	Total	Referencias
Documentos más citados **Total: 15**	15	[19], [60], [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [49]
Documentos de los autores de mayor producción **Total: 29**	7	*Nitin Naik* y *Paul Jenkins*: [73], [1], [74], [36], [75], [76], [77]
	3	*Qinghua Lu* y *Yue Liu*: [78], [79], [80]
	1	*Qinghua Lu*: [81]
	4	*Reza Soltani*, *Uyen Trang Nguyen* y *Aijun An*: [31], [82], [83], [84]
	3	*Eranga Bandara*, *Xueping Liang*, Peter *Foytik* y *Sachin Shetty*: [85], [86], [87]
	4	*Christoph Meinel*: [88], [89], [90], [91]
	2	*Andreea-Elena Panait*: [92], [93]
	2	*Andreas Abraham*: [94], [95]
	3	*A. Antonidoss*: [96],[97],[98]
Artículos de revisión **Total: 6**	6	[99], [100], [101],[102], [103], [104]
Artículos seleccionados por la ley de *Bradford* **Total: 11**	3	*Lecture notes in computer Science*: [105], [106], [107],
	5	*Frontiers in Blockchain*: [108], [33], [10], [46], [109]
	1	*IFIP Advances in information and communication technology*: [45]
	2	*Lecture notes in business information processing*: [110], [37]

Tabla 2.1: Resultados de la aplicación de criterios de inclusión de publicaciones basados en indicadores bibliométricos.
Fuente: Elaboración del autor.

fuente se asigna a un conjunto dependiendo del número de citaciones que presenta [112]. En la zona 1 se tendrán las fuentes de publicación con mayor preferencia e impacto en el área de investigación.

Finalmente, la Tabla 2.1 resume los resultados obtenidos después de aplicar los diferentes criterios de inclusión en la revisión sistemática de literatura, definidos a partir del análisis bibliométrico del conjunto de publicaciones recuperado de las bases de datos. En el caso de los artículos que satisfacen más de una condición se asignaron al primer criterio determinado.

2.1.4 Selección

Criterio de exclusión	Total	Referencias
Texto completo no disponible	24	[113],[114], [115],[116], [117], [118],[119], [120], [121], [122], [123], [124], [125], [126], [127], [128], [129], [130],[131], [132], [133], [134], [135], [136]
Aborda *SSI* sin profundizar en atributos, principios o arquitecturas	23	[137], [138], [139], [140], [141], [142], [143], [144], [145], [146],[147], [148], [149], [150], [151], [152], [153], [154], [155], [156], [157], [158], [159]
SSI limitada al contexto *IoT* o *IoV*	16	[160], [161], [162], [163], [164], [165], [166], [167], [168], [169], [170], [171], [172],[173],[174], [175]

Tabla 2.2: Resultados de la aplicación de criterios de exclusión para la selección de artículos en la revisión sistemática de literatura
Fuente: Elaboración del autor.

La etapa de selección se dividió en dos fases. En la primera fase, se aplicó un filtro de exclusión a los documentos relacionados en la tabla 2.1. En la segunda fase, se realizó una revisión general de los artículos aún no clasificados para encontrar las publicaciones enfocadas en las preguntas de investigación planteadas.

La eliminación de artículos aplicó tres condiciones de exclusión: (1) imposibilidad de acceder al texto completo de la publicación, (2) artículos cuyo foco principal no sea la identidad autogobernada, lo que dificultaría establecer atributos y requisitos de una *SSI* o determinar su arquitectura, y (3) documentos que limitan el diseño de *SSI* a contextos específicos como la Internet de las cosas o la Internet de los vehículos. En la Tabla 2.2 se presenta el listado de los artículos excluidos por los criterios mencionados.

Criterio de inclusión	Total	Referencias
Atributos *SSI*	7	[32], [176], [177], [178], [179], [180], [181]
Arquitectura y *framework*	10	[182], [4], [183], [184], [185], [186], [187], [188], [189], [190]

Tabla 2.3: Criterios de inclusión de publicaciones basados en el contenido y las características del artículo. Fuente: Elaboración del autor.

Framework	**Sigla**	**Cita**	**Año**	**Tecnología**
A Protocol and Token for Self-Sovereign Identity and Decentralized Trust	*Sovrin*	[191]	2018	*Hyperledger Indy* [192]
A platform for self-sovereign identity	*uPort ⇒ {serto, veramo}*	[193]	2016	Ethereum [194] , IPFS [20]
A Globally Interoperable Network for Identity	*Veres One*	[195]	2019	Blockchain diseñada especialmente para administrar *DID* [195]
Decentralized Layer 2 network for Decentralized Identifiers	*ION*	[196]	2020	bitcoin [50], *sidetree* [197], *IPFS* [20], *MongoDB* [198]
Identity Management Verified Using the Blockchain	*Shocard*	[199]	2015	*bitcoin* [50]
Decentralised Citizens Owned Data Ecosystem	*Decode*	[200]	2016	chainspace [201], zenroom [202]
Stacks 2.0: Apps and Smart Contracts for Bitcoin	*BlockStack ⇒ stacks*	[203]	2017	*bitcoin* [50], *Proof of Transfer -PoX- [204]*, *Clarity language* [205]
A Decentralized, Open Source Solution for Digital Identity and Access Management	*Jolocom*	[206]	2019	*Ethereum, Rinkeby Testnet* [194], *IPFS* [20]
Proof of Humanity: Decentralized human identity without sybils or bots	*Democracy.earth*	[207]	2017	*Ethereum* [194], *kleros* [208]
A decentralized cross-chain Identity Aggregator	*Litentry*	[209]	2021	parachain en Polkadot [210]
SelfKey: Self-Sovereign Identity for more Freedom and Privacy	*Selfkey*	[211]	2017	*Ethereum* [194]
Civic Pass: An integrated permissioning tool that helps businesses control access to their dApps	*Civic*	[212]	2017	*ethereum* [194] Token ERC-20, *RSK* [213], bitcoin [50]
Social identity network of unique humans. BrightID allows people to prove to applications that they're only using one account.	*brightID*	[214]	2022	*Blockchain* propia, *arangoDB* [215]
A blockchain identity protocol for issuing self-sovereign, anonymous, verifiable credentials and decentralized identifiers	*KILT*	[216]	2022	*Parity substrate* [217]

Tabla 2.4: Información general de los *frameworks* para identidad digital autogobernada identificados en el proceso de revisión sistemática de la literatura. Fuente: Elaboración del autor.

Por último, la segunda fase de selección consistió en una revisión manual de los documentos para aplicar dos criterios complementarios de inclusión: el primero, orientado a identificar los artículos que describen los atributos necesarios en un sistema *SSI*, y segundo, las publicaciones que contienen el diseño de una arquitectura para *SSI*.

Los documentos agregados mediante los dos criterios de inclusión de la fase 1 se presentan en la Tabla 2.3. La Tabla 2.4 enumera los documentos adicionales incluidos, correspondientes a literatura gris, como *whitepapers*, que son generados por los desarrolladores de los *frameworks* de identidad autogobernada y proporcionan detalles técnicos sobre su diseño e implementación. Los datos presentados en esta tabla son el resultado de una revisión sistemática de la literatura sobre proyectos y *frameworks* relacionados con la identidad digital autogobernada basada en tecnología de registro distribuido. La tabla resume los 14 *frameworks* identificados, incluyendo el año de inicio, la referencia bibliográfica y las tecnologías *BC-DLT* utilizadas en cada uno.

2.1.5 Inclusión

El proceso de inclusión de artículos mediante un análisis bibliométrico se orienta a minimizar el sesgo en la selección manual de los artículos para su análisis. Para lograr esto, se utilizó el paquete *Bibliometrix* [55], una herramienta bibliométrica que permite descubrir patrones en un conjunto de referencias bibliográficas y promover una selección objetiva y sistemática de publicaciones.

El conjunto final de artículos seleccionados para construir el estado de arte consta de 92 publicaciones, distribuidas en 78 documentos de revistas y conferencias, y 14 *whitepapers* de *frameworks* para SSI. Se resalta que, los *frameworks SoraID* [218] y *EverID* [219] fueron descartados debido a la falta de información técnica sobre su diseño e implementación.

Se implementó un enfoque metodológico reproducible que integra la vigilancia tecnológica con la revisión sistemática de la literatura. Este método permitió realizar búsquedas de actualización periódicas para mantener la vigencia de la información. La última actualización bibliométrica, que refleja el estado actual del conocimiento en el campo, se encuentra detallada en [220]. Este proceso iterativo asegura que el análisis se base en la literatura más reciente y relevante, proporcionando una visión integral y actualizada del tema de estudio.

Información principal del conjunto de datos	
Periodo	[2018-2023]
Fuentes (Revistas, Libros, etc.)	190
Documentos	327
Tasa de Crecimiento Anual %	50.61
Edad Promedio de los Documentos	2.48
Citas Promedio por Documento	9.682
Citas Promedio por Año por Documento	2.146
Referencias	1
TIPOS DE DOCUMENTOS	
artículo	91
artículo de conferencia	225
revisión	11
CONTENIDO DE LOS DOCUMENTOS	
Keywords Plus (ID)	1249
Palabras Clave del Autor (DE)	729
Autores	
Autores	907
Apariciones de Autores	1222

Autores de documentos de un solo autor	21
COLABORACIÓN ENTRE AUTORES	
Documentos de un solo autor	23
Documentos por Autor	0.361
Co-Autores por Documento	3.74
Co-autorías Internacionales %	8.257

TABLA 2.5: Descripción del conjunto de datos analizado en [220].
Fuente: Elaboración del autor.

En la Tabla 2.5 se presenta la actualización del conjunto de referencias bibliográficas. El número de publicaciones aumentó de 169 a 327, con una tasa de crecimiento anual del 50,61 %.

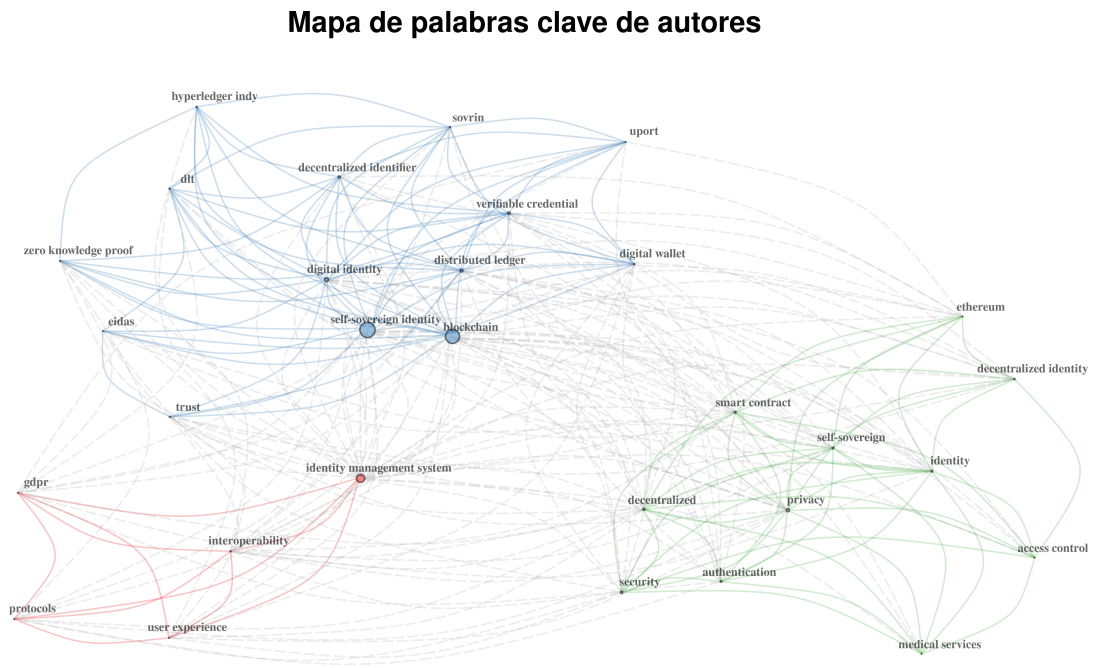


FIGURA 2.3: Relación entre palabras claves propuestas por los autores.
Fuente: Elaboración del autor.

Asimismo, la Figura 2.3 muestra la correlación entre las palabras clave definidas por los autores en el conjunto de publicaciones revisado, las cuales se agrupan en tres bloques. El primer grupo, representado en color rojo, tiene como término principal "*identity management system*" y está asociado con los términos "*interoperability*", "*gdpr*", "*user experience*" y "*protocols*". Este grupo se centra en el concepto de gestión de la identidad, sugiriendo un enfoque integral que abarca aspectos técnicos, legales y de usabilidad. La inclusión de *GDPR* refleja una preocupación por la privacidad y el cumplimiento normativo, mientras que la interoperabilidad y los protocolos señalan la necesidad de estándares comunes en este campo. El segundo *cluster*, en color azul, se enfoca en "*blockchain*" y su relación con conceptos como "*digital identity*", "*verifiable credential*", "*distributed ledger*", "*decentralized identifier*", "*digital wallet*", "*zero knowledge proof*", "*hyperledger indy*", "*dlt*", "*sovrin*", "*eidas*", "*uport*" y "*ethereum*". Este grupo aglutina conceptos relacionados con la tecnología blockchain y su aplicación en la gestión de identidad digital. Evidencia que blockchain emerge como una tecnología esencial en el ámbito de la identidad digital, mostrando una fuerte asociación con credenciales verificables, identificadores descentralizados y pruebas de conocimiento cero, lo que indica un

marcado énfasis en la seguridad y la privacidad. La referencia a proyectos específicos como *Hyperledger Indy*, *Sovrin*, *uPort* y *Ethereum* sugiere un ecosistema diverso de soluciones *blockchain* para identidad. La mención de *eIDAS* subraya la relevancia de estos conceptos en el contexto regulatorio europeo. El tercer grupo, en color verde, tiene como tema principal "*Self-sovereign*" y muestra su relación con "*privacy*", "*decentralized*", "*security*", "*identity*", "*smart contract*", "*authentication*", "*decentralized identity*", "*access control*", "*trust*" y "m*edical services*", características clave de un sistema de gestión de identidad digital. Este grupo presenta la soberanía de datos como un concepto central, integrando aspectos cruciales como privacidad, seguridad, autenticación y control de acceso. La inclusión de términos como "*decentralized*" y "*self-sovereign*" apunta hacia una tendencia de sistemas más distribuidos y centrados en el usuario. La mención de contratos inteligentes indica la integración de funcionalidades automatizadas. La presencia de "*medical services*" sugiere aplicaciones específicas en el sector de la salud, donde la gestión segura de la identidad es particularmente crítica. En resumen, este diagrama refleja un ecosistema de identidad digital en evolución, con un fuerte énfasis en la descentralización, la seguridad, la privacidad y el control del usuario. La tecnología *blockchain* emerge como un facilitador para la implementación de estos conceptos, mientras que la interoperabilidad y el cumplimiento normativo se mantienen como consideraciones importantes en el desarrollo de sistemas de identidad digital autogobernados.

2.2 Análisis crítico de la literatura

Un sistema de administración de identidad (*IdM*) contempla un conjunto de herramientas, procesos y políticas diseñados para gestionar la identidad de manera efectiva. Este sistema abarca un ciclo de vida que se compone de cuatro etapas: creación de la identidad, autenticación, emisión de afirmaciones (*claims*) sobre un sujeto y verificación de identidad [101]. Los *IdM* pueden ser (i) centralizados, siguiendo un modelo de silo, donde el proveedor de servicio (SP) se encarga de todas las etapas del ciclo de vida; (ii) federados, donde existe un proveedor de identidad (*IdP*) responsable de la creación y autenticación de las identidades para acceder a un *SP*; y, finalmente, (iii) descentralizados, donde se crea una identidad autogobernada y centrada en el usuario, quien tiene el control sobre su identidad.

A continuación, se presenta la síntesis del conjunto de publicaciones establecido en la sección 2.1.5 para la revisión completa, que permite dar respuesta a las preguntas de investigación planteadas en la sección 2.1.1. En primer lugar, la sección 2.2.1 describe los atributos y la interacción entre los actores que conforman un IdM autogobernado. En segundo lugar, la sección 3 presenta las arquitecturas propuestas para el diseño de sistemas de identidad autogobernada (SSI).

2.2.1 Atributos esenciales de una identidad autogobernada

SSI adiciona la capa de identidad digital ausente en el diseño y evolución de la Internet. Permite a cualquier sujeto crear, poseer y controlar una identidad verificable y persistente en un ecosistema de datos centrado en el humano (*HCDE*, por su sigla en inglés), facilitando la construcción de relaciones únicas, independientes y confiables para el intercambio de información entre pares, como credenciales verificables, por medio de canales de comunicación seguros [108].

Los requisitos para el diseño de un sistema gestor de identidad autogobernada se soportan sobre la regla *WORM (Write Once Read Many),* almacenando los atributos de identificación personal en repositorios externos al *DLT* [65], los principios de identidad propuestos por *Christopher Allen*, patrones de diseño para sistemas *SSI* basados en *blockchain*, y sobre los cuatro pilares básicos en un sistema de identidad: identificación, autenticación, credenciales verificables y almacenamiento

[1],[49]. La creación de identificadores descentralizados [221] y la gestión de credenciales verificables [222] para un modelo de *SSI* se pueden implementar mediante la aplicación de estándares diseñados por el *World Wide Web Consortium -W3C-*.

2.2.1.1 Conceptos fundamentales en identidad digital autogobernada

Ferdous et al. proponen una definición de términos relativos a *SSI* con el objeto de proporcionar el significado semántico más adecuado [67]. La Tabla 2.6 presenta una lista adaptada de estas definiciones.

Término en Español	**Término en Inglés**	**Definición**
Entidad, Sujeto, Titular	*Entity, Sujet, Holder*	Es un objeto humano, jurídico, físico, digital o abstracto quién es el titular de los derechos de identidad digital. La existencia del objeto se caracteriza mediante un conjunto de atributos. Recibe las credenciales generadas por un emisor y las presenta para su verificación. El titular es independiente si tiene el control de las llaves criptográficas, y dependiente cuando su identidad es controlada por un tercero debido a limitaciones físicas o legales [1].
Atributo	*attribute*	Es una característica medible de una entidad que lo califica como miembro de un determinado conjunto [60]. Se representa con un nombre y un valor, el cual puede ser asignado por un tercero de confianza. Los atributos pueden variar en el tiempo y podrán ser revocados.
Identificador	*Identifier*	Es un atributo especial de la entidad que no representa una característica que describe al sujeto sino que permite su identificación inequívoca en un dominio dado.
Afirmación	*Claim*	Es una declaración que se puede realizar sobre una entidad. La afirmación es un conjunto de n pares ($n >= 1$) nombre-valor que puede ser generada por la misma entidad o por un tercero de confianza.
Credencial	*Credential*	Es un conjunto no vacío de afirmaciones que junto a un identificador le permite a una entidad atestiguar su titularidad en un proceso de autenticación.
Credencial verificable	*Verifiable credential*	Es una credencial a prueba de manipulaciones que preserva la privacidad y permite su comprobación por parte de un verificador [1]
Certificación	*Attestation*	Proceso por el cual una entidad verifica una afirmación, expresada mediante una credencial verificable.
Proveedor de identidad	*Identity provider* -IdP-	Gestiona la identidad parcial de una entidad y permite su interacción entre diferentes dominios.
Proveedor de servicios	*Service provider* -SP-	Proporciona servicios digitales a una entidad conforme a un perfil de usuario acordado.
Terceros de Confianza	*Trusted Third Party* -TTP-	Entidad cuyas afirmaciones sobre otras entidades son aceptadas por los otros actores del sistema.
Emisor	*Issuer*	Es una entidad confiable que emite afirmaciones como credenciales verificables sobre una entidad y las transfiere al titular [1]
Verificador	*Verifier*	Es una entidad que solicita credenciales a un titular y atestigua la autenticidad e integridad de tales afirmaciones. Usualmente el verificador es un proveedor de servicios [1].
Infraestructura de llave pública descentralizada	*Decentralized Public Key Infrastructure -DPKI-*	Proporciona un entorno de confianza descentralizado para el registro de llaves públicas como *DID* y la realización de las operaciones conforme a la criptografía asimétrica sin comprometer la seguridad e integridad del sistema [31].

Continúa en la siguiente página

Tabla 2.6 – continuación de la página anterior

Término en Español	Término en Inglés	Definición
Registro de datos verificables	*Verifiable data registry*	Registro confiable para la creación, revocación o validación de identificadores, credenciales y presentaciones verificables. Por lo general se utiliza una *blockchain*, aunque el sistema *SSI* también podría adicionar otras bases de datos, como por ejemplo el registro de identificación del gobierno [31].
Centros de identidad	*Identity Hub*	Solución de almacenamiento de datos centrada en el usuario, con alta disponibilidad, segura e interoperable [31], [13].
Billetera	*Digital Wallet*	Componente lógico o físico responsable del almacenamiento de las llaves criptográficas que aseguran la privacidad y control del usuario. Opcionalmente la *Wallet* podría almacenar los atributos de identidad [31]. Por medio de la billetera el usuario podrá generar sus llaves, firmar y verificar transacciones, crear o revocar permisos y realizar copias de seguridad o recuperación de llaves [31].

Tabla 2.6: Definición de los conceptos clave en una identidad digital autogobernada.
Fuente: Adaptado de [67].

2.2.1.2 Principios de diseño para la identidad autogobernada

Christopher Allen en el año 2016 propuso diez principios normativos para una identidad autogobernada [223], los cuales son considerados como referente para el diseño y evaluación de una plataforma *SSI*, y se consideran factores diferenciales respecto a un esquema centralizado o federado [32]. Estos principios se agrupan en tres categorías: controlabilidad, seguridad y portabilidad [2], [49].

- **Controlabilidad**
  1. **Existencia**: La existencia de una persona prevalece sobre la representación digital de sus identidades y debe ser independiente de estas. Una *SSI* debe permitir expresar digitalmente los atributos de una entidad [67], posibilitando el ejercicio del derecho individual de la autodeterminación respecto a la identidad [32].
  2. **Control**: El usuario es propietario de su información y debe tener la máxima autoridad sobre sus identidades. Una *SSI* debe permitir una autonomía total en la gestión y administración de la identidad digital [67]. La soberanía de la información se puede dividir en dos categorías, (1) de estado, referente a la autoridad territorial y jurisdiccional que ejerce un gobierno en todas la entidades de su territorio, y (2) de ciudadano, concerniente a los derechos inherentes del sujeto [1].
  3. **Consentimiento**: El usuario deberá tener la facultad de otorgar o denegar el acceso a sus datos. Por lo tanto, el intercambio de información solo será posible si existe una autorización vigente. La entidad debe ser la única fuente de confianza sobre su identidad para evitar colusión entre entidades con el objeto de compartir atributos sin la autorización del poseedor [67].
- **Seguridad**
  4. **Minimización**: El usuario podrá realizar divulgación selectiva de sus atributos de identidad, minimizando la exposición de su información.
  5. **Persistencia**: La identidades deben perdurar en el tiempo mientras sean requeridas por el propietario, quién será el único autorizado para su eliminación. Las credenciales

verificables podrán ser actualizados o eliminadas dependiendo del contexto de uso [181]. Una afirmación emitida por un tercero de confianza deberá persistir mientras exista el emisor [67].

6. **Protección**: Se debe priorizar mediante entornos descentralizados, el ejercicio de los derechos individuales propendiendo por la libertad con sistemas resistentes a censura. Una *SSI* deberá implementar métodos criptográficos que garanticen un no-repudio de la identidad y satisfagan la confidencialidad, integridad y autenticidad de los atributos [67].

- **Portabilidad**

7. **Acceso**: Una entidad deberá tener siempre acceso directo y sin restricciones a sus atributos de identidad y podrá conocer las consultas realizadas sobre sus identidades [67]; y no deberán existir *PII* que sean ocultos para el sujeto [181].
8. **Transparencia**: Los algoritmos y plataformas utilizados para administrar la identidad digital deben ser de código abierto, sin restricciones por licenciamiento e independientes de una arquitectura específica. El uso de estándares abiertos maximiza la transparencia, portabilidad, interoperabilidad, adopción y sostenibilidad de un sistema *SSI* [67].
9. **Portabilidad**: Un usuario deberá poder mover o transportar su identidad sin restricciones jurídicas, políticas o tecnológicas, garantizando de esta manera el control sobre la identidad frente a imprevistos. Una *SSI* deberá definir mecanismos para recuperación de la identidad en caso de fallo o perdida del dispositivo de almacenamiento [67]; por lo tanto, es importante el diseño de modelos para la gestión de llaves criptográficas seguros, amigables con el usuario y que preserven la privacidad [82].
10. **Interoperabilidad**: Una persona podrá utilizar sus identidades digitales en múltiples escenarios o plataformas, inclusive de forma global sin perder o ceder el control.

2.2.1.3 Patrones de diseño de una identidad autogobernada basados en *blockchain*

Liu et al. han recopilado y clasificado doce patrones de diseño para la implementación de aplicaciones que permitan una *SSI* basada en *blockchain*, enfocados en tres áreas: llaves criptográficas, *DID* y *VC* [79],[80].

- Llaves criptográficas

1. Generación de llave maestra y secundarias: por la naturaleza polifacética de la identidad digital se requiere que la entidad posea una llave principal a partir de la cual se deriven n-llaves secundarias para firmar las transacciones de sus sub-identidades, con el objetivo de mitigar el riesgo de correlación puesto que separa la interacción de una entidad en roles.
2. Almacenamiento: la entidad dispondrá de dos tipos de billeteras digitales, una conectada a Internet (*hot*) y otra sin conexión (*cold*). La *hot wallet* conecta al usuario a la *blockchain* y a Internet, y acota los casos de uso a operaciones especificas relacionadas con los *DID* registrados en la *DLT*, con el objeto de minimizar el efecto de un ataque informático. La *cold wallet* almacena las llaves criptográficas, por ejemplo *Trezor*, *ledger* o papel. Este esquema requiere una constante interacción entre las dos billeteras para la firma de transacciones.
3. Fragmentación: la llave privada asegura el control sobre la identidad digital, su perdida es un incidente grave ya que imposibilita al usuario acceder a su *SSI*. Esta llave es difícil de memorizar, por lo que se requieren de métodos seguros para realizar su copia de seguridad y restauración. La fragmentación criptográfica (por ejemplo, el esquema Shamir) permite

dividirla en n-fragmentos, y distribuirlos en diferentes ubicaciones, como por ejemplo una lista de contactos confiables.

- Identificadores descentralizados
  4. Registro de identificadores: vincula un *DID* registrado *on-chain* con los atributos almacenados *off-chain*. Este control de acceso garantiza que únicamente el propietario del *DID* pueda realizar modificaciones.
  5. Registro múltiple: una entidad podrá registrar un único *DID* para cada contexto o subidentidad, y así, mantener las transacciones independientes.
  6. *Blockchain* y redes sociales: se establece una relación bidireccional entre los perfiles de redes sociales y la identidad basada en *blockchain*, para mejorar la confiabilidad de las dos identidades.
  7. Doble resolución de *DID*: establecer una comunicación entre un par de entidades puede requerir que cada una resuelva el documento *DID* de la otra, ya que el *DDO* contiene los métodos de verificación y los servicios disponibles.
  8. Lista de delegados: la entidad define una lista de usuarios confiables para la recuperación de su identidad, junto con el umbral mínimo de usuarios requerido para restaurar la llave privada.
- Credenciales verificables
  9. Generación selectiva de contenido: un *holder* específica los atributos que deben ser incluidos por el emisor en su *VC*, minimizando la divulgación de información y ajustando la credencial a cada contexto.
  10. Vigencia: un *holder* establece el período del tiempo que desea compartir una credencial.
  11. Acceso único: el *holder* comparte un enlace único y temporal para vincular la *VC* y así satisfacer la condición de vigencia establecida; una vez expira el tiempo la credencial no podrá ser verificada.
  12. Registro en la *DLT*: el *hash* de los atributos almacenados *off-chain* deben ser registrados de forma periódica en la *blockchain*.

2.2.1.4 Identificadores Descentralizados

Es un identificador único que permite asegurar canales de comunicación confiables y persistentes entre entidades [110], la dificultad de su creación se enmarca con el triángulo de *Zooko*, dilema planteado en el 2001 por *Bryce Wilcox-O'Hearn* y establece la dificultad de tener un identificador que sea simultáneamente descentralizado, seguro y legible por el humano [49]. Una de las primeras propuestas para la creación de identificadores descentralizados se tiene con el *RFC* 4122 [224], donde se presenta la especificación de un identificador único descentralizado (*Universally Unique IDentifier -UUID- o Globally Unique IDentifier -GUID-*); las dos primeras versiones de *UUID* son parcialmente centralizadas ya que requieren la dirección *MAC* de la tarjeta de red, y estas se asignan a cada fabricante mediante un control centralizado. La versión 4 utiliza números aleatorios o pseudo-aleatorios en un espacio 2^{122}; y las versiones 3 y 5 funciones *hash* para la generación de los identificadores, específicamente, la versión 3 aplica una función *MD5* y la versión 5 utiliza *SHA1*.

Estos identificadores pueden ser considerados seguros sin la necesidad de una autoridad de registro central, pero no son fácilmente legibles por el humano y, además, requieren de un tercero de confianza para la verificación de los identificadores en esquemas sin auto-autenticación [49]. Luego, con el advenimiento de las *blockchains* y sus identificadores seguros y descentralizados, se crearon servicios tipo DNS para resolver estos identificadores a nombres legibles, por ejemplo, *Namecoin*

Objetivo de diseño	Descripción
Descentralización	No se requiere de una autoridad central para la administración de los identificadores.
Control	Las entidades controlan y generan directamente sus identificadores sin depender de un tercero. Debido a la naturaleza polifacética de la identidad, una entidad podrá poseer múltiples *DID* para cada uno de sus roles y así preservar su privacidad conforme al contexto de interacción.
Privacidad	La entidades tienen el control de su información personal, incluyendo la divulgación selectiva de atributos.
Seguridad	Los *DID* se registran en *DLTs* sin dependencias tecnológicas (*ledger-agnostic*) y en los documentos *DID* se establecen los niveles de seguridad requeridos.
Basado en pruebas	Los controladores *DID* disponen de pruebas criptográficas, como firmas digitales para asegurar la titularidad y la interacción entre entidades
Visibilidad	Las entidades pueden visualizar *DID* de otras entidades para obtener información o establecer una interacción.
Interoperabilidad	Se requiere el uso de estándares interoperables para *DID* que permita la integración con librerías y software existentes.
Portabilidad	Se podrán utilizar los identificadores en cualquier plataforma que soporte *DID* y sus métodos.
Simplicidad	El diseño del *DID* debe presentar un conjunto reducido de funciones que permita una fácil comprensión e implementación.
Extensibilidad	Se debe permitir la adición de nuevas funcionalidades pero preservando la interoperabilidad, portabilidad y simplicidad.

Tabla 2.7: Objetivos de diseño propuestos para los identificadores descentralizados.
Fuente: Adaptado de [221].

[225], *Emercoin* [226] o *Ethereum Nameservice* [227], con la restricción que no existe un espacio de nombres universal que permita asignar etiquetas significativas y legibles para todos los usuarios [228].

Un identificador descentralizado -*DID*- se define como una referencia inequívoca y global a una entidad, que no requiere de un control centralizado y sin acoplamiento a organizaciones certificadoras o proveedores de servicios de identidad [221], no se puede reasignar, es permanente y verificable criptográficamente [10]. Un *DID* tiene una llave pública, la cual se comparte o registra en una *DLT*, y una llave privada para acreditar digitalmente la titularidad del identificador [181]. La recomendación para el desarrollo de *DID* se orienta en principios de diseño dirigidos hacia el usuario y la descentralización, propuestos por el grupo de trabajo en identificadores descentralizados de la *W3C*, ver Tabla 2.7; y son esenciales para el logro de los principios de identidad autogobernada.

Un *DID* hace referencia al titular de los derechos de identidad, está formado por tres elementos separados por el carácter "**:**", el primero, es *did* y determina el esquema a utilizar; el segundo, establece el método o *driver did* para la conexión, y, por último, se tiene el identificador específico generado para la entidad. Esta parametrización permite el diseñar un sistema de resolución universal para identificadores descentralizados, las aplicaciones o usuarios se conectan al servicio de resolución que integra el conjunto de métodos *DID* disponibles, donde cada plataforma deberá proveer su método *DID* de conexión. El sistema de resolución universal se encuentra en desarrollo, contiene 45 métodos *DID* habilitados[1], entre los cuales se destacan: **btcr** → *blockchain* de *bitcoin*, **sol** → *blockchain* de *Solana*, **indy** → *Hyperledger Indy*, **ion** → *ION network*, Implementación del protocolo *Sidetree* sobre la *blockchain* de *Bitcoin*, **elem** → Protocolo *Sidetree* para *Ethereum* e *IPFS*, **kilt** → Protocolo *KILT*, **ethr** → *blockchain* de *Ethereum* o llaves públicas tipo *secp256k1* y **sov** → Red pública de *Sovrin* [229]. Por ejemplo, la cadena *did:ion:EiClkZMDxPKqC9c-umQfTkR8vvZ9JPhl_xLDI9Nfk38w5w* representa un identificador descentralizado, se visualiza en color rojo el esquema, en color azul el método utilizado y en color negro el identificador específico asignado.

La arquitectura general y las conexiones entre los componentes de un sistema de identificadores

[1]Fecha de consulta: 10 de Junio de 2022

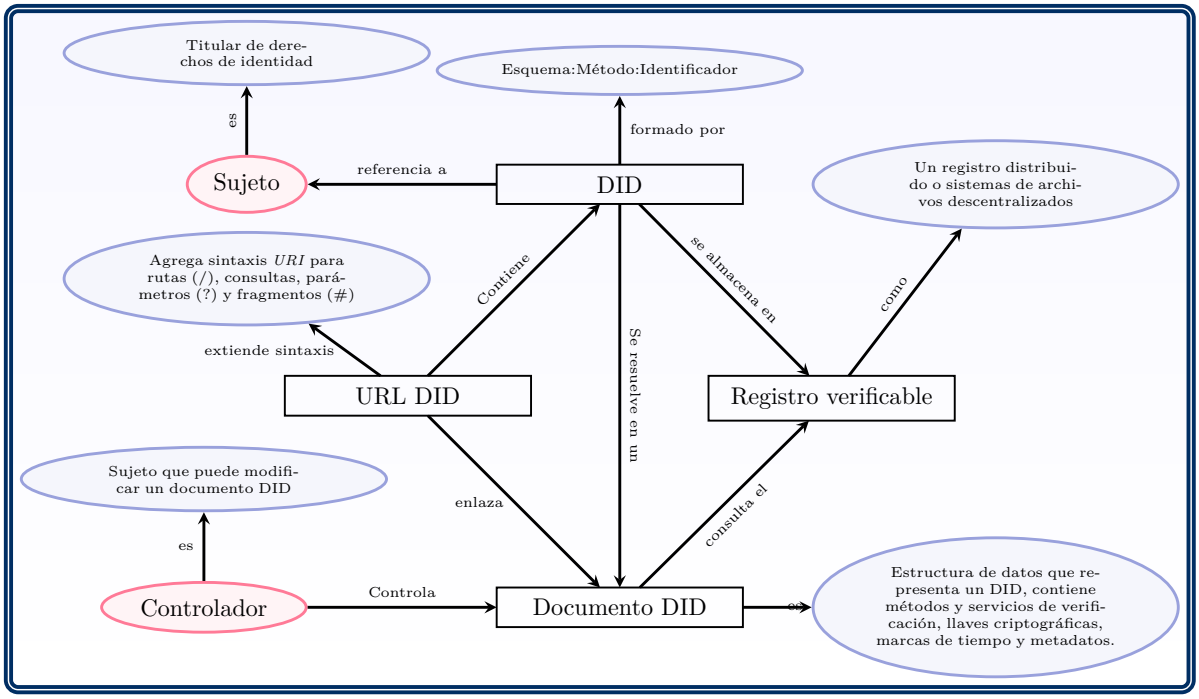


FIGURA 2.4: Arquitectura y componentes de un identificador descentralizado.
Fuente: Adaptado de [221].

descentralizados se ilustran en la Figura 2.4. *URL DID* incluye la sintaxis establecida en el *RFC3986* para la definición de un identificador uniforme de recursos -*URI*- [230].

Un *DID* se almacena en un registro de datos verificable y define la interface de comunicación y uso mediante un documento *DID*; generalmente un *JSON-LD* construido dinámicamente e integrado por seis componentes: un *DID*, material criptográfico como llaves públicas requeridos en la autenticación, los métodos criptográficos aplicados, la lista de servicios finales asociados, sellos de tiempo para evitar manipulación y la firma digital del documento [110], [181]. Los sujetos referidos en los métodos que modifican el documento *DID* son denominados los controladores, y la confianza entre controlador e identificador depende de la autoridad que define la raíz de confianza. Este control puede ser diseñado bajo tres arquitecturas: (1) administrativa, donde se dispone de un administrador que actúa como *root of trust* para vincular los métodos de autenticación con el identificador (2) algorítmica, presenta un registro como *root of trust*, por ejemplo, *blockchain* o *IPFS*, y (3) autónoma, el controlador puede crear auto-afirmaciones y firmarlas con su llave privada sin requerir un registro distribuido [10].

El código fuente 2.1 muestra un documento *DID* en formato *JSON* para el identificador *did:ion: EiClkZMDxPKqC9c-umQfTkR8vvZ9JPhl_xLDI9Nfk38w5w*. En este caso, el controlador es el mismo sujeto, define un método de verificación tipo *JSON Web Key 2020* [231] con una llave de curva elíptica y algoritmo criptográfico *secp256k1*, y dos servicios asociados: *linkedin* y *github*.

CÓDIGO FUENTE 2.1: Ejemplo Documento DID (ION).

```
1{
2        "id": "did:ion:EiClkZMDxPKqC9c-umQfTkR8vvZ9JPhl_xLDI9Nfk38w5w",
3        "verificationMethod": [
4        {
5                "id": "#someKeyId",
6                "controller": "did:ion:EiClkZMDxPKqC9c-umQfTkR8vvZ9JPhl_xLDI9Nfk38w5w",
7                "type": "EcdsaSecp256k1VerificationKey2019",
```

```
8                "publicKeyJwk": {
9                        "kty": "EC",
10                       "crv": "secp256k1",
11                       "x": "WfY7Px6AgH6x-_dgAoRbg8weYRJA36ON-gQiFnETrqw",
12                       "y": "IzFx3BUGztK0cyDStiunXbrZYYTtKbOUzx16SUK0sAY"
13               }
14       }
15       ],
16       "service": [
17       {
18               "id": "#linkedin",
19               "type": "linkedin",
20               "serviceEndpoint": "linkedin.com/in/henry-tsai-6b884014"
21       },
22       {
23               "id": "#github",
24               "type": "github",
25               "serviceEndpoint": "github.com/thehenrytsai"
26       }
27       ],
28       "authentication": [
29       "#someKeyId"
30       ]
31 }
```

De la misma forma, el código fuente 2.2 presenta los metadatos incluidos para la resolución del identificador como son: el método *DID* requerido, la ubicación del *driver*, el patrón de conexión y la conversión necesaria entre los formatos *JSON-BASED* y *JSON-LD*.

CÓDIGO FUENTE 2.2: Ejemplo Metadatos para la resolución de un DID (ION).

```
1 {
2        "pattern": "^(did:ion:(?!test).+)\$",
3        "driverUrl": "http://driver-did-ion:8080/1.0/identifiers/",
4        "duration": 979,
5        "did": {
6                "didString": "did:ion:EiClkZMDxPKqC9c-umQfTkR8vvZ9JPhl_xLDI9Nfk38w5w",
7                "methodSpecificId": "EiClkZMDxPKqC9c-umQfTkR8vvZ9JPhl_xLDI9Nfk38w5w",
8                "method": "ion"
9        },
10       "contentType": "application/did+ld+json",
11       "convertedFrom": "application/did+json",
12       "convertedTo": "application/did+ld+json"
13 }
```

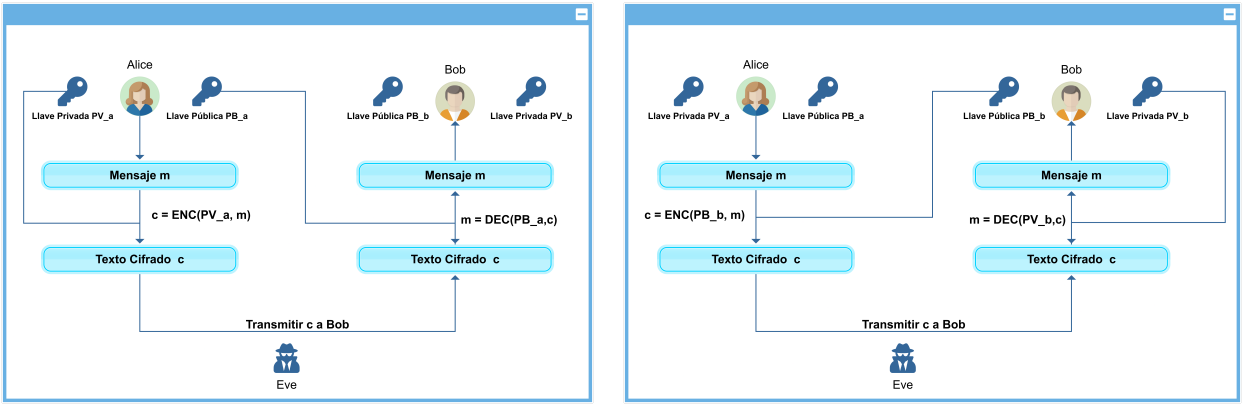
Por último, los métodos *DID* establecen como se crean, resuelven, actualizan y desactivan (*CRUD*) los correspondientes *DID*. En [110] se realiza la comparación de los métodos *did:btcr*, *did:sov*, *did:ethr*, *did:web*, *did:v1* y *did:peer*. (1) *did:btcr* se implementa sobre la *blockchain* de *bitcoin* y utiliza el campo *op_return* para devolver la referencia al documento *DID*, se gobierna de forma descentralizada y abierta conforme al protocolo de *bitcoin*, por lo tanto, las operaciones *btcr* no requieren permisos por la naturaleza pública de la *blockchain*, los cambios son propuestos por medio de un *BIP* (*Bitcoin Improvement Proposal*)[2] que será analizado y aprobado por el 95 % de los nodos mineros de los últimos 2 016 bloques, con el punto débil que los mineros con mayor poder de cómputo podrán ser más influyentes en la toma de decisiones; la especificación de *did:btcr* es cerrada a un grupo selecto de participantes. (2) *did:sov* es gobernado por un consorcio responsable de definir y actualizar las reglas y autorizar los nodos de confianza para validar transacciones. Los cambios se realizan mediante propuestas denominadas documentos controlados, que son públicos para su revisión pero de aprobación limitada a los miembros del consorcio. Implementa una *blockchain* con permisos especialmente diseñada para identidad digital, con nodos de solo lectura, llamados observadores y nodos de escritura denominados *stewards*. (3) *did:ethr* se implementa sobre la *blockchain*

[2] https://github.com/bitcoin/bips

de *ethereum* y considera la llave pública como *DID* con un registro basado en un contrato inteligente tipo ERC-1056; el gobierno de la red es democrático y descentralizado, con cambios sometidos a evaluación y aprobación de la comunidad mediante propuestas de mejora *EIP*. La especificación fue creada por *uPort*, es de acceso abierto y se encuentra bajo la administración de la *Decentralized Identity Foundation -DIF-*. Las operaciones en la red no requieren permisos pero puede ser necesario el pago de tarifas por transacción a los nodos mineros. (4) *did:web* emplea nombres de dominio como identificadores; por consiguiente, el modelo depende del esquema de gestión existente para *DNS*, el cual es susceptible de censura. La creación del *DID* asume el costo de alquilar un dominio, y su existencia depende de la renovación y de la conexión al servidor web que aloja el documento *DID*. Resolver un *DID* se realiza mediante una operación *HTTP GET* y el resto de operaciones *CRUD* se realizan mediante modificaciones al documento almacenado en un servidor web. (5) *did:v1* fue creado por el proyecto *Veres one* y opera en modo federado con un algoritmo de consenso *BFT* denominado *continuity*, que aún se encuentra en validación. La especificación es mantenida por el grupo de credenciales de la W3C; Existe una tarifa para creación o actualización de *DID*. (6) *did:peer* se enfoca en la creación de *DID any-wise* y *N-wise* para su utilización en redes *peer-to-peer*.

2.2.1.5 Autenticación

La autenticación es el proceso mediante el cual se proporcionan las credenciales apropiadas para probar la identidad de un sujeto y conceder su autorización, en caso de ser exitosa [181]. La autorización asigna los permisos necesarios conforme al rol de la entidad en el servicio requerido [31]. En los modelos de identidad autogobernada se tiene una infraestructura de llave pública descentralizada *-DPKI-*, soportada principalmente en la criptografía asimétrica y *DLT* como base para los procesos de autenticación y confidencialidad. La gestión de la llave privada es responsabilidad del usuario, mientras que la llave pública generalmente es incluida en el registro distribuido [49].



A Autenticación. B Confidencialidad.

FIGURA 2.5: Autenticación y confidencialidad mediante criptografía asimétrica.
Fuente: Elaboración del autor.

La Figura 2.5 presenta esquemas para los procesos de autenticación y confidencialidad mediante la aplicación de la criptografía asimétrica. Se presenta un escenario con tres actores: un emisor (*Alice*), un receptor (*Bob*) y un usuario malicioso (*Eve*) sobre el canal de transmisión. La autenticación (ver Figura 2.5a) requiere comprobar el origen del mensaje, para lo cual *Alice* cifra el mensaje original **m** con su llave privada y transmite el texto cifrado **c** al usuario *Bob*, quién lo descifra con la llave pública de *Alice* para comprobar la autenticidad; y para asegurar la confidencialidad (ver Figura 2.5b), *Alice* cifra el mensaje **m** con la llave pública de *Bob*, quién al recibir el texto cifrado **c** y poseer la llave privada, es el único que puede descifrarlo.

Por otro lado, el proceso de autenticación podría incluir información biométrica, por ejemplo, el protocolo *Horcrux* combina *DID* y autenticación biométrica basada en el estándar *BOPS -Biometric Open Protocol Standard-*, para dividir los datos biométricos en fragmentos y almacenarlos de forma descentralizada y redundante en sistemas *off-chain* como *IPFS* [66]. Para un uso seguro y confiable de los datos biométricos, *Rebooting the Web of Trust (RWoT)* [232] formuló en el año 2 018 seis principios para su inclusión en *SSI* [233]: (1) descentralizados: el almacenamiento de los datos biométricos debe estar descentralizado; (2) *off-chain*: no se deben almacenar en el registro distribuido por su característica de inmutable y público; (3) acceso a través de una *DLT*: se accede a los datos biométricos almacenados en un repositorio privado controlado por la entidad, por medio de un *hash* registrado en el *DLT*; (4) controlados del usuario: el control y administración de los datos biométricos siempre será del propietario; (5) confiables: los datos biométricos deben ser fiables y resistentes a fraudes; y (6) son un componente: actúan en conjunción con otros métodos del sistema para gestionar la autenticación de los usuarios.

Por último, una plataforma *SSI* debe disponer de un método para recuperación/cambio de llaves criptográficas, que le permita al usuario preservar su identidad, y, en caso de ser necesario, implementar sistemas de autenticación con firmas transitivas para mejorar el rendimiento del *BIMS*; por ejemplo, el modelo propuesto en [70].

2.2.1.6 Credenciales Verificables

Actualmente la interacción social y económica se fundamenta sobre la expedición y validación de credenciales como principal mecanismo de comprobación de identidad o de sus atributos, por ejemplo, se tiene el pasaporte para demostrar la tenencia de una nacionalidad. Una credencial verificable -*VC*- es un tipo especial de credencial digital que contiene la información del sujeto de identidad y puede tener una presentación verificable criptográficamente que es compartida para su validación [222].

La credencial verificable es una pieza de información criptográficamente confiable sobre un hecho de una entidad [181], con la misma función que la credencial física. Una *VC* esta compuesta por tres elementos: primero, un conjunto no vacío de afirmaciones, por ejemplo, nacionalidad, títulos académicos, edad o relaciones sociales; segundo, los metadatos que describen las propiedades de la credencial como: información del emisor o vigencia temporal de la credencial; y tercero, las pruebas que verifican criptográficamente la emisión o tenencia de una *VC*, marcas de tiempo y métodos de verificación [49]. Además, una *VC* debe ser descentralizada y contextualizada al caso de uso, permitiendo al emisor la selección de su contenido, verificadores independientes de los emisores con la potestad de aceptar o rechazar credenciales y un titular con la capacidad de seleccionar sus *VC* y la información que desea compartir [10]. La Figura 2.6 presenta las características de una *VC* junto con las interrelaciones de los actores involucrados. Un sistema de *VC* presenta tres roles, (1) Un sujeto Emisor que tiene la facultad de atestiguar afirmaciones sobre sujetos, por ejemplo, el gobierno, un organismo de tránsito y transporte o una universidad. El emisor genera la credencial verificable con las reclamaciones que administra y la transfiere a su respectivo poseedor, además puede revocar las credenciales cuando su integridad criptográfica esta comprometida, se cumple su fecha de vencimiento o se anula la afirmación por acciones legales. (2) Un Poseedor quién es el sujeto con los derechos sobre las *VC*, por ejemplo una persona puede tener credenciales como: pasaporte, tarjeta profesional, cédula de ciudadanía y carné de la empresa donde labora. El poseedor puede enviar directamente una credencial a un verificador o generar una presentación verificable, la cual dispone de una privacidad por diseño ya que permite realizar una divulgación selectiva de sus atributos de identidad conforme al escenario de uso, e integrar datos de multiples *VC*, aún de diferente emisor. El último actor es el (3) verificador, por ejemplo, un servicio web, agencias de seguridad gubernamentales o el departamento de recursos humanos en una organización,

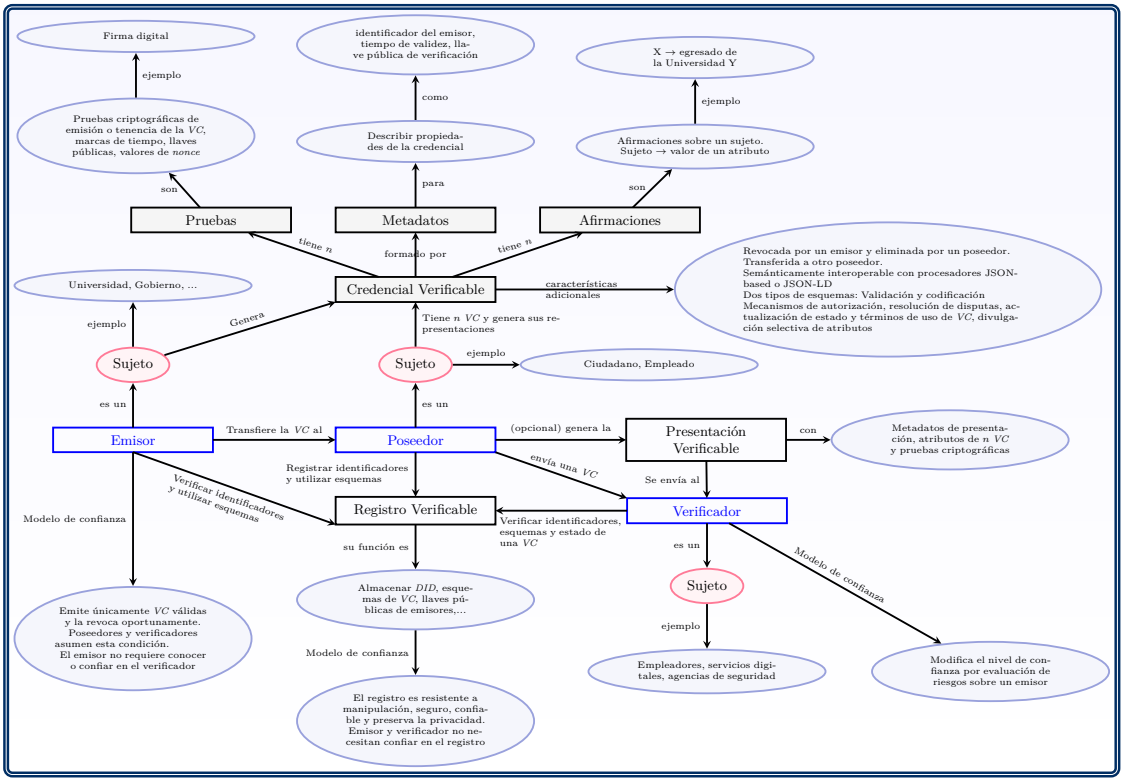


FIGURA 2.6: Actores y componentes para el intercambio de credenciales y presentaciones verificables. Fuente: Adaptado de [222].

y es responsable de realizar la comprobación criptográfica de las credenciales. Estos tres actores conforman el triángulo de la confianza, el cual se rige por el conjunto de reglas del negocio, normas legales y técnicas emitidas por una autoridad de gobernanza, y bajo las cuales funcionan las *VC* [89].

El código fuente 2.3 presenta una hipotética credencial verificable para los resultados de una prueba rápida de *SARS-CoV* [234]. La *VC* se llama *qSARS-CoV-2 IgG/IgM Rapid Test Credential*, incluye una descripción de la prueba realizada y la marca de tiempo de emisión y expiración de la prueba. El tipo es *VerifiableCredential* y *qSARS-CoV-2-Rapid-Test-Credential* definido en el documento *JSON-LD* disponible en `https://w3c-ccg.github.io/vc-examples/covid-19/v2/v2.jsonld`; el emisor es "Stanford Health Care" con *DID* en la *blockchain* de pruebas *ropsten* de *Ethereum*. Esta credencial contiene tipo, número de catálogo de la prueba, el hipervínculo al archivo pdf con el resultado; y es transferida al sujeto con *DID* específico *z6MkjRagNiMu91DduvCvgEsqLZDVzrJzFrwahc4tXLt9DoHd*. Finalmente, se agregan las pruebas criptográficas de la credencial como: tipo de firma digital, marca de tiempo de la creación y el método de verificación.

CÓDIGO FUENTE 2.3: Ejemplo de credencial verificable.

```
1 {
2         "@context": [
3         "https://www.w3.org/2018/credentials/v1",
4         "https://w3c-ccg.github.io/vc-examples/covid-19/v2/v2.jsonld"
5         ],
6         "id": "http://example.com/credential/123",
7         "type": [
8         "VerifiableCredential",
9         "qSARS-CoV-2-Rapid-Test-Credential"
10        ],
```

```
11          "issuer": {
12                  "id": "did:elem:ropsten:EiBJJPdo-ONF0jxqt8mZYEj9Z7FbdC87m2xvN0_HAbcoEg",
13                  "location": {
14                          "@type": "CovidTestingFacility",
15                          "name": "Stanford Health Care",
16                          "url": "https://stanfordhealthcare.org/"
17                  }
18          },
19          "issuanceDate": "2019-12-11T03:50:55Z",
20          "expirationDate": "2020-12-11T03:50:55Z",
21          "name": "qSARS-CoV-2 IgG/IgM Rapid Test Credential",
22          "description": "Results from antibody testing should not be used as the sole basis to
                diagnose or exclude SARS-CoV-2 infection. False positive results may occur due to
                cross-reacting antibodies from previous infections, such as other coronaviruses, or
                from other causes Samples with positive results should be confirmed with alternative
                testing method(s) and clinical findings before a diagnostic determination is made.",
23          "credentialSubject": {
24                  "id": "did:key:z6MkjRagNiMu91DduvCvgEsqLZDVzrJzFrwahc4tXLt9DoHd",
25                  "type": [
26                  "qSARS-CoV-2-Rapid-Test-Credential"
27                  ],
28                  "catalogNumber": "5515C025, 5515C050, 5515C100",
29                  "ifu": "https://cellexcovid.com/wp-content/uploads/2020/04/Cellex-rapid-ifu.pdf",
30                  "assay": "Negative"
31          },
32          "proof": {
33                  "type": "Ed25519Signature2018",
34                  "created": "2020-04-18T18:35:13Z",
35                  "verificationMethod": "did:elem:ropsten:EiBJJPdo-
                        ONF0jxqt8mZYEj9Z7FbdC87m2xvN0_HAbcoEg#xqc3gS1gz1vch7R3RvNebWMjLvBOY-
                        n_14feCYRPsUo",
36                  "proofPurpose": "assertionMethod",
37                  "jws": "eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..
                        xnB7m8M6TcAFmz2efqb74IyJECUTAMpCkJAudfmVkLC3CPmCrMznvlD2E7
                        WCCkzF9nnrZlJw0VpHdXJpjEU-AQ"
38          }
39}
```


2.2.1.7 Almacenamiento

La persistencia de la información en un sistema *SSI* se divide en dos componentes, datos almacenados en un *DLT (on-chain)* y datos guardados en repositorios externos *(off-chain)*. La componente *On-chain* establece una relación de confianza para gestionar la identidad digital sin requerir un tercero de confianza [1], dadas sus características como anonimato o pseudo-anonimato, transparencia, privacidad, inmutabilidad y confiabilidad [92]. El *DLT* preserva un registro de los identificadores descentralizados y visibiliza las llaves públicas requeridas para el proceso de autenticación, permitiendo el despliegue de una infraestructura de llave pública descentralizada *-DPKI-*; además ofrece un servicio de notariado para las credenciales verificables, asignación y control de permisos de acceso y uso de contratos inteligentes para automatizar las reglas del negocio [181]. El almacenamiento *off-chain* está orientado a preservar la privacidad del usuario, para lo cual se despliegan agentes que preservan la información privada del usuario ya sea en dispositivos como teléfonos inteligentes, computadores personales o repositorio externos en la nube [49]. Este control en el almacenamiento favorece la interoperabilidad puesto que posibilita al titular la utilización de sus datos entre múltiples plataformas y con diferentes propósitos [181].

2.2.2 Arquitecturas propuestas para *SSI*

Dado el conjunto de publicaciones determinado mediante la revisión sistemática de la literatura aplicada, las plataformas para *SSI* se han clasificado en dos categorías; la primera comprende las

soluciones orientadas a un caso de uso específico, y la segunda se refiere a meta-sistemas de identidad (ver capítulo 3), los cuales permiten construir sistemas de identidad descentralizada interoperables que reducen la complejidad de las aplicaciones mediante la exposición de una interfaz unificada que facilita el acoplamiento de la identidad digital [10].

2.2.2.1 Principios y componentes básicos a nivel de arquitectura

El proyecto *DECODE -DEcentralized Citizen Owned Data Ecosystems-* define un entorno para la administración de datos centrado en el usuario, con una arquitectura diseñada sobre siete principios: (1) licencias de libre uso y código abierto; (2) modularidad e interoperabilidad en una estructura multicapa; (3) reusar y no re-inventar; (4) descentralización; (5) privacidad por diseño conforme con *GDPR*; (6) facilidad de uso; y (7) determinismo para garantizar la integridad de los datos y la consistencia de las transformaciones criptográficas [200], [200]. Por otra parte, en [100] se definen cuatro componentes básicos para una arquitectura *SSI*: (1) Afirmaciones, (2) identificadores descentralizados, (3) credenciales verificables y (4) almacenamiento de datos *off-chain* y *on-chain*. Además, en [31] se contemplan dos componentes adicionales (5) infraestructura de llave pública descentralizada (DPKI) y (6) registro de datos verificables. Asimismo, un modelo para *SSI* debe permitir la interacción de tres tipos de usuarios: (1) emisor de credenciales verificables, (2) titular de derechos de identidad, quién será el receptor de las credenciales emitidas, y (3) el verificador responsable de validar las credenciales existentes [62].

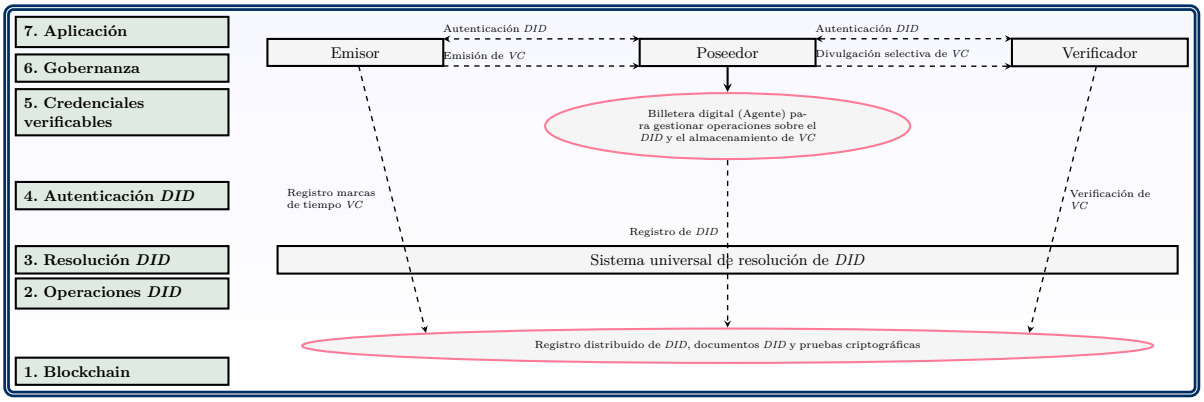


FIGURA 2.7: Arquitectura de alto nivel compuesta por siete capas para el despliegue de una identidad autogobernada.
Fuente: adaptado de [103].

Por otra parte, en la Figura 2.7 se ilustra el diagrama de arquitectura para *SSI* propuesta en [103], la cual está compuesta por siete capas, con un flujo de información entre los actores conforme al estándar para identificadores descentralizados (ver sección 2.2.1.4, página 19) y credenciales verificables (ver sección 2.2.1.6, página 24). La primera capa denominada *blockchain* hace referencia a la existencia de un registro descentralizado para la vinculación de *DID* y sus respectivos documentos; este registro preserva las evidencias criptográficas de las afirmaciones realizadas sobre los sujetos. La segunda capa, denominada operaciones *DID*, es responsable de las modificaciones sobre un *DID* establecidas en el respectivo método *DID*; la tercera capa, se orienta a la integración de soluciones *SSI* y permite la conexión con un servicio de resolución universal de identificadores descentralizados mediante la implementación de *drivers* nativos para cada plataforma *SSI* [90]; la cuarta capa describe los métodos de autenticación establecidos entre los actores; la quinta capa se centra en la emisión, validación, almacenamiento y revocación de credenciales verificables; la capa sexta indica la necesidad de definir un marco de gobernanza que propenda por garantizar la seguridad, confianza y lógica de cada caso de uso; y, por último, una capa de aplicación que deberá

integrar en sus desarrollos, la experiencia de usuario (*UX*) y el diseño de la interfaz (*UI*) de las billeteras digitales. Es importante resaltar que la autenticación mencionada en la cuarta capa y su posterior autorización se realiza en función de las llaves públicas, llegando a requerir por parte de los proveedores de servicios la implementación de librerías de integración que la soporte.

Finalmente, un sistema de identidad digital se puede complementar con modelos de reputación para cuantificar la calidad de las identidades. Por ejemplo, un modelo podría incluir un atributo para la reputación del usuario que se calcule al sumar la puntuación de todos sus atributos, y de esta manera incentivar la creación de una única identidad. En [158] se presenta un modelo de reputación basado en atributos cuyo valor inicial es $n * v_a$, donde n es la cantidad de atributos del usuario y v_a es un número natural. El valor de v_a es dinámico, se reduce ante operaciones que pueden afectar la confianza. Por ejemplo, un cambio de valor del atributo afecta en v_b la reputación, y restringe el número de cambios a un máximo de $\frac{v_a}{v_b}$, ya que un valor de cero para v_a anula el atributo, y se incrementa por relaciones de confianza entre pares que se generan cuando un usuario autoriza la consulta de un atributo.

2.2.2.2 Casos de uso que implementan gestión de identidad digital basada en *blockchain*

2.2.2.2.1 Administración de activos digitales: Se presentan dos casos de aplicación, uno orientado al cálculo de impuestos sobre la venta de inmuebles, y el segundo diseñado para monetizar los derechos de autor sobre material multimedia. El sistema para administrar la propiedad digital de activos y el pago de impuestos se basa en contratos inteligentes de *ethereum*, utiliza una dirección de esta *blockchain* para identificar a los usuarios y el modelo de privacidad propuesto por *Nakamoto* en *bitcoin*. El proceso para transferir la propiedad de un activo consta de seis pasos. (1) Se requieren tres actores, vendedor, comprador y testigo, quienes deben validar físicamente su identidad digital a partir de un documento oficial y sus datos biométricos, es decir, el sistema no da confianza sobre la identidad digital del usuario, la cual solamente se reconoce una vez sea aprobada por un tercero de confianza. El identificador de un actor es su dirección pública en *ethereum*. Además, el contrato inteligente contiene un listado de los activos que posee un usuario, (2) el contrato inteligente valida la identidad de los actores, (3) se verifica que el activo objeto de la venta sea propiedad del vendedor, (4) calcula el impuesto de la venta conforme a un porcentaje que se parametrizó, (5) elimina el activo de la lista de propiedades del vendedor y (6) lo agrega en la lista del comprador [105]. El segundo caso es una arquitectura basada en tres capas para administrar archivos de multimedia como texto, audio, vídeo o imágenes. La capa de servicio es responsable de las operaciones *CRUD* sobre los *DID*, provee la interface para agregar o retirar material multimedia y controlar/tokenizar el acceso al mismo. La segunda capa se encarga del almacenamiento *off-chain* de los archivos multimedia y de los certificados que autorizan su uso; y la última capa implementa el registro distribuido junto con los contratos inteligentes que automatizan la distribución de regalías. La implementación de la prueba de concepto utilizó *DID* basados en el estándar *ERC1056* para el registro de identidades digitales basadas en *blockchain*, *Parity* perteneciente al ecosistema *ethereum* para el despliegue de una *blockchain* federada, *Solidity* en la implementación de los contratos inteligentes e *IPFS* para la persistencia *off-chain* [78].

2.2.2.2.2 Autenticación con soporte para datos biométricos: Como se mencionó en la sección 2.2.1.5, los datos biométricos pueden ser utilizados como un factor adicional en procesos de autenticación. A continuación se presentan las aplicaciones *Horcrux* y *BlockID* que aplican este enfoque. *Horcrux* es un protocolo que implementa un método descentralizado para autenticación basado en datos biométricos conforme al estándar 2410-2017 *biometric open protocol standard -BOPS-* de

la *IEEE*. Los datos biométricos de autenticación son almacenados en repositorios descentralizados bajo el control del usuario, y se acceden por referencias almacenadas en una *blockchain*. El estándar *BOPS* permite la portabilidad e interoperabilidad de la información biométrica, para lo cual define plantillas y métodos para la recolección de datos biométricos, formatos para almacenamiento seguro y fragmentación criptográfica, métodos *REST* para su consulta y procesos para la validación de las plantillas. La inscripción de un usuario se realiza en dos pasos, primero, el servidor de *BOPS* genera el par de llaves criptográficas (*RKP*), y envía la llave pública a la *wallet* del usuario, y luego, se carga la plantilla biométrica inicial para producir un nuevo par de llaves (*LPK*) mediante el módulo de seguridad de *hardware* del teléfono inteligente. La llave privada de *LPK* se almacena localmente y la llave pública de LPK junto con los datos biométricos se cifran con la clave pública de *RPK* para generar el *DID* que será registrado en la *blockchain*, mientras que el documento *DID* respectivo se almacenará *off-chain*. El *DID* identifica a un usuario y puede ser resuelto por un servidor *BOPS* que actúa como verificador [66]. La segunda aplicación fue denominada *BlockID*, y realiza la autenticación del usuario mediante la combinación de datos biométricos, información registrada en un documento de identidad oficial y una llave pública. El diseño de *BlockID* se orientó principalmente a la gestión de identidad en la cadena de suministro, aunque su aplicación no se limita a este contexto o a una *blockchain* en específico. *BlockID* contempla cuatro actores: (1) usuario, que representa las personas involucradas en la cadena de suministro, por ejemplo conductores, (2) teléfono inteligente, almacena la identidad del usuario, quién es responsable de su administración y seguridad, (3) creador de identidad, en un tercero de confianza que centraliza la creación de las identidades que serán registradas en la *blockchain* y es responsable de crear la identidad de todos los usuarios y (4) administrador de identidades, conformado por un conjunto de nodos responsables de validar las transacciones relacionadas con la identidad en la *blockchain*. El modelo se compone de dos módulos, uno de creación y otro de administración. La habilitación de una identidad digital requiere que el usuario disponga de un documento oficial de identidad emitido por un gobierno, disponga de un teléfono inteligente con soporte para autenticación por biometría y presentarse físicamente ante el creador de identidad para la validación de datos y generar el par de llaves que conforman la identidad; el módulo de administración asigna y revoca miembros del conjunto de nodos confiables, quienes son responsables de verificar las transacciones, registrar en la *blockchain* los certificados generados para las nuevas identidades y revocarlos cuando un usuario se retira de la compañía o pierde el acceso a su dispositivo [68].

2.2.2.2.3 Modelos de credenciales verificables: *Stokkink et al.* proponen en [72] dos modelos de reclamaciones para identidad autogobernada. El primer modelo 1 presenta afirmaciones genéricas comprobables que aplican pruebas de conocimiento cero para proteger los atributos del usuario y realizar una divulgación selectiva de información. Los *claims* son independientes de una *blockchain* en particular, con el objeto de tener portabilidad e interoperabilidad, y su esquema de metadatos está compuesto por cinco campos: (1) nombre del atributo, el cual debe ser estandarizado por el esquema de gobernanza de la red, (2) marca de tiempo del instante en el que se generó para evitar la manipulación y detectar fraudes, (3) vigencia, determina el intervalo de tiempo en el cual es válida la afirmación, (4) formato de la prueba criptográfica, donde se determina el método de comprobación criptográfico utilizado, y (5) enlace o referencia de la prueba para garantizar la comprobación de los metadatos por parte de un tercero. Por otro lado, el segundo modelo construye una cadena de afirmaciones, las cuales constan de tres niveles auditables y escalables para el uso de las afirmaciones, proporcionando al sistema de la transparencia y persistencia requerida para un contexto legal de la identidad digital. El primer nivel es el pasivo, permite enviar a la *blockchain* una afirmación genérica comprobable, compuesta por los metadatos de identificación y las firmas de un tercero que atestigüe (opcional) y del titular (requerida), pero el bloque únicamente se registrará cuando sea detectada la primera validación. El siguiente nivel es basado en intención y genera un

registro para la detección de fraude, agrega al bloque del nivel pasivo metadatos para identificar la intención y una doble firma realizada por un verificador y el titular. Este bloque permite validar la consistencia en las marcas de tiempo de creación o revocación de afirmaciones. Por último, el nivel activo es responsable de revocar identidades o afirmaciones comprometidas, para lo cual requiere una comunicación sincrónica con los terceros de confianza, quienes deben resolver una prueba única que demuestre su integridad. Este modelo se implementó para la creación de un pasaporte Alemán digital y descentralizado, utilizando la *blockchain* de *Trustchain* [235].

2.2.2.2.4 Vinculación de nuevos usuarios: Las organizaciones se enfrentan al requerimiento de validar la identidad de un nuevo usuario con el objeto de ajustarse a normas como anti-lavado de activos, prevenir la financiación del terrorismo o la evasión fiscal; esta validación cada vez demanda un número mayor de recursos como tiempo y dinero [84]. *BBM*, *Casper* y *KYC2* definen casos de uso sobre un proceso de *KYC* en el sistema financiero, pero restringen la existencia del usuario a la aprobación de un tercero confiable en un proceso de verificación manual y presencial. *BBM* es un modelo de identidad autogobernada aplicado a la banca abierta utilizando el meta-sistema *uPort* (ver sección 3.2, página 38) como *middleware*. La arquitectura presenta cuatro capas: (a) capa de aplicación, establece la interfaz de comunicación entre usuarios y define los servicios de integración entre bancos y los productos financieros disponibles; (b) capa *uPort*, contiene la billetera *wallet* que permite generar las llaves criptográficas del nuevo usuario y vincula los contratos inteligentes *proxy* y controlador originales, pero alteró el contrato de registro y el método para la recuperación de llaves. *BBM* modificó la creación de usuarios en *uPort* para agregar la validación física de la identidad por parte de un tercero confiable, por ejemplo, una institución financiera, y, en caso de una aprobación correcta, se generará el *uPortID* de la cuenta y se procederá a su activación. Este paso extra permite simplificar la actualización de llaves sustituyendo la lista de contactos de recuperación por el verificador de identidad confiable; (c) capa de red y *blockchain*, se despliega sobre *ethereum*, ya que es la *DLT* utilizado por *uPort*; y (d) capa de datos para almacenar la información sensible en repositorios *off-chain* [107]. *Casper* es una plataforma *SSI* basada en *blockchain* con métodos *ZKP* para verificar los atributos en las identidades. La arquitectura de *Casper* presenta dos tipos de usuarios, un administrador que emite o verifica *VC* y un titular de las *VC*; y consta de cuatro capas: (1) El almacenamiento de la información personal se realiza en el teléfono inteligente del mismo usuario y en la *blockchain* se registran los *DID* y las transacciones de consentimiento o revocación de permisos. La prueba de concepto utilizó la *blockchain Rahasak* [236]; (2) una capa de contratos inteligentes para crear la identidad, asignar permisos sobre las credenciales verificables y notificar al usuario sobre los eventos que sucedan; (3) una capa de credenciales verificables que realiza la validación mediante las pruebas criptográficas registradas en la *DLT*; y por último, (4) la capa de comunicación entre pares permite el intercambio de información. Se implementó un caso de uso para modelar un proceso *KYC* entre bancos, donde se requiere un administrador para habilitar la *wallet* del banco y otorgarle permisos como nodo validador de la *blockchain*. El usuario crea la identidad digital en su *wallet* pero requiere una validación física por parte del banco para su aprobación y establecer así una relación de confianza [85]. *KYC2* propone un marco para la incorporación de nuevos clientes en un grupo de entidades financieras relacionadas, presenta dos actores, banco y cliente, cada uno con su respectiva *wallet* donde se almacena la información privada, y una *DLT* federada tipo *Hyperledger Indy* para proporcionar la infraestructura descentralizada de llave pública, y es administrada por los bancos que forman la red. El registro de un nuevo cliente requiere para su aprobación, la validación física de la documentación del cliente por parte de uno de los bancos asociados. Una vez es habilitado, el usuario genera una *VC* de identificación, la cual es aceptada para vincularse como cliente en otra entidad financiera adscrita a la *blockchain* sin necesidad de realizar otra validación *KYC*. El sistema supone que la comprobación física de la identidad del usuario ha sido realizada correctamente, creando confianza en la credencial verificable de identidad

que se emitió, y permitiendo a las otras entidades omitir el proceso *KYC* para la vinculación de un nuevo cliente validado previamente por otra institución [84].

2.2.2.2.5 Servicio de validación de identidad: *SSI* proporciona un servicio de proveedor de identidad (*IdP*) descentralizado o el acomplamiento con *IdP* existentes para permitir la comprobación y autorización de usuarios en un servicio dado. A continuación se presentan cuatro ejemplos de estos escenarios. El primero, *DNS-IdM* permite integrar un servicio de identificación establecido, *WiP* facilita la autenticación de usuarios para proveedores de servicios en la nube, *BPDIMS* se enfoca en el intercambio controlado de datos con un proveedor de servicios y *ATIB* crea un servicio tipo *gateway* para interactuar con un *SP*. *DNS-IdM* incorpora la funcionalidad de un *DNS* para que un proveedor de servicios vincule y valide la identidad digital de un usuario. La arquitectura despliega dos *blockchains* independientes, la primera es una red *ethereum* privada para registrar las interacciones entre clientes y proveedores de servicios, y la segunda es una *blockchain* sin permisos que conserva el *hash* de los atributos del usuario y la referencia a su almacenamiento cifrado en un servidor *IPFS*, registra los identificadores y las llaves públicas de los clientes. El diseño requiere implemenar dos tipos de billeteras, una para el cliente y otra para los proveedores de servicio. La creación de una identidad se realiza desde la billetera del cliente, y ejecuta un contrato inteligente que se conecta con un proveedor de identidad predefinido, quién valida y autoriza su escritura en el *ledger* privado. Una vez se crea la identidad, el cliente puede agregar sus atributos al *ledger* público, previa aprobación y validación por parte de un tercero de confianza. Cada atributo tiene un tipo asignado con un contrato inteligente especializado responsable de su verificación, proceso que realiza mediante un contrato inteligente tipo *DNS* que resuelve el contrato adecuado para cada atributo y establece la comunicación entre las dos *blockchains* con la ruta exacta del contrato de verificación requerido [61]. El segundo, *WiP* plantea un modelo de confianza basado en *blockchain* que le permite a los proveedores de servicios en la nube -*CSP*- verificar de forma dinámica y distribuida la identidad de los usuarios. La arquitectura contempla tres entidades: (a) usuario, la entidad que requiere acceder a múltiples *CSP*; (b) un *CSP* que ofrece servicios y recursos a los usuarios, con el despliegue de un *CSP* especial denominado *CSP home* responsable de generar la identidad del usuario creando un token de acceso con su respectivo registro en la *blockchain*, para su utilización en la identificación y autenticación. El token contiene la información de los recursos permitidos al usuario; finalmente, (c) la plataforma de gestión de confianza -*TMP*- conformada por el registro distribuido, donde los nodos mineros son los diferentes *CSP* y validan la transacción de autenticación verificando el token del usuario y, en caso de aprobación, permiten el acceso a los recursos conforme a los permisos establecidos. El consenso de la red aplica un algoritmo de prueba de participación combinado con un sistema de reputación para los *CSP* [64]. Y, en tercer lugar *BPDIMS*, un diseño conceptual para la administración de identidad y datos personales basado en *blockchain*, centrado en el usuario y compatible con *GDPR*, que permite un empoderamiento del titular de los derechos de identidad, transparencia en el uso de la información que posibilita el consentimiento para su comercialización, y dispone de un almacenamiento protegido criptográficamente. La arquitectura define cuatro roles: (1) usuario, (2) proveedor de servicio, (3) comprador de datos y (4) validadores o curadores de datos. Además, la información se divide en dos tipos de datos: (1) estáticos, referentes a atributos de identidad bajo el control del titular y (2) dinámicos, asociados a datos generados por la interacción del usuario con un proveedor de servicio. Finalmente, la propuesta presenta cinco capas: (1) contratos inteligentes que definen las reglas para el intercambio de información entre usuarios y proveedores de servicios, (2) *blockchain* de acceso que autoriza la comunicación del usuario con la capa de persistencia y permite otorgar permisos a un proveedor de servicio, (3) *blockchain* de identidad para registrar el *hash* de los datos verificados y permitir su comprobación por parte de terceros, (4) persistencia de los datos en un repositorio *off-chain* externo lo que permite el cumplimiento *GDPR* respecto al derecho a eliminar información y revocar autorización de acceso, y

(5) interfaz de usuario para visualizar los datos almacenados y su administración [69]. Por último, *Grüner* et al. han propuesto un esquema de integración similar a un *gateway* para autenticación y autorización basada en atributos, que integra plataformas *SSI* como *uPort* (ver sección 3.2, página 38) y *Jolocom* (ver sección 3.3 con un proveedor de servicios [90]); este sistema fue la base para *ATIB* que integra un *SSI* intermediario con una combinación de atributos de diferentes fuentes [88]. El sistema presenta cinco componentes, (1) un usuario que atestigua una dirección de correo electrónico y obtiene una *VC* sobre su *e-mail* que lo activa en el sistema; (2) un servicio que traduce el nombre de una afirmación entre dominios conforme al esquema de credencial definido en cada contexto y lo estandariza conforme a los nombres propuestos en *Open ID connect - OIDC* [237]; (3) un controlador que implementa un conjunto de protocolos soportados para la integración con la aplicación web del proveedor de servicios, por ejemplo, *OIDC*; (4) un *Broker SSI* que proporciona una interfaz estandarizada para la comunicación con las plataformas *SSI*; y, finalmente, (5) un motor de confianza para comprobar la validez de las afirmaciones en una solicitud de autenticación. *ATIB (Attribute Trust-enhancing Identity Broker)* actúa igual que su predecesor como un proveedor de identidad sin almacenar *PII*, permite la autenticación desde la *wallet SSI* del usuario en una aplicación de un proveedor de servicios y autorizarlo para el intercambio de *VC*. *ATIB* presenta los mismos cinco componentes, adicionando la posibilidad de utilizar diferentes modelos de confianza, se agregó el protocolo *SAML2* [238], una interfaz genérica que abstrae la funcionalidad de cada plataforma *SSI*, por el momento soporta *uPort*, *Jolocom* , página 39) y *Hyperledger Aries*; y proporciona interfaces de administración y comunicación para cada uno de los componentes [88].

2.2.2.2.6 *SSI* aplicado a salud pública: *Connect* permite una *SSI* basada en la *blockchain Rahasak* para informar la proximidad física con casos positivos para COVID-19. *Rahasak* es una *blockchain* diseñada bajo una arquitectura de microservicios, con soporte para transacciones en tiempo real, analítica de datos y aprendizaje de máquina [236]. El uso de *DID* preserva la privacidad del individuo, facilitando el registro de sus movimientos en una *blockchain*, y así mejorar la eficiencia del cerco epidemiológico y el retorno seguro a la normalidad. *Connect* requiere dos billeteras digitales, una de usuario y otra para los terceros que supervisan los posibles focos de retransmisión del virus, como aeropuertos, hospitales o empresas. La *wallet* del usuario genera el *DID* y recolecta atributos básicos a partir de documentos oficiales de identidad, otorga permisos a terceros y recibe alarmas sanitarias. La *wallet* de las entidades solicita a través de un código *QR* la asignación de permisos para seguimiento de la ubicación del usuario y así poder notificarle un riesgo de contagio en el momento que un usuario sea diagnosticado positivo para COVID-19. Esta plataforma tiene cuatro capas, (1) *DLT* para registrar *DID* y pruebas de actividad personal (2) capa de comunicación entre pares para el intercambio de información entre billeteras digitales, (3) creación, intercambio y verificación de credenciales y (4) la capa de seguimiento del usuario para detectar el posible contagio por proximidad física con un infectado en los últimos catorce días [87].

2.2.2.2.7 Privacidad en la Internet: Una de las promesas de *SSI* es la soberanía de los datos de identificación personal, que se evidencia en los principios de identidad autogobernada. *TrustChain Identity* (*TCID*) está orientado a la auto-soberanía, credibilidad y anonimato a nivel de red. La soberanía permite el control de la identidad y minimiza la exposición de datos mediante el uso de credenciales verificables con piezas de información, sin requerir un comunicación directa entre verificador y emisor, tal como sucede en el mundo físico. La información del usuario es almacenada en su *wallet*. La credibilidad se soporta en las pruebas de identidad obtenidas mediante firmas digitales contenidas en las *VC* y procesos de autenticación de usuarios que vinculen al usuario con un dispositivo físico, y el anonimato en la red, que es el factor diferenciador en este modelo, se obtiene por una comunicación entre pares mediante la implementación adaptada de los protocolos *TOR* y *GOSSIP*, lo que protege al usuario de adversarios que analizan el tráfico de la red en la

búsqueda de patrones que permitan una correlación de la identidad [4].

2.2.2.2.8 *SSI* para la Internet de las cosas: Gestionar la identidad digital de los dispositivos *IoT* es un requerimiento fundamental para generar confianza sobre los datos generados por estos. En [63] se analizan cuatro aspectos claves para administrar la identidad digital basada en *blockchain* para la Internet de las cosas. En primer lugar, el control de acceso basado en *DLT* elimina la necesidad del tercero de confianza centralizado que administra las políticas de acceso a los dispositivos *IoT*, además proporciona un registro auditable de eventos; en segundo lugar, facilita preservar la privacidad de los datos sensibles como atributos de identidad, ubicación o mediciones de los sensores y permite minimizar la divulgación de información; en tercer lugar, genera confianza en el origen de los datos y permite un almacenamiento distribuido, inmutable y resistente a censura o manipulación. Por último, se debe tener en cuenta el desempeño de la *blockchain* medido en la escalabilidad sujeta al algoritmo de consenso y en las limitaciones de diseño establecidas por las restricciones de almacenamiento, procesamiento, comunicaciones y autonomía de los dispositivos. Finalmente, en [81] se presenta una arquitectura para gestionar la identidad digital de dispositivos *IoT* soportada en *blockchain*. El diseño plantea una *DLT* separada para las operaciones de registro, autenticación y revocación, ya que realizar estas operaciones de forma paralela permite una mayor escalabilidad. El sistema consta de cinco componentes: (1) el protocolo de identidad responsable del registro, revocación y validación de *DID* del dispositivo; (2) un servicio de membresía para asignar o retirar nodos validadores de la *blockchain* federada construida con *Hyperledger Fabric*; (3) un conjunto de políticas para el uso de la red definido y aprobado por el consorcio de gobierno; (4) los contratos inteligentes de *chaincode* para implementar las políticas junto con la lógica del negocio y (5) un algoritmo de consenso para garantizar la integridad y confiabilidad del sistema basado en el servicio de ordenamiento del flujo de las transacciones en *Hyperledger Fabric*.

Además, en la Tabla 2.8 se sintetizan los casos de uso relacionados anteriormente, desde la perspectiva de la arquitectura en siete capas presentada en la Figura 2.7.

Caso de Uso	***Capas***						
	DLT Blockchain	**Operaciones *DID***	**Resolución *DID***	**Autenticación *DID***	**Credenciales verificables**	**Gobernanza**	**Aplicación**
Liquidación de impuestos [105]	*ethereum*	✗	✗	✗	✗	Validación presencial de la identidad de los usuarios.	*Wallet* y *smart contract* bajo *Solidity*
Derechos de propiedad para archivos multimedia [78]	parity	✓ ERC-1056 Ethereum Lightweight Identity	✓ compatible con *Universal Resolver*	✓ Registro *DID*	✗	se genera un certificado de registro para cada obra multimedia que contiene los permisos.	Desarrollado con *Node.js*, *API RESTful*, *Solidity* y JSON Web Token.
Horcrux [66]	*blokchain-agnostic*	✓ *DID* 1.0 de la *W3C*	✓ un BOPS server resuelve el *DDO*	✓ Registro *DID* con perfil biométrico	✗	Se administra un listado de proveedores de servicios verificados, pero los usuarios se registran libremente	Servidor *BOPS* bajo el estándar IEEE 2410-2017 con conexión mediante una aplicación móvil.
BlockID [68]	*blokchain-agnostic*	✗	✗	✗ Se utiliza un perfil biométrico	✗	Validación presencial de la identidad de los usuarios.	Uso del hardware biométrico de un dispositivo móvil. Se presenta el modelo conceptual.

Continúa en la siguiente página

Tabla 2.8 – continuación de la página anterior

Caso de Uso	*Capas*						
	DLT Blockchain	**Operaciones *DID***	**Resolución *DID***	**Autenticación *DID***	**Credenciales verificables**	**Gobernanza**	**Aplicación**
Modelo de *VC* para pasaporte digital [72]	*t*rustchain	✗	✗	✗	☑ *VC* con pruebas de conocimiento cero interactivas y no interactivas	Dada por el algoritmo de consenso de la *DLT*	Se desarrollaron *wallets* en *python* y *java*.
BBM [107]	*u*Port	☑ *DID* 1.0 de la *W3C*	☑ compatible con *Universal Resolver*	☑ Registro *DID*	✗ *VC* conforme al modelo establecido por *uPort*	Validación presencial de la identidad de los usuarios.	se requiere una *Wallet* para cada tipo de usuario. Se presenta el modelo conceptual.
Casper [85]	*r*ahasak	☑ el *DID* es la llave pública base 58 y se registra la prueba de identidad en la *DLT*	☑ Utiliza la prueba *DID* para comprobación	☑ registro distribuido de pruebas de identidad	*VC* anónimas con *ZPK*	Validación presencial de la identidad de los usuarios.	Una Wallet en el teléfono inteligente almacena la información sensible junto con la llave privada
KYC2 [84]	*H*yperledger Indy	☑ *DID* 1.0 de la *W3C*	☑ Método KYC2 compatible con *Universal Resolver*	☑ registro de *DID* que opera como una *DPKI*	*VC* anónimas con *ZPK*	Se requiere validación presencial de la identidad de los usuarios y administrar los nodos mineros (bancos en este caso)	Dispone de una *Wallet* para cada tipo de usuario. Se presenta el modelo conceptual.
DNS-IdM [61]	*e*thereum	✗ basado en direcciones tipo ethereum	✗	✗	✗ Validación y presentación de atributos por contratos inteligentes	Diseñar un contrato inteligente para cada atributo y administrar la lista de proveedores de identidad	Dos *DLTs*, una pública para el hash de los atributos y otra privada exclusiva para clientes y *SPs*
WiP [64]	*H*yperledger Fabric	✗	✗	✗ se realiza mediante un token de acceso creado por un nodo especial llamando *Home CSP*	✗	El consenso lo realiza un consorcio dinámico de *CSPs* en un esquema denominado plataforma de gestión de confianza.	Se presenta el modelo conceptual.
BPDIMS [69]	*blokchain-agnostic*	✗	✗	✗	✗ El intercambio de atributos se da mediante contratos inteligentes.	Los datos del usuario se clasifican en dinámicos y estáticos	Se presenta el modelo conceptual.
ATIB [88]	*N*o aplica. Usa un *SSI Wrapper*	✗ obtenidas de una plataforma externa	☑	☑ adiciona la resolución de una prueba	☑ Se envía al e-mail del usuario la *VC* de acceso.	Es un *IdP* para aplicaciones web que se conecta a una plataforma *SSI*	Se implementa con *pyhton* bajo el *framework* Tornado y usa *wrappers* para *uPort* y *Jolocom*
Connect [87]	*r*ahasak	☑	☑	✗ Se basa en JSON Web Token.	✗	Se debe escanear un código *QR* en el sitio que realizará la trazabilidad del usuario	Aplica una arquitectura de micro-servicios

Continúa en la siguiente página

Tabla 2.8 – continuación de la página anterior

Caso de Uso	*Capas*						
	DLT Blockchain	**Operaciones *DID***	**Resolución *DID***	**Autenticación *DID***	**Credenciales verificables**	**Gobernanza**	**Aplicación**
TCID [4]	*t*rustchain	✗ seudónimos creados por criptografía asimétrica	✗	✗	✓	Las credenciales se ocultan hasta que se desee su divulgación	La comunicación entre pares se da mediante un combinación de los protocolos *Tor* y *Gossip*
Identidad para *IoT* [81]	*H*yperledger Fabric	✗	✗	✗	✗	Un administrador gestiona las organizaciones en la *blockchain* federada y autoriza el registro de dispositivos *IoT*	Se utilizan tres *DLTs* independientes para favorecer el desempeño.

Tabla 2.8: Síntesis de los componentes de arquitectura presentes en los casos de uso que implementan una identidad digital autogobernada.
Fuente: Elaboración del autor.

El capítulo 3 realiza un análisis de los meta-sistemas SSI identificados en la revisión de la literatura y se evalúa el nivel de adherencia a los principios de identidad digital autogobernada.

Capítulo 3

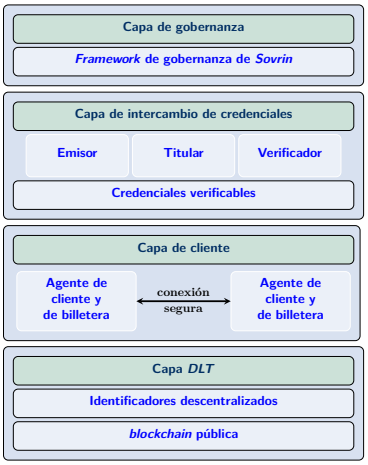
Meta-sistemas para el despliegue de una identidad digital autogobernada

Este capítulo presenta un análisis comparativo de los meta-sistemas de identidad digital autogobernada identificados en la revisión sistemática de la literatura. Los resultados han sido publicados en [2], y el artículo fue enviado al *journal* "*Frontiers in Blockchain*" debido a que el proceso de revisión lo identificó como una de las principales fuentes de publicación en esta área de investigación.

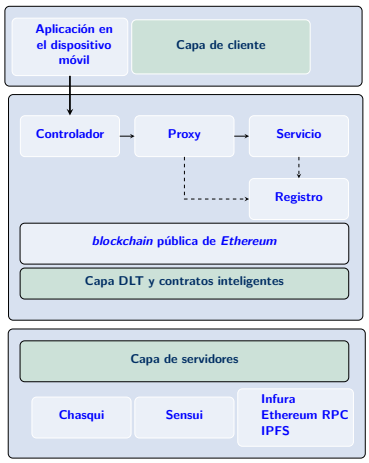
3.1 *Sovrin Network*

Es un meta-sistema que provee el servicio de identidad autogobernada en una red federada [10], y opera conforme a lo definido en su marco de gobernanza (*Sovrin Governance Framework -SGF-*) [242] administrado por una fundación sin ánimo de lucro [191]. El código fuente inicial de *Sovrin* originó *Hyperledger Indy* [192]. *Sovrin* presenta nodos confiables denominados "*Stewards*", administrados por el *SGF*, quiénes son los únicos habilitados para validar transacciones. *Sovrin* presenta doce principios [243] para la identidad autogobernada, los cuales son una extensión de los fundamentos planteados por *Christopher Allen*, adicionando usabilidad y equidad [2].

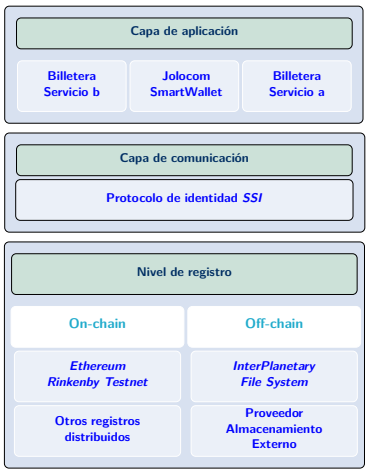
1. **Representación**: Una entidad humana, jurídica, física o digital se representa por n identidades digitales.
2. **Verificabilidad y autenticidad**: Los titulares de derechos de identidad podrán agregar pruebas verificables de autenticidad de sus atributos.
3. **Control y Agencia**: Los titulares de derechos de identidad tienen el control de sus datos y ejercen este derecho mediante la selección de agentes y tutores.
4. **Participación**: El sistema *SSI* no requiere la participación del titular de los derechos de identidad en los procesos de verificación.
5. **Transparencia**: Disponibilidad de la información y algoritmos de gobernanza de la red como incentivos y políticas de todos los componentes del sistema.
6. **Portabilidad**: Los titulares de derechos de identidad podrán irrestrictamente mover o copiar sus identidades a los agentes o sistemas que desee.
7. **Interoperabilidad**: Los atributos de identidad se representan, administran e intercambian bajo estándares abiertos, asequibles y sin restricciones de licenciamiento.



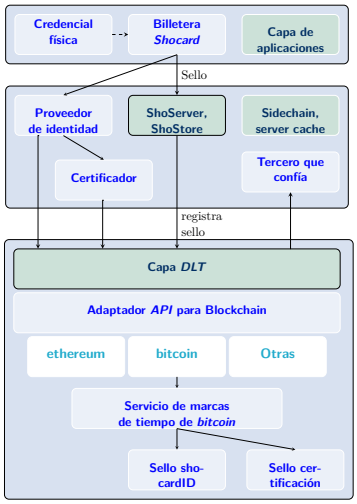
A *Sovrin*: adaptado de [73].



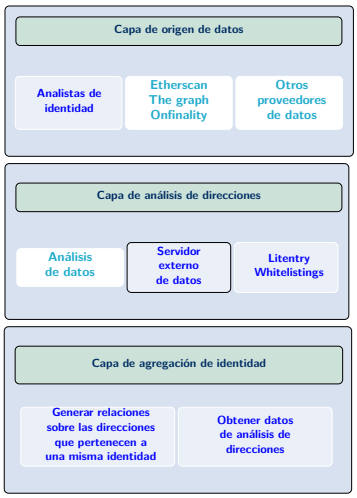
B *uPort*: adaptado de [19, 75].



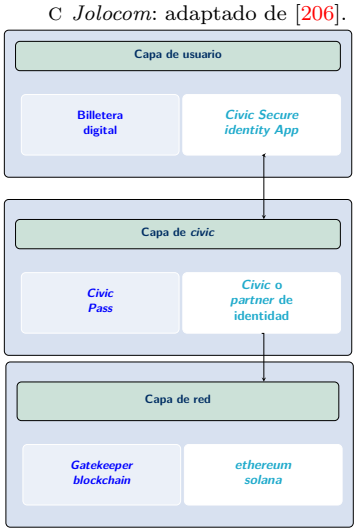
C *Jolocom*: adaptado de [206].



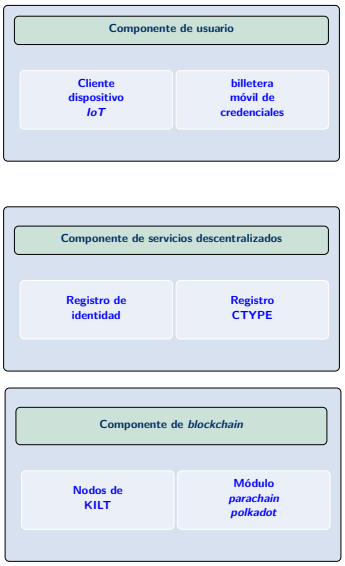
D *Shocard*: adaptado de [62, 239].



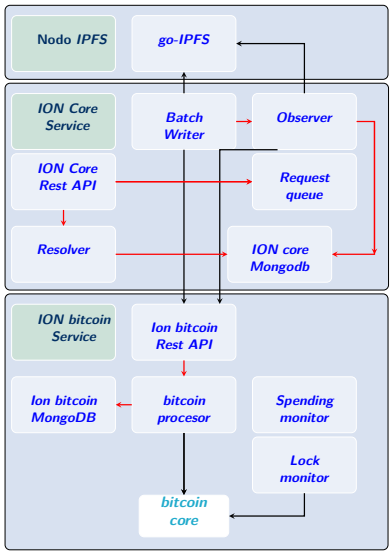
E *Litentry*: adaptado de [209, 210].



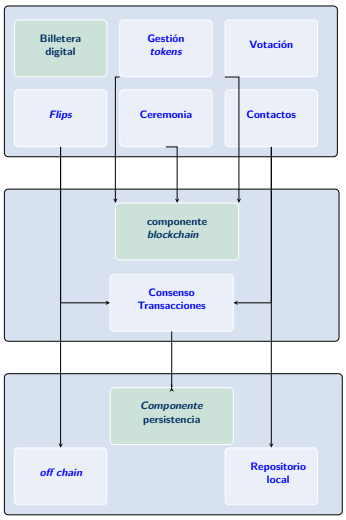
F *Civic*: adaptado de [212].



G *Kilt*: adaptado de [216].



H *ION*: Tomado de [196].



I *Idena*: adaptado de [240, 241].

FIGURA 3.1: Diagrama de arquitectura por capas de los principales *frameworks* para la creación de una identidad digital autogobernada.
Fuente: adaptado de [2].

8. **Usabilidad, accesibilidad y coherencia**: Los titulares de derechos de identidad tendrán la maximiza usabilidad posible y accesibilidad a los agentes y componentes del sistema *SSI*.

9. **Privacidad y divulgación mínima**: Los titulares de derechos de identidad podrán compartir los datos de identidad mínimos para cada contexto.

10. **Equidad e inclusión**: Los titulares de derechos de identidad no serán excluidos por el gobierno del ecosistema *SSI*.

11. **Seguridad**: Los titulares de derechos de identidad protegen sus atributos, administran sus identificadores y llaves criptográficas.

12. **Descentralización**: Un ecosistema *SSI* no dependerá de un entorno centralizado.

La arquitectura de *Sovrin* se ilustra en la Figura 3.1a. Se compone de cuatro capas:

1. Gobernanza: Esta red de identidad se encuentra bajo el gobierno de un conjunto de miembros confiables que articulan el marco de gobernanza de *Sovrin -SFG-*. *SFG* es responsable del cumplimiento de las políticas de gestión de datos definidas en cada jurisdicción evitando la censura y preservando la seguridad, privacidad, protección y portabilidad de la identidad [73].

2. Intercambio de credenciales: responsable del flujo de información para la emisión, tenencia y verificación de credenciales. Un emisor genera una credencial verificable mediante una definición de credencial, donde se vincula el *DID* del emisor, el esquema de la credencial y un registro de revocación. Esta definición es almacenada en la *blockchain* y se transfiere a la billetera del titular. Un verificador podrá resolver el *DID* del emisor de la credencial y confrontarlo con el almacenado en la *blockchain*, y verificar la firma y vigencia de la credencial [19]. El titular puede compartir información de múltiples credenciales minimizando la cantidad de información personal que divulga utilizando pruebas de conocimiento zero *-ZPK-* [73].

3. Cliente: en esta capa se despliegan los agentes para establecer la interacción *peer-to-peer* entre dos entidades, las cuales intercambian sus respectivos *peer DID*. Por lo general, cada entidad dispone de dos agentes, uno local en el dispositivo móvil (*edge agent*) para firmar las transacciones y otro en la nube (*cloud agent*) que gestiona el almacenamiento de atributos por terceros [73]. La comunicación entre agentes es privada y segura gracias a la utilización del protocolo *DIDComm* [244] invocado desde el *Hyperledger Aries* [245].

4. *DLT*: despliega una *blockchain* en *Hyperledger Indy*, la cual es de acceso público para lectura pero se restringe la escritura a los nodos confiables administrados por el marco de gobernanza [62]. El *DLT* preserva identificadores descentralizados públicos, credenciales verificables y definición de revocación de registros, sin almacenar atributos de identidad. El algoritmo de consenso se basa en una prueba de autoridad inspirado en el algoritmo de tolerancia a fallas bizantinas *-RBFT-*, denominado *Plenum Indy* [1], [71], [73].

Las capas (1) y (2) se orientan a garantizar la procedencia de las credenciales, mientras que las capas (3) y (4) a garantizar la fidelidad [10].

3.2 *uPort*

Ha sido diseñado sobre la *blockchain* de *Ethereum* para gestionar la identidad digital de una entidad por medio de contratos inteligentes [75], se encuentra disponible en dos versiones, *Veramo*,

concebida como un *framework Javascript* para el desarrollo de aplicaciones SSI, y *Serto* que ofrece un servicio federado y de código cerrado para el despliegue de identidades descentralizadas [2], [93]. La arquitectura de *uPort Open* se ilustra en la Figura 3.1b y está propuesta en tres capas: cliente, *blockchain* y persistencia.

1. Capa de cliente: la *wallet* genera el par de llaves asimétricas para crear la identidad digital en *ethereum*, almacena la llave privada y un identificador permanente *uPortID* que vincula la llave privada del usuario, lo que permite actualizar las llaves criptográficas conservando la identidad [193], [62].

2. Capa de *blockchain* y contratos inteligentes:

   (a) Controlador: establece el acceso inicial y gestiona la comunicación con el *Proxy*. Este contrato permite a una entidad definir su lista de delegados para recuperación de identidad en caso de perder el acceso a la billetera digital.

   (b) *Proxy* o representación: es responsable de actualizar el contrato de registro y establecer la comunicación con un servicio mediante el envío de una transacción firmada que recibe desde el controlador [62].

   (c) Registro: gestiona el enlace entre un *uPortID* y los atributos personales de identificación almacenados en repositorios externos como *IPFS* o servicios en la nube. El almacenamiento es descentralizado y los atributos se pueden cifrar de forma independiente, pero el registro es centralizado, por lo cual los metadatos en formato *JSON* son públicamente visibles con riesgo de filtración [61].

   (d) Servicio: define la interacción con una aplicación específica. Este contrato se comunica con el *Proxy* para obtener la solicitud del usuario enviada mediante el contrato controlador y acceder a la información *off-chain* requerida por medio del registro.

3. Capa de servidores:

   (a) *Chasqui*: servicio de mensajería responsable de la comunicación entre las aplicaciones descentralizadas, la billetera de *uPort* y los servidores. El intercambio de mensajes se realiza mediante documentos JSON [246].

   (b) *Sensui*: provee el *token ether* necesario para cubrir el costo (gas) requerido en la ejecución de una transacción en *Ethereum*. Este contrato libera al usuario de la necesidad de adquirir los *tokens* para crear su identidad en *Uport* [247].

   (c) *Infura Ethereum RPC*: permite la comunicación a través de una interfaz *RPC* estándar entre el servicio de *uPort* y la *blockchain* de *Ethereum* [248]

   (d) *Infura IPFS*: permite la comunicación a través de una interfaz estándar entre el servicio de *uPort* y el sistema descentralizado de archivos *IPFS* [249]

3.3 *Jolocom*

Es un protocolo que permite a una entidad, ya sea persona, organización, dispositivo *IoT* o un agente autónomo, crear su identidad principal y derivar n sub-identidades. La identidad tiene asociado un identificador descentralizado y credenciales verificables con esquemas en documentos JSON que se codifican como *JSON Web Tokens -JWT-* para su verificación y no repudio, además, utiliza *JSON Web Encryption -JWE-* para su privacidad [2], [206]. La Figura 3.1c ilustra las tres capas de la arquitectura:

1. Aplicación: La billetera denominada *Jolocom SmartWallet* provee la interfaz por defecto para la creación y administración de las identidades digitales, junto con sus credenciales verificables asociadas. Desde la billetera se generan las llaves criptográficas, y a partir de la llave pública se crea el *DID*, el cual se resuelve en un documento *DDO* almacenado en *IPFS*. El usuario debe disponer de *ether* para pagar las comisiones necesarias para el registro o actualización de los *DID* [206].

2. Comunicación: Implementa la librería *jolocom-lib* para dar soporte al protocolo. Esta librería es de código abierto y está diseñada con los estándares de la *W3C* para identificadores descentralizados (identidad) y credenciales verificables (atestación).

3. Registro: La persistencia de la información se realiza de dos modos: *on-chain* y *off-chain*. En la *blockchain* se realiza el registro confiable de los identificadores descentralizados. El protocolo utiliza por defecto la *blockchain* de pruebas de *Ethereum Rinkeby*, pero su característica de "ledger agnostic" permite la utilización de otras redes [206]. *Off-chain* facilita la conexión a un servicio de almacenamiento externo como *IPFS* para guardar los documentos *DID* y los esquemas públicos de las credenciales verificables. Por defecto, se utiliza el dispositivo donde se ha instalado la billetera digital [206].

3.4 *ShoCard*

Es una plataforma federada para autenticación que permite crear una identidad digital a partir de una credencial física confiable y datos biométricos capturados desde un teléfono inteligente, y registrarla usando la *blockchain* de *bitcoin* como servicio de marcas de tiempo [2], [62]. Las tres capas de la arquitectura, ilustradas en la Figura 3.1d son:

- Capa de aplicaciones: La billetera de *Shocard* genera las llaves criptográficas junto con el *shocardID* respectivo y escanea a través de la cámara del teléfono la credencial física que se desee agregar, por ejemplo, la licencia de conducción [61]. Los datos se cifran y almacenan en el dispositivo del usuario y el *hash* de los mismos se registra en la *blockchain* de *bitcoin* vinculados con el *shochardID* [62]. Un usuario controla la creación y divulgación de su *shocardID* y genera autorizaciones sobre sus credenciales. Únicamente terceros invitados podrán acceder a la información del usuario, aunque el servidor de *ShoCard* siempre tendrá acceso sin requerir invitación para realizar la validación de los atributos [250]. El *SDK* permite desarrollar *wallets* para sistemas operativos *iOS* y *Android* [239].
- Capa de servicio: despliega un entorno centralizado que actúa como un intermediario entre usuarios y terceras partes. Este servidor puede asociar el *shochardID* con un determinado servicio o tercero que confía, pero no proporciona un registro público de los identificadores [62]. Esta capa crea un canal de comunicación seguro entre las diferentes aplicaciones, donde los mensajes son firmados y cifrados por el cliente. Los servicios *ShoStore* y *server Cache* mantienen índices locales incluyendo una copia de la *blockchain*, con el propósito de mejorar la escalabilidad de la red, las sideChains o cadenas laterales contienen los contratos inteligentes que administran las certificaciones y almacenan códigos de verificación sobre estas.
- Capa *DLT*: La plataforma se considera *ledger-agnostic* por lo cual abstrae la conexión con la *blockchain* mediante una interfaz proporcionada por el adaptador. Actualmente, se utiliza el servicio de marcas de tiempo de *bitcoin* para firmar criptográficamente la información de identidad del usuario, y se registra en esta la prueba criptográfica de la creación del *shocardID* y para la validación de credenciales.

3.5 *Litentry*

Ensambla una identidad digital a partir de la agregación de los *DID* que posee una entidad en diferentes redes o *blockchains*, proporcionando datos confiables y cuantificados mediante un algoritmo de ponderación configurable, diseñado en una arquitectura compuesta por tres capas, las cuales se ilustran en la Figura 3.1e [2], [209].

1. Capa de origen de datos: define la conexión a proveedores de datos externos, como exploradores de una cadena de bloques (ej. *etherscan* [251]), protocolos descentralizados para indexar y consultar datos de una *blockchain* (ej. *The graph* [252]), e información de plataformas *BaaS* (ej. *onfinality* [253]) [210].

2. Capa de análisis de direcciones: proporciona un servidor externo para el procesamiento de la data obtenida en la capa de origen de los datos. Esta plataforma se encuentra en desarrollo y se proyecta el diseño de un servicio denominado *Litentry Whitelisting* [210].

3. Capa de agregación de identidad: se relacionan los identificadores que pertenecen a un mismo sujeto y obtiene el resultado del análisis de las direcciones para calcular el algoritmo que pondera la identidad. Esta capa cifra los datos y protege el cálculo con un *TEE* implementado con *Intel SGX* [210].

En el momento, se han desplegado dos *parachains*, *Litentry* sobre *Polkadot* [254] y *Litmus* en *Kusama*, una red de pruebas totalmente operativa para *Polkadot* [255]; y se han propuesto para su futura implementación casos de uso [210] como *drop3*, un protocolo para el lanzamiento de proyectos *blockchain* y la distribución de recompensas como nuevos *tokens* o *airdrops* controlando que los usuarios beneficiados posean una única dirección; o *my crypto profile* que permitirá una administración descentralizada de datos personales agregados de múltiples *blockchains* y sistemas de almacenamiento descentralizados, con la posibilidad de convertir la identidad en una colección *NFT*.

3.6 *Civic*

Presenta un ecosistema de identidad seguro y centrado en el humano para controlar y proteger la identidad digital combinando datos biométricos, *blockchain* y almacenamiento de *PII* en el teléfono inteligente del usuario; ofreciendo un servicio de verificación de identidad - IDV- a bajo costo. *Civic* ofrece el servicio de identidad con el pago de una tarifa de uso mediante su *token ERC20* nativo denominado *CVC* [65]. A partir de *Civic* se derivó el proyecto *Identity.com* [256], el cual se declara como un ecosistema de código abierto para verificación segura de identidad conforme al proceso definido en *Civic* pero permitiendo una interacción *peer-to-peer* entre los usuarios y nuevos métodos de autenticación, además de mejoras en la seguridad y privacidad con un *KYC* que requiere atributos como número de teléfono, correo electrónico, nombre y contraseña para generar un *civic secure ID* [2]. *Civic* fue diseñado en una arquitectura de tres capas, las cuales, se ilustran en la Figura 3.1f.

1. Capa de usuario: este sistema despliega un servicio denominado plataforma de identidad segura (*SIP*), donde la interacción con el usuario se realiza a través de una billetera digital (*Civil Secure Identity App*). La habilitación del usuario requiere una prueba de identidad basada en un documento oficial, ya sea pasaporte, tarjeta de identificación nacional, licencia de conducción o permiso de residencia (disponible en la mayoría de países del mundo), y un vídeo selfie para confrontar con la imagen del documento. La billetera del usuario puede asociar muchos identificadores *civic pass* pero cada uno de ellos asociado a un único servicio o *gatekeeper* [212], almacena la información cifrada y permite el uso de datos biométricos para inicio de sesión.

2. Capa de *Civic*: en esta capa, *Civic* o sus socios de identidad verifican la información suministrada por el usuario, y, en caso de ser aprobada, envían las afirmaciones a la capa de red y retornan al usuario los *PII* verificados y cifrados para su almacenamiento en la billetera digital. Por último, *SIP* permite el intercambio consentido y seguro de información entre un usuario *civic* y un solicitante de identidad con autenticación en tiempo real [212].

3. Capa de red: la *DLT* provee un registro de afirmaciones verificadas por la capa de *civic*, que permite comprobar la autenticidad de los datos, propiedad y vigencia. Actualmente permite integración con las *blockchains* de *solana* y *ethereum*, esta última en fase preliminar de pruebas [212].

3.7 *Kilt*

Es un protocolo *blockchain* para administrar (crear, reclamar, emitir, presentar y revocar) credenciales verificables, con una estructura de confianza *Top-Down* en la cual se dispone de entidades con mayor reputación como gobiernos o empresas, que atestiguan a otros sujetos. Una entidad tiene tres roles posibles conforme al modelo de datos para credenciales verificables definido por la *W3C*: (1) *claimer o holder*, la entidad que tiene la titularidad sobre una afirmación solicitada a un emisor confiable; (2) *attester*, provee la confianza sobre las reclamaciones que reciben los sujetos y emite las credenciales verificables sobre estas. Cada *attester o issuer* publica el conjunto de afirmaciones (tipos) que puede validar para recibir recompensas en el token nativo [257] y ganar o conservar su reputación; o (3) *verifier*, permite el intercambio de las credenciales verificables entre los diferentes sujetos, decide cuales emisores son confiables y valida la identidad del titular mediante un desafío criptográfico. *Kilt* permite a un *holder* generar auto-afirmaciones, las cuales serán validadas por un emisor y convertidas en credenciales verificables; y clasifica las afirmaciones en tipos (*Claim Type, CTYPE*) cuyos esquemas se describen en documentos *JSON* [216], [258].

Los componentes de la plataforma *Kilt* se ilustran en la Figura 3.1g y se comunican entre sí mediante un *SDK* desarrollado en *JavaScript* que contiene las bibliotecas criptográficas requeridas por el protocolo, e implementa las funciones para almacenar una afirmación, registrar un *CTYPE* en la *blockchain* y gestionar identidades, tipos de afirmaciones, reclamos y validaciones [2]. Estos componentes se describen a continuación:

1. Componente de usuario: La *wallet* le permite al sujeto crear su identidad digital e incluir auto-afirmaciones, las cuales se legitiman mediante una credencial emitida por una fuente confiable. El protocolo permite crear y registrar el *DID* en la *blockchain* y almacenar el *DOD* en un repositorio externo. El método *DID-KILT* y su adición al *universal resolver* se encuentra en desarrollo. También, cualquier usuario puede crear un nuevo *CTYPE* a partir de un meta-esquema *JSON* definido en el *SDK* y registrar el *hash* en la *DLT*. El usuario solicita la comprobación (reclamación) de una auto-afirmación por parte de un emisor. Una atestación incluirá la llave pública y la firma del emisor, el *hash* de la verificación y un campo adicional para la revocación

2. Componente de servicios descentralizados: El *token* es utilizado en la gobernanza y permite el pago de comisiones a los emisores, el registro de nuevos *CTYPES*, escritura en la *DLT* y revocación de credenciales. Este componente es llamado por el usuario para la administración de tipos de reclamaciones.

3. Componente de *blockchain*: Se diseñó con el *framework Parity Substrate* [217] y la *blockchain* de *Polkadot* [254], el cual se basa en la arquitectura modular WebAssembly [259], desarrollada

en *RUST*, con un uso de memoria eficiente y un rápido proceso de compilación [216]. En general, la *DLT* implementa módulos para la creación de *CTYPES* y el registro, revocación y búsqueda de atestaciones.

3.8 *Identity Overlay Network*

ION es una red pública de identidad basada en *DID* que implementa el protocolo *sidetree* [197] sobre la *blockchain* de *bitcoin* para desplegar una infraestructura determinística *DPKI* a gran escala, gobal, inmutable, sin autoridad central y resistente a censura o manipulación, con la posibilidad de gestionar miles de *DID* por segundo (superior a 10 000 transacciones en la red *ION*) ya que las encapsula en una única transacción de *bitcoin* [196]. La arquitectura de *ION* no requiere un mecanismo de consenso adicional al de *bitcoin*, el protocolo *sidetree* evita conflictos en la *DPKI* ya que define un conjunto estricto de reglas deterministas para el cambio de estado en un *DID* y restringe la transferencia de propiedad del identificador entre usuarios [2]. La arquitectura se diagrama en la Figura 3.1h, y se describe a continuación.

1. Nodo *IPFS*: Es un servicio de almacenamiento direccionado de contenido (*Content Addressed Storage, CAS*) con integridad criptográfica que preserva las transacciones encapsuladas por el *batch-writer*.

2. Servicios principales: A través de una billetera digital un usuario realiza una solicitud de transacción mediante *ION core Rest API*, la cual puede incluir un cambio de estado sobre el *DID*. Las solicitudes se almacenan en una cola hasta que se alcance un número predefinido (*batch size*) y serán tomadas por el servicio *batch-writer* y luego de ser encapsuladas en un único *hash*, son enviadas para ser procesadas por la *blockchain* mediante *ION bitcoin Rest API*. Para prevenir que un usuario malicioso complete el *batch size* con una sola transacción *ION*, se agregó una prueba denominada *proof of fee*, que asignó el costo de cada operación en un milésima parte del valor de una transacción en *bitcoin*. Por otro lado, la sincronización entre nodos utiliza el servicio *Observer* responsable de consultar un registro local en *mongoDB* para identificar los lotes de transacciones encapsuladas o embebidas para su procesamiento.

3. Servicios asociados a *bitcoin*: se conecta con la *blockchain* de *bitcoin* (*bitcoin core*). El servicio de *bitcoin processor* lee directamente de su copia local en *mongoDB* la información de los bloques, mientras que los servicios *spending monitor*, supervisa los valores máximos de escritura predefinidos para evitar una congestión en la red, y *lock monitor*, cumple con el requerimiento temporal de bloqueo de *BTC*, el cual es proporcional al *batch size*.

3.9 *Idena*

Presenta una *blockchain* diseñada con el objeto de resistir un ataque *sybil*, mediante un algoritmo de consenso denominado prueba de persona, basado en la resolución de un test no *turing* durante un evento sincrónico para todos los usuarios. La identidad de *Idena* o cryptoidentidad es global y verificable digitalmente, sin restricciones de acceso, descentralizada sin dependencia de terceras partes, resistente a *Sybil*, no censurable y anónima [240], [241]. La Figura 3.1i presenta un diagrama de arquitectura de alto nivel [2].

1. Componente de usuario: La billetera digital permite el acceso del titular a la *blockchain* de *Idena*. El primer paso es generar el par de llaves criptográficas, donde la llave pública será

el identificador de la cryptoidentidad, y la llave privada debe ser almacenada en un lugar seguro, ya que no se dispone de un mecanismo de recuperación. La nueva cuenta debe ser habilitada por medio de una invitación recibida de un usuario activo en la red y validada durante tres ceremonias de comprobación. Una ceremonia es un evento sincrónico en el que todos los miembros deben resolver una prueba de *turing* en un tiempo limitado. Cada usuario tiene la responsabilidad de demostrar que es un ser humano único. La cryptoidentidad presenta la siguiente secuencia de estados: (1) No invitado, asignado al momento de la generación de las llaves; (2) invitado, cuando se recibe la invitación de un miembro activo; (3) novato, si se aprueba con mínimo un 75 % de efectividad la primer ceremonia; (4) verificado, por la aprobación exitosa de tres ceremonias consecutivas con mínimo un 92 % y (5) humano, es el estado final de la identidad. A partir del nivel novato, el usuario debe aportar tres pruebas *turing*, las cuales se llaman *flips*. Cada *flip* está compuesto por cuatro imágenes asociadas lógicamente a una historia basada en dos palabras claves, sin incluir texto o números; se presenta en dos secuencias, una correcta y otra incorrecta, para su evaluación en las ceremonias de comprobación de identidad.

2. Componente *blockchain*: El algoritmo de consenso se basa en ceremonias sincrónicas de validación de identidad, las cuales se programan con una periodicidad inversamente proporcional a la cantidad de usuarios N, con una frecuencia mínima de 3 días y máxima de 28 días. En otras palabras, si la cantidad de usuarios disminuye, el número de ceremonias aumenta. L´a ceremonia se realiza a las 13:30 *UTC* del día seleccionado, y se divide en dos partes, una sección corta con 6 *flips* los cuales se deben resolver en menos de dos minutos, y un segunda sección larga que contiene entre 12 y 20 *flips*, dependiendo de la cantidad de usuarios en línea y un tiempo máximo de 30 minutos. Si el usuario falla en la ceremonia, ya sea debido a ausencia o por un número mayor al 25 % en las respuestas incorrectas, su estado se modificará así: (1) muerto, la identidad deja de ser parte de la red si estaba en candidato, novato o zombie; (2) suspendido, si ha fallado una ceremonia y su estado era verificado; y (3) zombie, si ha fallado en dos ceremonias consecutivas y su estado era verificado o humano. Una fuerte restricción del algoritmo se encuentra en el requerimiento de disponer a todos los usuarios en línea para un momento específico de tiempo y de forma periódica, con el objetivo de evitar la creación de múltiples identidades. La participación en las ceremonias tiene el incentivo adicional de recibir invitaciones, ya que en el protocolo se distribuyen recompensas a los usuarios cuyos invitados realizan la ceremonia de forma exitosa.

3. Componente de almacenamiento: La *blockchain* conserva el *hash* de los identificadores creados, las invitaciones enviadas y los resultados de la ceremonia de validación. Las imágenes incluidas en los flips se almacenan en un servicio descentralizado como *IPFS*.

3.10 Nivel de cumplimiento de los principios de identidad digital autogobernada

Los principios de identidad autogobernada son fundamentales para garantizar que un sistema de gestión de identidad digital respete la privacidad, la seguridad y el control de los atributos de identidad personal por parte del usuario. La comparación de los *frameworks* SSI descritos en la sección 3 se realizó de acuerdo con el nivel de cumplimiento de cada uno de los principios de identidad digital autogobernada. Para ello, se diseñó una escala discreta de medición que permite una evaluación objetiva, ya que proporciona un marco de referencia común para la comparación de los *frameworks* e identificar fortalezas y debilidades. A continuación se presenta la escala discreta para medir el nivel de cumplimiento de los principios de identidad autogobernada [2].

1. No cumple 0.0: El *framework* no se adhiere al principio de SSI.
2. Cumplimiento bajo 0.25: El *framework* cumple parcialmente con alguna característica del principio de SSI, pero tiene importantes deficiencias en su implementación.
3. Cumplimiento moderado 0.5: El *framework* cumple con una parte sustancial de un principio de SSI, pero presenta deficiencias que pueden comprometerlo.
4. Cumplimiento alto 0.75: El *framework* implementa características esenciales que permiten satisfacer el principio de SSI, pero puede presentar condiciones que generan deficiencias menores.
5. Cumplimiento total 1.0: El *framework* cumple completamente con un principio de SSI.

La aplicación de la escala de medición sobre cada principio de identidad autogobernada [223] se presenta en las tablas desde la 3.1 hasta la 3.10.

3.10.1 Principio de Existencia

La Tabla 3.1 compara los *frameworks*: *Sovrin*, *uPort*, *ION*, *Shocard*, *Jolocom*, *Litentry*, *Civic*, *Idena* y *KILT*, y muestra una tendencia positiva hacia el cumplimiento del principio de existencia. Para cada *framework*, se indica si permite la creación independiente de identidades y se proporciona una descripción de como se aborda.

Principio 1: Existencia		
Framework SSI	**Creación independiente**	**Descripción**
Sovrin	☑ 1.0	Permite la generación de múltiples *DID*, facilitando el uso de identificadores únicos para cada servicio [62], [65].
uPort	☑ 1.0	Genera un *uPortID* basado en claves criptográficas en la *blockchain* de Ethereum [62], con la ventaja adicional de permitir la actualización de la clave privada sin comprometer la identidad del usuario [75].
ION	☑ 1.0	Un usuario puede crear su *DID* sin restricciones o barreras de acceso y controlar sus llaves criptográficas [196].
Shocard	☒ 0.0	El registro en *Shocard* requiere un verificador de identidad que valide y otorgue confianza, por ejemplo, se requiere la tenencia de una identidad oficial establecida por un documento legal como un pasaporte [65], [102].
Jolocom	☑ 1.0	La entidad determina la existencia y persistencia de su identidad y sub-identidades digitales asociadas [206].
Litentry	☒ 0.0	Es un agregador de identidad por lo tanto la existencia depende de terceros [209].
Civic	☒ 0.0	Genera una identidad verificada con un identificador público tipo *ethereum* que puede ser usada para inicio de sesión sin contraseña y factor de doble autenticación, pero requiere de un documento oficial como pasaporte, tarjeta de identidad nacional, licencia de conducción o permiso de residencia [65].
Idena	☑ 1.0	Permite la creación de identidades basadas en pares de claves criptográficas sin condiciones ni restricciones, promoviendo la autonomía del usuario [240].
KILT	☑ 1.0	Facilita la creación de identidades con capacidad de generar auto-afirmaciones, sin barreras de entrada y con flexibilidad para asumir diversos roles [216].

TABLA 3.1: Nivel de cumplimiento del principio de existencia en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

Este principio fundamental para garantizar la autonomía y el control del usuario sobre su identidad digital, pero su implementación efectiva requiere un equilibrio cuidadoso entre autonomía, usabilidad y confianza en el ecosistema de identidad digital.

La mayoría de los *frameworks* (6 de 9) cumplen apropiadamente con el principio de existencia, ya que permiten la creación independiente de identidades digitales, a excepción de *Shocard*, *Litentry* y *Civic* donde la creación de la identidad esta supeditada a la tenencia de una identidad provista por un tercero de confianza, situación que los hace dependientes de verificadores externos. En el caso de *Civic* y *Shocard*, se requiere un documento oficial como pasaporte o tarjeta de identidad nacional para la habilitación en el sistema. Esta condición limita el ingreso de los individuos que carecen de documentación legal. Por su parte, *Litentry*, al ser un agregador de identidades, depende de la existencia de identidades preexistentes, lo que puede introducir vulnerabilidades si las fuentes de estas no son confiables o seguras. Como facto adicional, *uPort* implementa la actualización de claves privadas sin comprometer la identidad del usuario [2].

3.10.2 Principio de Control

La Tabla 3.2 evalúa el cumplimiento del principio de control. Se analiza como cada *framework* permite a los usuarios mantener el control sobre sus identidades digitales, incluyendo la gestión de llaves criptográficas y la capacidad de actualizar o revocar información. La tabla proporciona una visión comparativa de las características de control ofrecidas por cada solución, destacando aspectos como los mecanismos de recuperación de llaves y el grado de autonomía del usuario en la gestión de su identidad digital.

Principio 2: Control			
Framework SSI		**Gestión de llaves**	**Descripción**
Sovrin	☑ 1.0	*DPKI*	El *Holder* tiene control sobre sus *DID*, con un método de recuperación social de llaves [103],[101], [102]. Puede actualizar sus atributos y revocar sus *VC* [36].
uPort	☑ 1.0	*Wallet*	Las llaves criptográficas se almacenan en la billetera digital del *holder* [103],[101],[102]. La identidad se recupera mediante la aprobación de delegados preestablecidos en caso de pérdida del dispositivo [100]. El usuario puede actualizar atributos y revocar *VC* [36].
ION	☑ 1.0	Clave de recuperación	El titular tiene control total sobre su *DID*, y puede cambiar su estado, modificar servicios asociados y actualizar llaves. La recuperación se realiza mediante una clave generada en la creación o actualización del *DID*. Actualmente solo soporta *bitcoin* (curva elíptica *secp256k1*). Permite desactivación irreversible de la identidad [196].
Shocard	☑ 1.0	*Wallet*	La identidad se cifra y almacena en el teléfono inteligente del usuario, pero no dispone de un sistema para recuperar llaves criptográficas [102]. El proveedor de servicio puede retirar de forma unilateral una credencial del usuario pero no puede modificar su historial [65].
Jolocom	☑ 1.0	*HD keys*	El *Holder* controla el almacenamiento de atributos y llaves criptográficas, decidiendo qué información compartir. [101]. Ofrece un método nativo de rotación de llaves para recuperación en caso de compromiso [206].
Litentry	☒ 0.5	☒	Ya que es una capa de agregación, el control de la información depende del diseño de la aplicación que utilice *Litentry* [210].
Civic	☑ 1.0	*Wallet*	La información se almacena en el teléfono inteligente bajo la custodia del usuario [65]. En caso de un atributo obsoleto se permite que una entidad de verificación pueda revocarlo [102].
Idena	☑ 1.0	☒	El usuario controla su identificador de identidad, que le permite participar en los eventos de validación de identidad, realizar transferencias del token nativo *IDNA* [257] y responder encuestas. No se define un mecanismo para recuperación de llaves [240].

Continúa en la siguiente página

Tabla 3.2 – continuación de la página anterior

Principio 2: Control			
Framework SSI	**Gestión de llaves**		**Descripción**
KILT	☑ 1.0	☒	La identidad es creada mediante el par de llaves pública-privada y se enlaza con su respectivo *DID*, el cual queda bajo control total del titular [216].

TABLA 3.2: Nivel de cumplimiento del principio de control en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

Se observa que ocho de los nueve *frameworks* evaluados cumplen plenamente con el principio de control, lo que indica un fuerte compromiso del sector con la autosoberanía de la identidad digital, con la implementación de una diversidad de mecanismos de gestión de llaves, como *DPKI* (*Sovrin*), *wallets* digitales (*uPort*, *Shocard*, *Civic*), y claves de recuperación (*ION*), y métodos para recuperar el acceso a la identidad en caso de pérdida de llaves (*Sovrin*, *uPort*, *ION*, *Jolocom*), lo que aumenta la seguridad y usabilidad, además de ofrecer flexibilidad para diferentes casos de uso. Se detectan debilidades como dependencia de un dispositivo o control de un tercero, como sucede en *Shocard* y *Civic*, lo que podría ser un punto único de falla [2].

3.10.3 Principio de Consentimiento

La Tabla 3.3 muestra un panorama generalmente positivo en cuanto al cumplimiento del principio de consentimiento en los *frameworks* SSI evaluados. La mayoría ofrece mecanismos robustos para que los usuarios controlen la compartición de su información personal. Sin embargo, existen áreas de mejora, especialmente en la estandarización de los mecanismos de consentimiento y en la garantía de que no haya acceso no autorizado a la información del usuario.

Principio 3: Consentimiento		
Framework SSI	**Descripción**	
Sovrin	☑ 1.0	El usuario controla qué *DID* y atributos revelar, permitiendo solo a terceros autorizados consultar PII [71].
uPort	☑ 1.0	El usuario asigna y revoca permisos para consultar su información personal almacenada *off-chain* [75]. Se advierte precaución con el contrato inteligente de registro para evitar consultas no autorizadas de atributos [71].
ION	☑ 1.0	Se requiere el consentimiento del usuario para todas las operaciones relacionadas con su *DID* [196]
Shocard	☑ 1.0	El *Holder* autoriza a terceros para consulta de su *PII*, pero los servidores de *Shocard* podrán consultar los atributos sin necesidad de un consentimiento explícito [71].
Jolocom	☑ 1.0	El protocolo implementa métodos para que un titular asigne o revoque acceso a su información personal [206].
Litentry	☒ 0.5	Los escenarios para compartir atributos de forma segura y privada se implementarán en cada caso de uso, por ejemplo, *my crypto profile* [210].
Civic	☑ 1.0	El usuario decide los datos que desea intercambiar directamente con un proveedor de servicios o autoridad de autenticación [65].

Continúa en la siguiente página

Tabla 3.3 – continuación de la página anterior

Principio 3: Consentimiento		
Framework SSI	**Descripción**	
Idena	☑ 0.5	El titular administra su identificador de identidad y se requiere la firma criptográfica del usuario para el envío de invitaciones, transferencias de *tokens*, creación de *flips* y votación en consultas. El usuario puede cancelar una invitación en cualquier momento [240].
KILT	☑ 0.0	Dado que las *VC* están almacenadas en la *wallet*, el titular controla con quién realizará la presentación y el contenido que desea exponer [216].

Tabla 3.3: Nivel de cumplimiento del principio de consentimiento en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

Se encontró que *frameworks* como *Sovrin*, *uPort*, *Jolocom*, *Civic* y *KILT* ofrecen a los usuarios un control detallado sobre qué información compartir y con quién hacerlo. Además, *uPort* y *Jolocom* indican específicamente la capacidad de revocar permisos, lo que aumenta el control del usuario a lo largo del tiempo. *Litentry* delega la implementación del consentimiento a cada caso de uso específico, lo que podría resultar en inconsistencias o brechas de privacidad si no se implementa correctamente [2].

3.10.4 Principio de Minimización

La Tabla 3.4 muestra que la mayoría de *frameworks* ofrece mecanismos robustos para la divulgación selectiva de información, utilizando técnicas avanzadas para proteger la privacidad del usuario. Sin embargo, existen áreas de mejora, especialmente en la estandarización de los mecanismos de minimización y en garantizar que todos los *frameworks* ofrezcan un nivel adecuado de soporte para este principio.

Principio 4: Minimización			
Framework SSI	**Divulgación selectiva**	**Mecanismo**	**Descripción**
Sovrin	☑ 1.0	*ZPK*	Implementa divulgación selectiva en credenciales verificables utilizando *Zero-Knowledge Proofs (ZPK)* [103], [100].
uPort	☑ 1.0	Contratos inteligentes	La creación y uso de UportID no requiere divulgar *PII* [101], [71]. Los contratos inteligentes implementan métodos para minimizar la correlación de identidades entre las diferentes DApps [75].
ION	☑ 1.0	*DID*	Se centra en el despliegue de una Infraestructura de Clave Pública Descentralizada, que puede utilizarse para diseñar casos de uso que administren *PII* de manera eficiente [196].
Shocard	☒ 0.0	☒	No presenta soporte para divulgación selectiva [101].
Jolocom	☑ 1.0	Acoplado en el protocolo	Control granular sobre las credenciales verificables que componen la identidad digital [101],[206].
Litentry	☐ 0.5	☐	Depende de las plataformas de terceros y del diseño del caso de específico [210].
Civic	☑ 1.0	Árbol de *Merkle*	La información personal verificada es almacenada como un *hash* dentro de un árbol de *Merkle*, y el *holder* puede revelar selectivamente los fragmentos de este árbol [102].

Continúa en la siguiente página

Tabla 3.4 – continuación de la página anterior

Principio 4: Minimización			
Framework SSI	**Divulgación selectiva**	**Mecanismo**	**Descripción**
Idena	☐ 0.25	☐	No almacena *PII* ya que su objetivo es proveer un identificador para una identidad única, que pueda ser vinculada en una plataforma que gestione atributos personales [240].
KILT	☑ 1.0	*ZPK*	El titular puede seleccionar la información de una credencial que será presentada a un verificador y esta solamente podrá ser verificada por los usuarios habilitados [216].

Tabla 3.4: Nivel de cumplimiento del principio de minimización en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

Es crucial que los desarrolladores de estos *frameworks* continúen refinando sus enfoques para asegurar que la minimización de datos sea una característica central y consistente en todas las implementaciones de SSI, equilibrando la necesidad de protección de la privacidad con la usabilidad y la flexibilidad para diferentes casos de uso. La mayoría de los *frameworks* (6 de 9) muestran un fuerte cumplimiento del principio de minimización, con la implementación de técnicas para lograr la divulgación selectiva, incluyendo *Zero-Knowledge Proofs* (*ZKP*), contratos inteligentes, árboles de *Merkle* y enfoques integrados en los protocolos, aunque mecanismos avanzados como ZKP son efectivos, pueden ser complejos de implementar y entender para los usuarios finales. *uPort* se destaca por implementar métodos para minimizar la correlación de identidades entre diferentes aplicaciones, lo que aumenta la privacidad del usuario. Los *frameworks* que ha presentado debilidades son *Litentry*, *Shocard* e *Idena*. En el caso de *Litentry*, la implementación de la divulgación selectiva depende de plataformas de terceros, lo que podría comprometer la consistencia y la seguridad, *Shocard* no presenta soporte para divulgación selectiva, lo cual es una debilidad significativa en términos de minimización de datos, e *Idena* se diseñó para asegurar una identidad única para un determinado servicio [2].

3.10.5 Principio de Persistencia

El principio de persistencia es crucial en SSI, ya que garantiza que las identidades y la información asociada permanezcan accesibles y válidas a lo largo del tiempo. La Tabla 3.5 analiza como cada *framework* implementa mecanismos para asegurar la durabilidad de las identidades, incluyendo el tipo de almacenamiento utilizado (*on-ledger* u *off-ledger*) y las estrategias específicas para mantener la persistencia de los datos. Esta comparación proporciona una visión integral de como los diferentes *frameworks* abordan el desafío de la longevidad de las identidades digitales en el ecosistema SSI.

Principio 5: Persistencia			
Framework SSI		**Almacenamiento**	**Descripción**
Sovrin	☑ 1.0	*Off ledger*	*PII* son almacenados por un agente controlado por el *holder*. La persistencia puede utilizar servicios en la nube [103]. Usa *DID* que son identificadores de larga duración [76]
uPort	☑ 1.0	*Off ledger*	Almacena los *PII* en repositorios externos como *IPFS*, *AWS* o *Dropbox* [100], [102]. El perfil del usuario se registra en formato *JSON* plano y es público, por lo cual, el análisis de los meta-datos de estos documentos podrían generar fallos en la privacidad [103],[101], [102]. Usa *DID* que son identificadores de larga duración [76]

Continúa en la siguiente página

Tabla 3.5 – continuación de la página anterior

Principio 5: Persistencia			
Framework SSI		**Almacenamiento**	**Descripción**
ION	☑ 1.0	*Off ledger*	Las transacciones se almacenan con seguridad criptográfica en *IPFS* y *mongoDB* [196].
Shocard	☑ 0.0	*Off ledger*	Usa la *blockchain* de *bitcoin* para almacenar el *hash* de los *claims* emitidos y conserva en un servidor centralizado una copia cifrada de los *PII* certificados. Este servidor es un intermediario entre titulares, emisores y verificadores [103],[101]. El usuario puede realizar copias de seguridad utilizando de forma obligatoria el servicio de *Dropbox* [65].
Jolocom	☑ 0.0	*Off ledger*	La arquitectura permite adaptar repositorios externos para el almacenamiento seguro de *PII*, lo que extiende y controla la longevidad de las identidades [101], [206].
Litentry	☑ 0.5	*Off ledger*	Vincula atributos de una entidad alojados en múltiples redes, creando un sistema de identidad independiente de plataforma y solucionando el problema de registros *DID* aislados [210].
Civic	☑ 1.0	*Off Ledger*	Los datos del usuario se almacenan de forma cifrada en la billetera digital del *holder* con una copia de respaldo mediante *google drive* [103]. En la *blockchain* se registran el *hash* de los datos como un *token ERC-20* y pueden ser revocados por la autoridad de autenticación, por ejemplo, en el caso de cambio de valor de un atributo, la confianza en la identidad depende de la confianza en este actor [102]
Idena	☑ 0.25	*On Ledger*	Se crea un identificador persistente en la *blockchain* propia de *Idena* sin almacenar datos adicionales. El usuario puede disponer de una lista de contactos almacenada en su billetera digital [240].
KILT	☑ 1.0	*Off ledger*	Las afirmaciones se almacenan en la *wallet* del titular. En la *DLT* se registra el *hash* de las afirmaciones revocables, el *hash* del *CYTPE* y la información de pago con el token *KILT*. El *CTYPE* como tal y el documento *DID* se almacenan en un repositorio externo [216].

Tabla 3.5: Nivel de cumplimiento del principio de persistencia en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

Los *frameworks* analizados utilizan una variedad de estrategias para asegurar la persistencia, desde almacenamiento en la nube hasta sistemas distribuidos como *IPFS*, marcando una preferencia por almacenamiento *off-ledger* para *PII*, lo que permite mayor flexibilidad y escalabilidad. *Shocard* y *Civic* dependen de servicios centralizados para almacenamiento o respaldo, lo que podría comprometer la descentralización, mientras que *KILT* utiliza múltiples capas de almacenamiento (*wallet*, *DLT*, repositorio externo), lo que podría aumentar la complejidad del sistema. Es crucial que los desarrolladores de estos *frameworks* continúen refinando sus estrategias para asegurar que las identidades digitales permanezcan accesibles, seguras y bajo el control del usuario a lo largo del tiempo, mientras se mantienen los principios fundamentales de la SSI [2].

3.10.6 Principio de Protección

La Tabla 3.6 presenta como los *frameworks* SSI están abordando el principio de protección, con un enfoque predominante en la descentralización parcial y el cumplimiento regulatorio, además, brindan resistencia a la censura por parte de gobiernos u organizaciones criminales. Mientras que estas características ofrecen un buen nivel de seguridad y privacidad, también introducen desafíos en términos de complejidad y dependencia de terceros en algunos casos. La mayoría de los *frameworks* muestran un fuerte compromiso con la protección de las identidades, pero existen áreas de mejora, especialmente en lograr una descentralización total y en clarificar el cumplimiento de la normatividad en cada jurisdicción.

Principio 6: Protección				
Framework SSI		**Descentralización**	**Reglamentación**	**Descripción**
Sovrin	☑ 0.75	Parcial	*GDPR* [73]	La red de *Sovrin* establece un marco de gobernanza que define el conjunto de nodos confiables denominados *stewards*, habilitados para ejecutar el protocolo de consenso *Plenum* [103], [102], basado en *RBFT* [260]. Además, cada transacción utiliza un seudónimo para el usuario con el objeto de reducir el riesgo de correlación de identidad [65].
uPort	☑ 0.75	Parcial	*GDPR* [75]	Riesgo de fallo y censura debido a la centralización del servicio de mensajería *Chasqui* [101], [102].
ION	☑ 1.0	Total	NA	El sistema es público, descentralizado y de libre acceso, donde el usuario controla completamente sus identificadores, sin la necesidad de un mecanismo adicional de consenso ni de un nuevo token de gobernanza, puesto que se utiliza la *blockchain* de *bitcoin* junto con su token para el funcionamiento [196].
Shocard	☑ 0.0	Parcial	*KYC* y *AML* [65]	Presenta servidores centralizados que actúan como intermediarios entre los actores (*titulares, emisores, verificadores*)[102]. La verificación de datos para *KYC* o *AML* se basa en la información contenida en la licencia de tránsito o pasaporte [65].
Jolocom	☑ 0.5	Parcial	NA	*Ethereum Rinkeby* requiere la definición de un conjunto de nodos de confianza responsables de validar las transacciones [206].
Litentry	☑ 0.5	Parcial	NA	Los cálculos del algoritmo de ponderación o reputación de la identidad son cifrados y protegidos bajo un entorno de ejecución de confianza (*TEE*) [210].
Civic	☑ 0.75	Parcial	*KYC* [65]	Mediante contratos inteligentes se administra el conjunto de nodos validadores [103]. Las identidades son resistentes a censura por parte de un gobierno o una organización criminal [102]. El cumplimiento de *GDPR* es ambigüo ya que *Civic* ni lo confirma ni lo rechaza [65].
Idena	☑ 1.0	Total	NA	La plataforma presenta una *blockchain* de diseño exclusivo para gestionar identidades únicas sin requerir el almacenamiento de información personal [240].
KILT	☑ 0.75	Parcial	*GDPR* [216]	Presenta privacidad por diseño, no almacena datos personales y permite el derecho al olvido ya que registra únicamente el *hash* de *PII*. La futura integración con *polkadot* proporcionará una mayor seguridad en la red debido al consenso global de dicha *blockchain* [216].

Tabla 3.6: Nivel de cumplimiento del principio de protección en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

En los *frameworks* revisados se observa la utilización de una variedad de estrategias para proteger las identidades, desde consensos descentralizados hasta entornos de ejecución de confianza. *ION* e *Idena* logran una descentralización total, reduciendo los puntos únicos de falla, mientras que algunos permiten por su diseño cumplir con regulaciones como *GDPR* (*Sovrin*, *uPort* y *KILT*), *KYC* (*Shocard* y *Civic*) o *ALM* (*Shocard*), lo que aumenta su viabilidad en contextos legales estrictos. En contraste, se tiene que *Shocard* y *uPort* dependen de servicios centralizados, lo que podría comprometer la seguridad y la privacidad; en *Civic*, el cumplimiento de regulaciones como *GDPR*

es ambigüo, lo que podría generar incertidumbre legal; *Sovrin*, utiliza mecanismos complejos de gobernanza y consenso, lo que podría dificultar su implementación y adopción; y *Shocard* depende de documentos tradicionales para la verificación *KYC/AML*, lo que podría limitar su aplicabilidad en escenarios puramente digitales [2].

3.10.7 Principio de Acceso

Este principio es fundamental, ya que garantiza que los usuarios tengan control sobre su identidad digital y puedan acceder a ella de manera libre y sin restricciones. La Tabla 3.7 analiza los *frameworks*, evaluando su tipo de *blockchain*, la naturaleza de su acceso (público o permisionado), y proporciona una descripción detallada de como cada uno de ellos aborda el principio de acceso.

Principio 7: Acceso				
Framework SSI		**Tipo**	**Blockchain**	**Descripción**
Sovrin	☑ 0.75	Permisionada	*Hyperledger Indy*	La escritura en el *DLT* esta limitada a un conjunto de nodos de confianza [73]. La identidad es gratuita para los usuarios y no se definió una tarifa por transacción [76].
uPort	☑ 1.0	Pública	*Ethereum*	Utiliza la *blockchain* pública de *Ethereum* con una gestión de costos de transacciones (gas) mediada automáticamente por un servicio denominado *Sensui* [103], [75]. La identidad es gratuita para los usuarios [76]
ION	☑ 1.0	Pública	*bitcoin*	Utiliza la *blockchain* totalmente descentralizada de *bitcoin* [196].
Shocard	☑ 1.0	Pública	*bitcoin*	Se despliega inicialmente sobre la *blockchain* de *bitcoin* [101], pero el adaptador diseñado en su arquitectura permite el uso de otros *ledgers*.
Jolocom	☑ 1.0	Pública/ Privada	*Ethereum Rinkeby tesnet*	Desarrollada sobre la *blockchain tesnet* de *Ethereum Rinkeby* [261], la implementa un algoritmo de prueba de autoridad para el consenso de la red [101], [206].
Litentry	☑ 0.75	Permisionada	*Parachain* en *Polkadot*	La gobernanza se basa en propuestas de referendo que pueden ser iniciadas por cualquier miembro admitido, este esquema reduce el riesgo de toma de decisiones dominada por un grupo gobernante y permite la discusión de múltiples temas. Se dispone de la red de pruebas *Kusama* para la validación de cambios previo a su aprobación para ser incluidos en la red principal [210].
Civic	☑ 1.0	Pública	*ethereum solana*	Se integra con las *blockchains* de *ethereum* y *solana* [103]. Dispone de librerías para una rápida integración de *Civic pass* en el diseño de *DAPPs*, tanto a nivel de aplicación como de la cadena de bloques [212].
Idena	☑ 1.0	Pública	Diseño propio	La plataforma presenta una *blockchain* exclusiva para gestionar identidades únicas, la cual es totalmente descentralizada y pública. El acceso a la identidad se asegura con la llave privada, la cual esta bajo custodia del titular, sin un mecanismo de recuperación [240].
KILT	☑ 1.0	Pública	*Polkadot* con *Parity Substrate*	Cualquier sujeto puede crear su identidad y convertirse en una entidad de la red *KILT* [216].

Tabla 3.7: Nivel de cumplimiento del principio de acceso en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

La mayoría de los *frameworks* muestran un fuerte compromiso con el principio de acceso a través de *blockchains* públicas y soluciones gratuitas para los usuarios, con variaciones significativas en sus

enfoques. Los desafíos principales incluyen equilibrar la accesibilidad con la seguridad, manejar la complejidad técnica, y asegurar la escalabilidad y la interoperabilidad. La elección del *framework* más apropiado dependerá de los requisitos específicos del caso de uso y del equilibrio deseado entre descentralización, accesibilidad y control del usuario.

Se encontró que los *frameworks* revisados utilizan una variedad de *blockchains*, incluyendo *Ethereum*, *Bitcoin*, *Polkadot*, y soluciones propias. Esta diversidad ofrece flexibilidad y opciones para diferentes casos de uso. *uPort*, *ION*, *Shocard*, *Civic*, *Idena* y *KILT* se despliegan en *blockchains* públicas, lo que favorece la transparencia y la descentralización. *Sovrin*, *uPort* e *Idena* ofrecen identidad gratuita para los usuarios, lo que promueve la adopción y la accesibilidad, aunque, *Sovrin* y *Litentry* utilizan *blockchains* permisionados, lo que podría limitar la descentralización y el acceso abierto [2].

3.10.8 Principio de Transparencia

La Tabla 3.8 presenta una evaluación comparativa del principio de transparencia en los *frameworks* de Identidad Auto-Soberana objeto de estudio. Este principio se orienta a garantizar que los sistemas y protocolos utilizados sean abiertos, verificables y confiables. La tabla evaluando aspectos clave como la disponibilidad del código fuente, el tipo de licencia, el uso de estándares abiertos y una descripción detallada de como cada *framework* aborda la transparencia. Esta comparación permite comprender mejor las diferentes aproximaciones y el nivel de apertura que cada *framework* ofrece, aspectos fundamentales para la confianza y adopción de soluciones SSI.

Principio 8: Transparencia

Framework SSI	**Código fuente**	**Licencia**	**Estándares**	**Descripción**
Sovrin	☑ [192] 1.0	*Open Source*	Abiertos	El código fuente fue cedido a la *Linux Foundation* y se denominó *Hyperledger Indy* [100], [102].
uPort	☑ [193] 1.0	*Open Source*	Abiertos	Provee herramienta para el desarrollo de aplicaciones sobre *Ethereum* con gestión de *PII* centrados en el usuario [102]. *uPort* es miembro de la *DIF* [13] y apoya el desarrollo de estándares abiertos para identidad digital.
ION	☑ [196] ☑ [197] 1.0	*Open Source*	Abiertos	El código fuente de *ION* se encuentra disponible [196] junto con la implementación del protocolo independiente de *blockchain sidetree* [197].
Shocard	☒ 0.0	Sujeto a patentes	Sujeto a patentes	Presenta métodos y algoritmos patentados para la administración de la identidad [239].
Jolocom	☑ [206] 1.0	*Open Source*	Abiertos	Desarrollado sobre la *blockchain* de *Ethereum* [206].
Litentry	☑ [209] 1.0	*Open Source*	Abiertos	se encuentra disponible el código fuente de las *Parachains* en *Polkadot* y *kusama* [210]. Un caso de uso específico podrá presentar limitaciones de transparencia.
Civic	☑ [262] 1.0	*Open Source*	Abiertos	Utiliza la red pública de *Ethereum* sin depender de infraestructura o *software* propietario [102]
Idena	☑ [241] 1.0	*Open Source*	No aplica.	El código fuente del nodo de Idena y de su billetera digital están disponibles para su revisión [240].

Continúa en la siguiente página

Tabla 3.8 – continuación de la página anterior

Principio 8: Transparencia				
Framework SSI	**Código fuente**	**Licencia**	**Estándares**	**Descripción**
KILT	☑ [258] ☑ [263] 1.0	*Open Source*	Abiertos	Tanto el código fuente del protocolo [258] como del *framework* aplicado [263] son abiertos. *Parity substrate* dispone de una arquitectura y código fuente públicos con desarrollo y validación por expertos de la comunidad *blockchain* [216].

Tabla 3.8: Nivel de cumplimiento del principio de transparencia en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

La mayoría de los *frameworks* analizados (8 de 9) muestra una clara tendencia hacia el código abierto. Esta preferencia se evidencia en la disponibilidad pública de su código fuente, lo que posibilita una revisión y auditoría independiente. Tal apertura fomenta la confianza y la colaboración comunitaria. Además, el uso de licencias de código abierto facilita la adopción, modificación y distribución de estos *frameworks*. Esta orientación se complementa con la adherencia a estándares abiertos, promoviendo así la interoperabilidad y la implementación de mejores prácticas en la industria. Por otra parte, *Shocard* se destaca como el único *framework* que no sigue el principio de código abierto, utilizando métodos y algoritmos patentados. Esto limita la transparencia y podría generar desconfianza en la comunidad SSI. En *Litentry*, se advierte que ciertos casos de uso podrían presentar limitaciones de transparencia, lo que podría ser problemático en aplicaciones que requieren total apertura [2].

3.10.9 Principio de Portabilidad

La portabilidad permite a los usuarios mantener el control de su identidad digital y moverla entre diferentes sistemas y plataformas. La evaluación del cumplimiento se presenta en la Tabla 3.9 y se basó en la capacidad de cada *framework* para permitir la transferencia de identidades y credenciales entre diferentes sistemas, el uso de estándares abiertos que faciliten la interoperabilidad, y la flexibilidad en la gestión de identidades en múltiples dispositivos o plataformas. Esta comparación ofrece una visión clara de las fortalezas y limitaciones de cada *framework* en términos de portabilidad, un factor clave para la adopción y utilidad a largo plazo de las soluciones SSI.

Principio 9: Portabilidad		
Framework SSI		**Descripción**
Sovrin	◩ 0.55	La portabilidad es limitada, pero implementa estándares abiertos para credenciales verificables e identificadores descentralizados, lo que podría facilitar futuras mejoras en este aspecto [73].
uPort	◩ 0.5	La portabilidad es limitada debido a su fuerte acoplamiento con *Ethereum*, lo que puede restringir la flexibilidad en diferentes entornos *blockchain*.
ION	◩ 0.75	La utilización del estándar *DID* de la *W3c* con la definición del método *DID-ION* en el sistema de resolución universal de identificadores [264] puede permitir el diseño de un módulo de interoperabilidad entre plataformas que soporten el estándar [196].
Shocard	☒ 0.0	La gestión de los identificadores *ShochardID* es parcialmente centralizada [102] y no permite exportar datos a un dispositivo secundario. Tampoco especifica soporte para multiples dispositivos o funcionalidades para eliminar datos de teléfonos extraviados [65].

Continúa en la siguiente página

Tabla 3.9 – continuación de la página anterior

Principio 9: Portabilidad		
Framework SSI		**Descripción**
Jolocom	☑ 0.5	Limitada. El protocolo se declara agnóstico facilitando el acoplamiento de conectores a otras redes como *bitcoin*, *BigchainDB* y *Quorum* [206].
Litentry	☑ 0.75	Ofrece una buena portabilidad al vincular los datos de identidad administrados en diferentes plataformas, permitiendo una gestión más flexible de la identidad digital. [210].
Civic	☒ 0.0	El sistema requiere un *token ERC-20* denominado *CVC* [257] para que los nodos validadores puedan vender la información verificada a los proveedores de servicios que requieran verificar la identidad de un usuario [102].
Idena	☒ 0.0	No ofrece portabilidad, ya que la identidad no puede ser transferida o utilizada en otros sistemas [240].
KILT	☑ 0.5	Aunque el diseño se basa en estándares abiertos, el protocolo no define mecanismos para la portabilidad [216].

TABLA 3.9: Nivel de cumplimiento del principio de portabilidad en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

Un factor clave es el uso de estándares abiertos, como en el caso de *Sovrin* e *ION*, que implementan estándares abiertos como *DID* de la W3C, lo que sienta las bases para una mejor portabilidad e interoperabilidad en el futuro. *uPort* y *Civic* están fuertemente acoplados a plataformas específicas (*Ethereum*), lo que limita su portabilidad; además, el requisito de *Civic* de usar un *token ERC-20* específico para la validación introduce una barrera adicional. *Litentry* se destaca por su capacidad para vincular datos de identidad de diferentes plataformas, ofreciendo una solución flexible y portable. *KILT* e *Idena*, carecen de mecanismos definidos para la portabilidad, lo que restringe severamente la flexibilidad de sus identidades digitales [2].

3.10.10 Principio de Interoperabilidad

La interoperabilidad posibilita que diferentes sistemas de identidad digital puedan comunicarse y trabajar conjuntamente, facilitando una adopción más amplia y una experiencia de usuario más fluida. La Tabla 3.10 evalúa aspectos clave como la implementación del estándar *DID*, el método *DID* utilizado, su versión, los formatos de datos soportados, y una descripción detallada de como cada *framework* aborda la interoperabilidad.

Principio 10: Interoperabilidad						
Framework SSI		**Estándar *DID***	**Método *DID***	**versión**	**Formatos**	**Descripción**
Sovrin	☑ 1.0	☑	*did-sov*	0.1	*JSON-LD*	Implementa el estándar *DID* y utiliza el método *did-sov* (versión 0.1) para conectarse a su *DLT* público [229]. Su interoperabilidad se limita a los sistemas de gestión de identidad compatibles con el sistema de resolución universal de identificadores [103], [102].

Continúa en la siguiente página

Tabla 3.10 – continuación de la página anterior

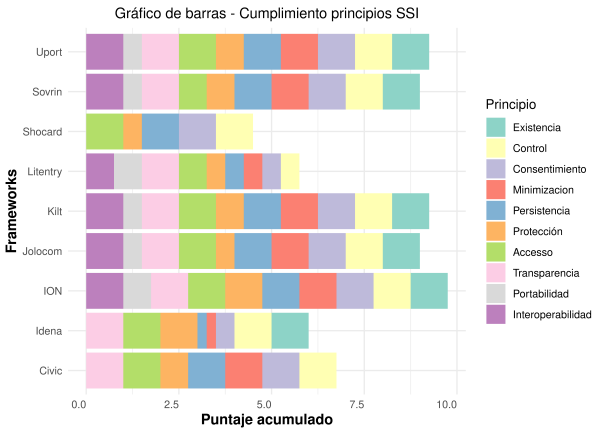
Principio 10: Interoperabilidad						
Framework SSI		**Estándar *DID***	**Método *DID***	**versión**	**Formatos**	**Descripción**
uPort	☑ 1.0	☑	*did-ethr*	2.4.0	*JSON*	Emplea un sistema de *Proxy* para gestionar la comunicación entre contratos inteligentes, facilitando el acceso a servicios de diversas aplicaciones [100], [75]. Utiliza el método *did-ethr* (versión 2.4.0).
ION	☑ 1.0	☑	*did-ion*	0.8.1	*JSON*	Despliega el método *did-ion* (versión 0.8.1) para conectarse a la red *ION*, implementando el protocolo *sidetree* sobre la *blockchain* de *Bitcoin* [229]. Su interoperabilidad también se limita a sistemas *IdMs* compatibles con la resolución universal de identificadores.
Shocard	☒ 0.0	☒	☒	☒	nombre: valor	No implementa un método *DID* de conexión, lo que limita significativamente su interoperabilidad con otros sistemas SSI.
Jolocom	☑ 1.0	☑	*did-jolo*	1.0	JWS	Utiliza el método *did-jolo* (versión 1.0) para conectarse a su sistema gestor de identidad [229]. Registra los *DID* en la *blockchain* de pruebas *Ethereum Rinkeby* y almacena los documentos *DID* en *IPFS* [206].La interoperabilidad se encuentra limitada a los *IdMs* habilitados en el sistema de resolución universal de identificadores.
Litentry	☑ 0.75	☒	☒	☒	No se describe	Se presenta como un agregador de identidad que integra *DID* bajo el estándar *W3C*, aunque no implementa un método *DID* propio [210].
Civic	☒ 0.0	☑	☒	☒	No se describe	No implementa un método *DID* de conexión propio, pero utiliza *DID* definidos por el estándar *W3C*, lo que permite cierto nivel de interoperabilidad con sistemas compatibles.
Idena	☒ 0.0	☒	☒	☒	*JSON*	No implementa un método *did* de conexión. Se espera que el identificador pueda ser vinculado con plataformas que requieran mantener una relación de uno a uno entre usuarios y cuentas, por ejemplo, una red social [240].
KILT	☑ 1.0	☑	*did-kilt*	2.4.1	*JSON*	Emplea el método *did-kilt* (versión 2.4.1) para conectarse a su protocolo [229], limitando su interoperabilidad a sistemas compatibles con la resolución universal de identificadores.

Tabla 3.10: Nivel de cumplimiento del principio de interoperabilidad en el conjunto de *frameworks* estudiados para el despliegue de una identidad digital autogobernada.
Fuente: Elaboración del autor.

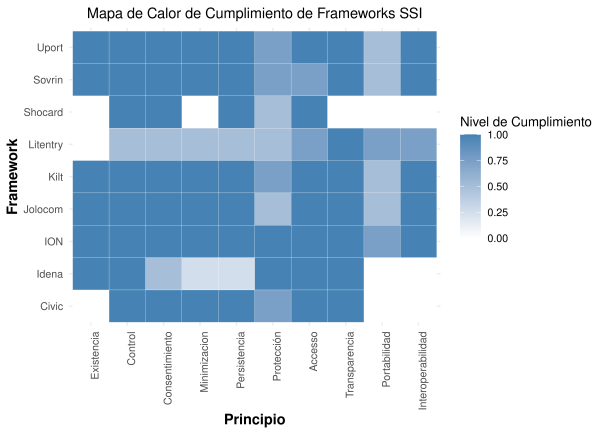
Se visualiza una adopción generalizada del estándar *DID*, donde la mayoría de los *frameworks* (6 de 9) implementan el estándar *DID* de la W3C, lo que sienta una base común para la interoperabilidad. *frameworks* como *Sovrin*, *uPort*, *ION*, *Jolocom* y *KILT* han desarrollado sus métodos *DID*, lo que les permite optimizar la interoperabilidad dentro de sus ecosistemas específicos. Además, *uPort* e *ION* utilizan *blockchains* ampliamente adoptadas como *Ethereum* y *Bitcoin*, lo que puede facilitar la integración con otros sistemas basados en estas plataformas. El uso de formatos como JSON y JSON-LD facilita el intercambio de datos entre diferentes sistemas. Por el contrario, *Shocard*, *Litentry*, *Civic* e *Idena* no implementan métodos *DID* propios, lo que puede limitar significativamente

su interoperabilidad en el ecosistema SSI, y la dependencia del sistema de resolución universal específicos puede crear silos de interoperabilidad, limitando la comunicación entre las plataformas [2].

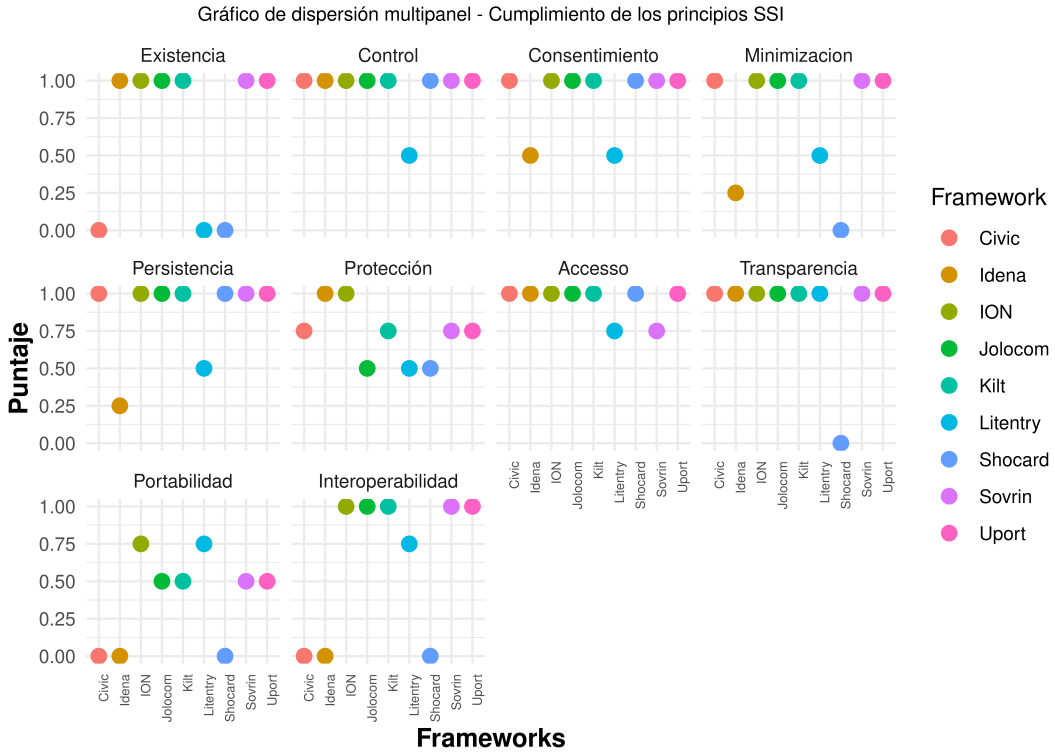
3.10.11 Conclusiones de la evaluación del nivel de cumplimiento de los principios SSI



A Barras apiladas. Tomado de: [2].



B Mapa de Calor.



C Vista multipanel.

FIGURA 3.2: Nivel de cumplimiento de los 10 principios de identidad digital autogobernada. Fuente: Elaboración del autor.

Las tablas desde la 3.1 hasta la 3.10 analizan el nivel de cumplimiento de los 10 principios de identidad autogobernada de Allen para el conjunto de *frameworks* SSI estudiados [223]. Cada tabla

muestra un *framework* SSI en las filas, y contiene por lo menos dos columnas adicionales. La primera columna presenta un indicador visual del nivel de cumplimiento de cada principio por parte del *framework* correspondiente. La segunda columna ofrece una descripción detallada de como se implementa dicho principio en el *framework* en cuestión. Esta presentación tabular permite una visualización clara y concisa del nivel de adherencia de cada *framework* a los principios de identidad autogobernada, facilitando así la comparación y evaluación de los diferentes enfoques. Además, en la Tabla 3.11 se consolida la valoración obtenida por cada *framework* y se visualiza en la Figura 3.2.

Framework	**Existencia**	**Control**	**Consentimiento**	**Minimización**	**Persistencia**	**Protección**	**Acceso**	**Transparencia**	**Portabilidad**	**Interoperabilidad**
Sovrin	1,00	1,00	1,00	1,00	1,00	0,75	0,75	1,00	0,50	1,00
Uport	1,00	1,00	1,00	1,00	1,00	0,75	1,00	1,00	0,50	1,00
ION	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	0,75	1,00
Shocard	0,00	1,00	1,00	0,00	1,00	0,50	1,00	0,00	0,00	0,00
Jolocom	1,00	1,00	1,00	1,00	1,00	0,50	1,00	1,00	0,50	1,00
Litentry	0,00	0,50	0,50	0,50	0,50	0,50	0,75	1,00	0,75	0,75
Civic	0,00	1,00	1,00	1,00	1,00	0,75	1,00	1,00	0,00	0,00
Idena	1,00	1,00	0,50	0,25	0,25	1,00	1,00	1,00	0,00	0,00
Kilt	1,00	1,00	1,00	1,00	1,00	0,75	1,00	1,00	0,50	1,00

Tabla 3.11: Consolidado del nivel de cumplimiento de los principio de identidad digital autogobernada en el conjunto de *frameworks* estudiados.
Fuente: Elaboración del autor.

La Figura 3.2 resalta que los *frameworks* evaluados cumplen satisfactoriamente con la mayoría de los principios de identidad autogobernada. Principios como transparencia, control y persistencia son implementados ampliamente, lo que indica un alto grado de control otorgado a los usuarios sobre su identidad digital. Este control es fundamental para la gestión autónoma y segura de los atributos de identidad personal, reduciendo la dependencia de intermediarios y fortaleciendo la privacidad del usuario.

No obstante, el análisis reveló una heterogeneidad en el cumplimiento de otros principios, como minimización, existencia y consentimiento. Esta variabilidad subraya la necesidad de un esfuerzo continuo para lograr una implementación uniforme de todos los principios esenciales en las soluciones SSI. *Frameworks* como *Sovrin*, *uPort*, *ION* y *Kilt* se destacan por su alto nivel de cumplimiento, logrando puntuaciones máximas en numerosas categorías. Estos incorporan mecanismos avanzados de divulgación selectiva y consentimiento, proporcionando a los usuarios un control granular sobre la información compartida. Sin embargo, presentan ciertas limitaciones en cuanto a la portabilidad, lo que podría restringir la flexibilidad del usuario para trasladar sus identidades entre distintas plataformas.

Por otro lado, *frameworks* como *Litentry* e *Idena* muestran un cumplimiento más variable, con puntuaciones bajas en varios principios, reflejando limitaciones en la implementación de características avanzadas. Particularmente, *Shocard* y *Civic* reciben puntuaciones bajas o nulas en existencia e interoperabilidad, indicando una dependencia excesiva de terceros y falta de compatibilidad con otros sistemas de identidad digital.

Una ventaja clave de los *frameworks* SSI es su capacidad para permitir a los usuarios crear y gestionar sus identidades de manera autónoma, sin depender de entidades centralizadas. Esto fomenta la privacidad y seguridad de los datos personales, ya que los usuarios mantienen control total de

sus atributos de identidad. Además, la mayoría utiliza tecnologías de vanguardia, como criptografía de curva elíptica y *blockchain*, para propender por garantizar la integridad y el no repudio de las identidades digitales. La variabilidad en las puntuaciones, especialmente en portabilidad e interoperabilidad, sugiere que estas áreas deberían ser prioritarias para el desarrollo futuro de un *framework* SSI. Mejorar estos aspectos podría resultar en sistemas de identidad más robustos y versátiles, facilitando su adopción en un contexto más amplio. El alto cumplimiento general en control y consentimiento es un resultado positivo, siendo estos principios fundamentales para la autonomía del usuario en la gestión de su identidad digital.

Sin embargo, una desventaja potencial de los *frameworks* SSI es su complejidad técnica inherente, lo cual puede dificultar su adopción por usuarios no técnicos. Además, la dependencia de dispositivos móviles y conexión a Internet para acceder y gestionar las identidades representa una limitación significativa en contextos donde estos recursos no están siempre disponibles o son poco confiables [2].

Capítulo 4

Aletheia: Un modelo de identidad digital descentralizada y autogobernada

En este capítulo se describe el modelo denominado Aletheia, diseñado para la gestión de una identidad digital descentralizada y autogobernada, utilizando tecnología de registro distribuido y almacenamiento descentralizado, orquestados en el diamante de la confianza. Aletheia busca proporcionar una representación verídica y verificable de la identidad digital de un individuo, garantizando el control total del usuario sobre su información. El modelo está fundamentado en la arquitectura de confianza de *Trust Over IP* (*ToIP*), estructurada en dos pilares principales: tecnología y gobernanza, que abarcan desde los identificadores descentralizados hasta la seguridad en la interacción entre entidades. Cada componente del modelo se describe con detalle, así como sus procesos clave para la emisión, almacenamiento y verificación de credenciales verificables.

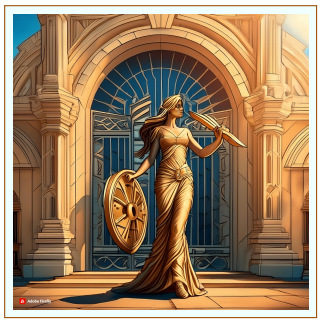


Figura 4.1: Aletheia: diosa de la verdad, la sinceridad y la revelación. Imagen generada con IA [265].

El modelo propuesto ha sido denominado **Aletheia**, en honor a la diosa griega que personifica la verdad, la sinceridad y la revelación. La naturaleza de esta diosa refleja profundamente la esencia y los objetivos fundamentales del modelo.

Aletheia simboliza el proceso de desvelamiento de la verdad, un concepto que está intrínsecamente relacionado con la privacidad, el control y la autenticidad, que son los pilares sobre los que se construye este modelo.

A continuación, se exponen detalladamente las razones que justifican esta denominación, subrayando cómo los principios encarnados por Aletheia encapsulan el objetivo de esta propuesta.

- Verdad y autenticidad: Aletheia representa la verdad, y el modelo propuesto proporciona una representación auténtica y verificable de la identidad digital de un individuo. DLT garantiza que la información sea inmutable y resistente a la manipulación, asegurando así su veracidad.
- Transparencia y revelación: Aletheia revela la verdad oculta y este modelo permite a los usua-

rios controlar la revelación de su información de identidad de manera granular y transparente, decidiendo que aspectos de su identidad compartir.

- Descentralización: Al no estar sometida al control de una divinidad superior, Aletheia representaba en la antigua cosmogonía una fuerza universal que actuaba como fuente de verdad. Esta característica se alinea con la naturaleza descentralizada del modelo, ya que la confianza se fundamenta en la solidez de las matemáticas proporcionada por los métodos criptográficos, los cuales aportan la fiabilidad necesaria a este sistema.
- Confianza: La verdad que Aletheia representaba era la base de la confianza en las relaciones humanas y divinas. El modelo basado en credenciales verificables y autogestionadas, establece una base sólida para la confianza en las interacciones digitales.
- Privacidad: Aletheia también simbolizaba la idea de que una verdad debe permanecer oculta hasta que sea oportuno revelarla. Esto se alinea con los principios de privacidad del modelo, donde los usuarios tienen control total sobre qué información comparten y en qué momento.
- Empoderamiento del usuario: Aletheia era una fuerza que motivaba a quienes buscaban la verdad. Este modelo empodera a los usuarios dándoles control total sobre sus identidades digitales.
- Integridad de los datos: La inmutabilidad de la *blockchain* y el almacenamiento en IPFS propenden por garantizar que la información de identidad mantenga su integridad, reflejando la naturaleza incorruptible de la verdad que Aletheia representaba.

Este capítulo está estructurado de la siguiente manera: en primer lugar, se presenta el marco de referencia para la confianza en Internet, conocido como *Trust Over IP*. A continuación, se detallan los requisitos específicos que deben cumplirse en cada capa para la construcción del modelo Aletheia, asegurando una implementación robusta y confiable. Finalmente, se proporciona una descripción detallada del modelo, que incluye tanto los artefactos de análisis y diseño como la información general sobre su implementación. Este enfoque integral permite comprender cada componente del modelo y su papel en la arquitectura general.

4.1 Marco de referencia

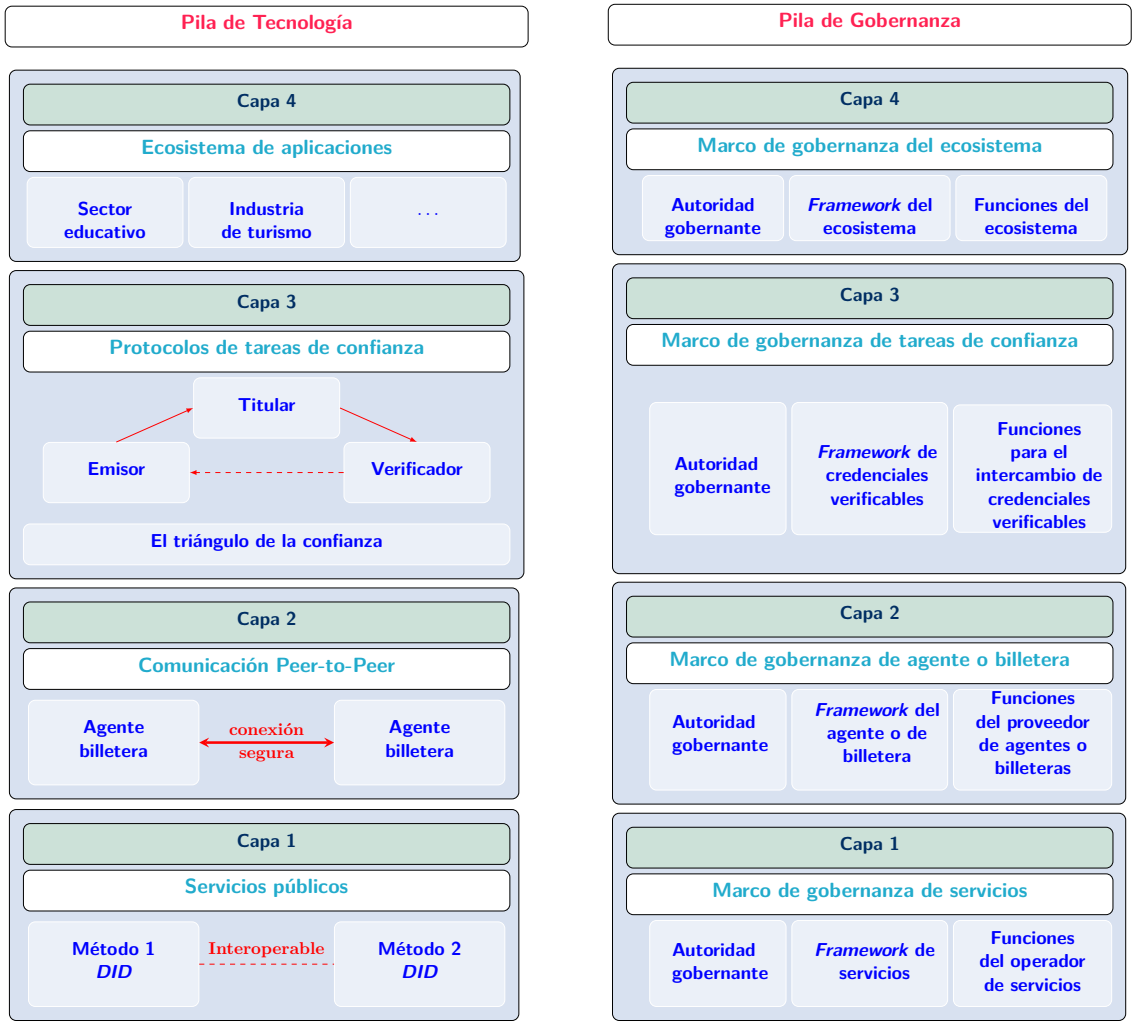
Un modelo de confianza medible para la identidad digital autogobernada basada en *blockchain* debe cumplir tres requerimientos: (a) la red se autocontrola mediante un esquema de gobierno y un algoritmo de consenso que genera confianza a partir de la misma, sin requerir un tercero de confianza, (b) las identidades son iguales, por lo cual nuevas identidades no tienen ventajas sobre las existentes previniendo ataques por reinicio de reputación, y (c) los proveedores de servicios son independientes y de forma libre aceptan o rechazan una afirmación realizada sobre un sujeto [91]. Estos tres requerimientos se pueden integrar en el modelo de confianza para la Internet [266].

4.1.1 Modelo de confianza para la Internet

El objetivo de este modelo es proporcionar una capa de confianza descentralizada en la Internet, que facilite el despliegue de servicios digitales a gran escala de manera segura y eficiente. Este marco conceptual organiza las funciones de comunicación en cuatro capas, agrupadas en dos categorías: técnica y normativa, conocidas como pilas (del término inglés *stacks*). En este modelo, las tecnologías de las capas superiores se benefician de la abstracción, ya que pueden utilizar los servicios de las capas inferiores sin depender de los detalles de implementación. En las secciones siguientes, estas agrupaciones se denominan pila tecnológica y pila de gobernanza. El componente tecnológico abarca la infraestructura necesaria para garantizar una comunicación confiable y segura entre las

entidades, asegurando la integridad y autenticidad de las interacciones. Por otro lado, el componente de gobernanza establece el marco normativo y regulador que define el contexto en el cual se crean, refuerzan o eliminan relaciones de confianza transitiva entre las partes involucradas.

Estos dos pilares se materializan en un modelo compuesto por cuatro capas esenciales, divididas en dos pilas (ver Figura 4.2), una de tecnología y otra de gobernanza [267], [266], [268].



A Pila de tecnología de *ToIP*.

B Pila de gobernanza de *ToIP*.

FIGURA 4.2: Arquitectura en capas del modelo de confianza propuesto por *ToIP*. Adaptado de [268].

- Pila de tecnología:
  1. Capa 1: servicios públicos orientados a la creación de los identificadores descentralizados y su interoperabilidad entre registros distribuidos o sistemas de almacenamiento descentralizados.
  2. Capa 2: comunicación *peer-to-peer* entre las billeteras de las entidades involucradas en una interacción. Una vez es establecida la comunicación, se mantiene de forma persistente hasta que una de las dos partes decide desconectarse. Esta capa previene el riesgo de desanonimización del usuario.
  3. Capa 3: protocolos de tareas de confianza para el intercambio seguro de credenciales. Esta capa se basa en el flujo de información asentado en el triángulo de la confianza, el

cual no requiere una integración directa entre emisor y verificador para generar confianza en el sistema, ya que la verificación de información se da mediante pruebas criptográficas publicadas en un registro de datos público y verificable, por ejemplo una blockchain. Por lo tanto, la confianza entre emisor y verificador se obtiene de forma transitiva, a partir de las relaciones dada entre emisor-titular y titular-verificador. Por su parte, la confianza de las credenciales verificables es relacional, direccional, contextual y limitada. Se considera relacional puesto que una credencial es emitida por un emisor con destino a un único poseedor en una relación preestablecida, direccional dado que la credencial fluye del emisor hacia el titular, y del titular hacia el verificador; contextual, en virtud que cada credencial se emite bajo un contexto dado, el cual a su vez la limita [267].

4. Capa 4: el ecosistema de aplicaciones define los requerimientos para la implementación de un caso de uso específico soportado en la utilización de identificadores descentralizados y credenciales verificables.

- Pila de gobernanza:
  1. Capa 1: el marco de gobernanza de servicios públicos establece el mecanismo para la generación de los identificadores descentralizados y su publicación en un registro distribuido.
  2. Capa 2: el marco de gobernanza sobre los agentes o las billeteras digitales, establece el uso de estándares para la seguridad y privacidad de la información almacenada en las billeteras, y posibilitar escenarios de interoperabilidad entre estos.
  3. Capa 3: el marco de gobernanza de tareas de confianza determina las reglas para el registro de emisores y verificadores, definiendo el contexto para emisión y transferencia de credenciales verificables a los titulares de los derechos de identidad. La autoridad de gobernanza define las políticas legales o comerciales que rigen la expedición de credenciales verificables, generando nuevamente un triángulo de confianza entre emisores y verificadores. Este par de triángulos, uno técnico y otro normativo forman una estructura denominada el diamante de confianza de la gobernanza digital [267].
  4. Capa 4: el marco de gobernanza del ecosistema define los procedimientos para la auditoría del ecosistema y la gestión de las capas inferiores, garantizando la integridad de la información en todo el sistema.

4.2 Requerimientos de Aletheia

En la Figura 4.3 se presenta un esquema de alto nivel del modelo Aletheia diseñado conforme a la arquitectura de confianza de *ToIP*. Este diagrama muestra el diamante de gobernanza, compuesto por dos triángulos: el triángulo superior, cuyos vértices son el emisor, el poseedor y el verificador; y el triángulo inferior, que conecta al emisor, el verificador y la autoridad de gobierno. Este esquema resalta la direccionalidad de las relaciones de confianza, así como el flujo de información entre las entidades involucradas. La Figura 4.3 se describe a profundidad en la sección 4.3.

Las secciones que siguen detallan los requisitos para el diseño e implementación del caso de prueba implementado para el despliegue de un sistema de identidad autogobernada basado en blockchain. Para la definición de estos requisitos, se empleó la metodología *EARS* (*Easy Approach to Requirements Syntax*) [269], que ofrece una sintaxis clara y estructurada, facilitando así su documentación y comprensión. EARS organiza los requisitos en secciones lógicas de manera jerárquica y permite su descripción en lenguaje natural, utilizando etiquetas estándar como 'debe', lo que simplifica su actualización a lo largo del ciclo de vida del proyecto. Aunque *EARS* no cuenta con un estándar formal para su adopción, y su enfoque basado en lenguaje natural puede limitar la expresión de

requisitos técnicos complejos, su estructura flexible permite la integración con diversas metodologías de desarrollo. Sin embargo, es fundamental realizar revisiones continuas para eliminar posibles ambigüedades y garantizar que los requisitos se mantengan claros y precisos.

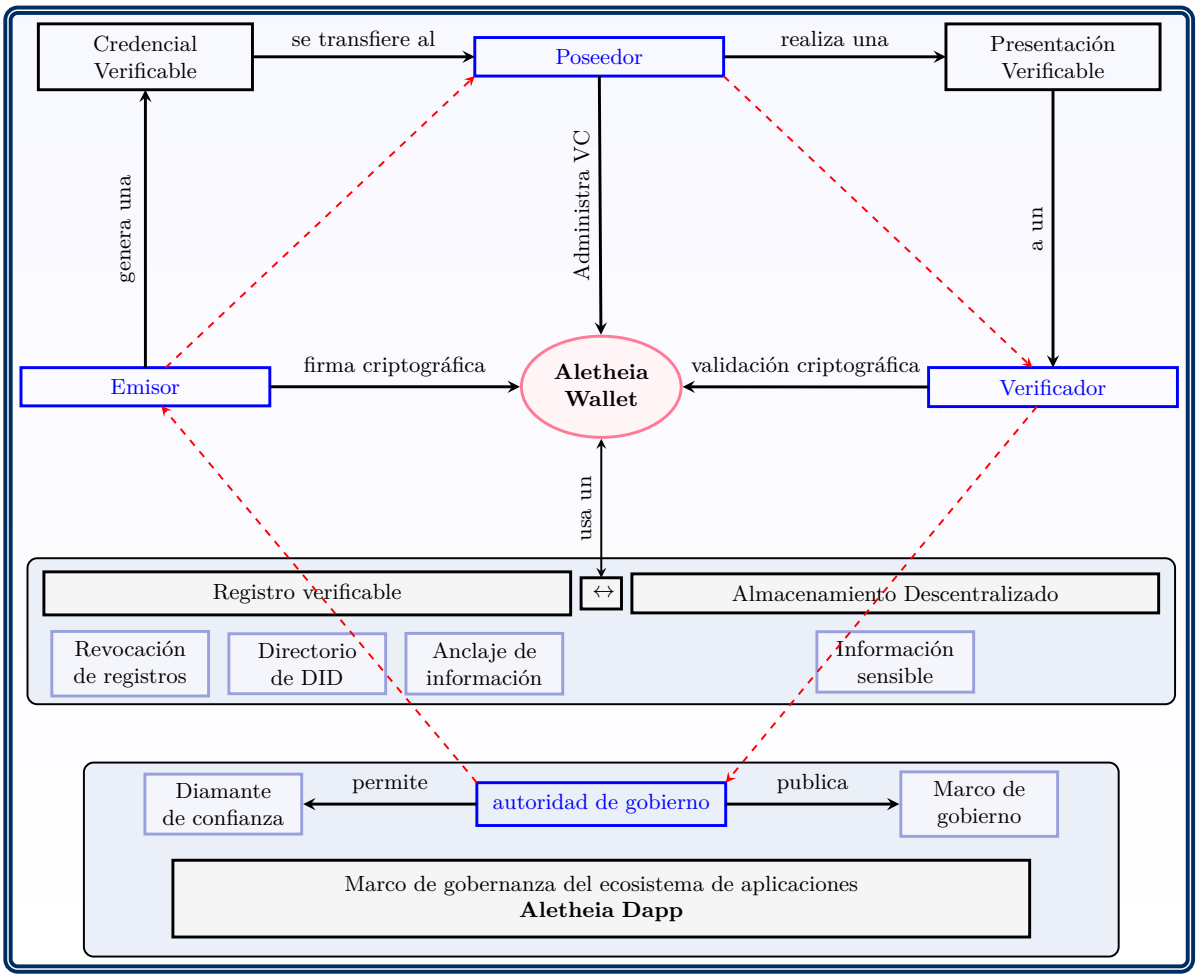


FIGURA 4.3: Vista de alto nivel de Aletheia: un modelo basado en DLT para el despliegue de una identidad autogobernada.
Fuente: Elaboración propia.

4.2.1 Descripción de entidades

1. Titular de derechos de identidad (**Poseedor**): Es el propietario de las afirmaciones que se emitan sobre su identidad. Se referencia por medio de un identificador descentralizado. El Poseedor usualmente es la entidad que tiene bajo su control el *DID*.

2. Emisor de credenciales verificable (**Emisor**): Es el responsable de emitir las afirmaciones de una entidad, bajo el esquema definido por la autoridad de gobierno para las credenciales verificables. Una vez ha sido emitida la credencial es transferida a su respectivo Poseedor. Los datos asociados a la credencial son cifrados con la llave pública del Poseedor, por lo cual solamente el titular tendrá acceso.

3. Verificador de credenciales (**Verificador**): Esta entidad comprueba la validez de una credencial verificable presentada por un Poseedor bajo un contexto determinado, y puede aceptarla o rechazarla conforme al resultado de la comprobación criptográfica de la misma.

4.2.2 Aletheia *Wallet*

El modelo planteado requiere una billetera digital denominada Aletheia *Wallet*, diseñada para recibir y presentar las credenciales verificables de un poseedor. Su objetivo principal es fortalecer la confianza en las transacciones digitales, asegurando la autenticidad y verificabilidad de la información compartida. La construcción de Aletheia *Wallet* se fundamenta en la recomendación *CHAPI* (*Credential Handler API*) [270], propuesta por el grupo de credenciales de la W3C. *CHAPI* se erige como un componente esencial no solo para el modelo Aletheia, sino también para los emergentes sistemas de identidad digital autogobernada, dado que potencia significativamente la interoperabilidad. La adopción de *CHAPI* representa un avance significativo en el flujo de las credenciales verificables. Al facilitar un intercambio seguro y privado de VC a través del navegador, *CHAPI* permite que Aletheia *Wallet* interactúe de manera confiable con emisores y verificadores de terceros. Este enfoque no solo preserva la privacidad y el control de las entidades, sino que también promueve un ecosistema descentralizado.

4.2.3 Aletheia-Dapp

Cómo escenario de validación se ha diseñado un caso de uso específico para la prueba de concepto del modelo de Aletheia. Este escenario se describe en el marco de gobernanza (ver sección 5.1), el cual está inmerso dentro de pila de gobernanza del *ToIP* (ver sección 4.1.1).

4.2.4 Requerimientos por capa *ToIP*

4.2.4.1 Requerimientos en la capa 1: utilidad pública

4.2.4.1.1 Creación de identificadores descentralizados: Una entidad para ser habilitada en el sistema debe realizar el proceso de registro en Aletheia *Wallet* establecido dentro del marco de gobernanza (ver sección 5.1.1). Esta inscripción crea y asigna un identificador descentralizado a la entidad, la cual tendrá la responsabilidad de administrar y realizar la copia de seguridad de las llaves criptográficas asociadas a su *DID*.

Tareas:

- Establecer un método para la creación de identificadores descentralizados conforme a los requerimientos definidos por la W3C, los cuales se agrupan en cuatro categorías: descentralización, persistencia, verificación criptográfica y resolución [271].

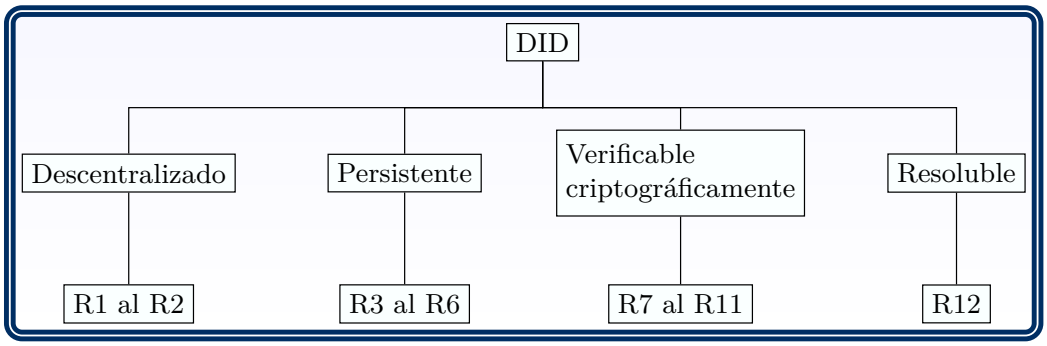


Figura 4.4: Requerimientos esenciales para la creación de un *DID*.
Adaptado de [271].

Los requerimientos asociados al *DID* se presentan en la Figura 4.4, y su descripción se realiza en la Tabla 4.1, discriminados en requerimientos funcionales (F) y no funcionales (NF).

N.	Tipo	Nombre	Prioridad	Descripción
R1	F	Unicidad	Debe	Cuando un *DID* es creado, entonces debe ser único y su propiedad es intransferible.
R2	NF	Usabilidad	Debería	El sistema deberá ser amigable y no requerir conocimientos especializados para su uso.
R3	NF	Globalidad	Debería	Un *DID* deberá ser válido y utilizable globalmente, independiente de la jurisdicción de creación y sin posibilidad de revocación administrativa.
R4	NF	Bajo costo	Debería	El sistema deberá minimizar los costos de mantenimiento y verificación, y no depender de un proveedor específico.
R5	F	Resistencia	Debería	Si la entidad emisora desaparece, entonces el *DID* deberá seguir siendo válido y funcional.
R6	F	Flexibilidad de Registro	Debería	Un *DID* deberá ser almacenable y verificable en cualquier tipo de registro.
R7	F	Autenticación	Debe	Cuando se solicita, el sistema debe permitir a la entidad probar que tiene control sobre un *DID* mediante pruebas criptográficas.
R8	F	Independencia del Emisor	Debe	La verificación y autenticación de un *DID* no debe requerir comunicación con el emisor.
R9	F	Privacidad	Debe	El sistema debe garantizar que solo la información necesaria sea revelada durante las transacciones, protegiendo la información sensible.

Tabla 4.1: Requerimientos propuestos por la W3C para la implementación de *DID*, reformulados según el formato *EARS*. Adaptado de [271].

- El registro de una entidad con la respectiva generación de DID debe ser habilitado en la billetera digital, y el *DID* obtenido deberá ser utilizado para la creación del usuario en un caso específico de uso.

N.	Tipo	Nombre	Prioridad	Descripción
R10	F	Creación de usuario	Debe	La entidad debe crear una cuenta de inicio en Aletheia *Wallet* (ver Figura 5.1), compuesta por un alias de usuario y su contraseña. Una vez esta cuenta ha sido creada, entonces se deberá vincular el *DID* en Aletheia-Dapp (ver Figura 5.2). En cado caso se debe permitir realizar la copia de seguridad de las llaves criptográficas.
R11	F	Inicio de sesión	Debe	Las entidades deben poder iniciar sesión tanto en la billetera digital como en el caso de uso mediante su alias de usuario y contraseña.

Tabla 4.2: Requerimientos para el registro y autenticación de una entidad.
Fuente: Elaboración propia.

4.2.4.2 Requerimientos en la capa 2: Infraestructura técnica de confianza

4.2.4.2.1 Comunicación segura *end-to-end*: Establece las características del canal de comunicación entre dos entidades para asegurar un intercambio de información seguro bajo un entorno confiable.

Tareas:

- Implementar un método de comunicación seguro y privado entre emisor y receptor, independiente del protocolo de transporte, por lo cual no se requerirá de intermediarios que aseguren la información para su transmisión. La confidencialidad de la comunicación estará dada por la interacción mediada por *DID* combinado con un mecanismo para el cifrado/descifrado de información que preserve la privacidad de los datos almacenados.

Los requerimientos asociados a esta capa se presentan en la Tabla 4.3.

N.	Tipo	Nombre	Prioridad	Descripción
R12	F	Custodia de llaves criptográficas	Debe	La billetera digital deberá permitir realizar la copia de seguridad de las llaves criptográficas y utilizarlas sin la necesidad de un intermediario.
R13	NF	Protocolo de comunicación unificado	Debe	El sistema deberá garantizar que todos los agentes o billeteras digitales conectados utilicen un protocolo de comunicación único para maximizar la interoperabilidad y minimizar las interfaces de interconexión. Para este caso se deberá utilizar *CHAPI*.

Tabla 4.3: Requerimientos para la implementación de la capa 2 para *ToIP* reformulados conforme al formato *EARS*. Adaptado de [268].

4.2.4.3 Requerimientos en la capa 3: Diamante de la confianza

4.2.4.3.1 Implementación de un panel de control para la gestión de credenciales verificables: Un Titular de los derechos de identidad podrá realizar solicitudes de emisión de credenciales verificables, consultar el estado de las mismas y almacenar en Aletheia *Wallet* las credenciales emitidas para su posterior presentación ante una entidad verificadora.

Tareas:

- Desarrollar un módulo para el despliegue de las credenciales verificables asociadas a un Poseedor, consultar las VC emitidas y posibilitar su almacenamiento en la billetera digital mediante una interface *CHAPI*.
- Implementar la solicitud de emisión de una VC dirigida a un emisor habilitado en Aletheia-Dapp. La VC emitida es direccionada al Poseedor.
- Diseñar un módulo para que un titular genere presentaciones verificables de una o más credenciales de forma segura, privada y con divulgación selectiva de las mismas. El verificador debe estar registrado en la Aletheia-Dapp.

Los requerimientos derivados de esta capa se presentan en la Tabla 4.4.

N.	Tipo	Nombre	Prioridad	Descripción
R14	F	Emisión de VC	Debe	Un emisor podrá consultar el listado de solicitud recibidas y seleccionar la VC que desea generar. Una vez procesada la remitirá al titular correspondiente.
R15	F	Almacenamiento de datos privados	Debe	Cuando se almacena información privada, entonces debe ser cifrada y guardada en un sistema de archivos descentralizado, como *IPFS*.
R16	F	Registro de credenciales	Debe	Cuando se crea una credencial verificable, entonces debe ser anclada en un sistema de almacenamiento descentralizado o registro distribuido.
R17	F	Listado de VC	Debe	El *dashboard* permitirá visualizar el listado de credenciales verificables de un Poseedor o aquellas que se encuentran pendientes de emisión.
R18	F	Presentación verificable de VC	Debe	Cuando un titular desea probar su identidad o atributos, entonces debe poder construir y presentar credenciales de manera verificable, revelando selectivamente la información necesaria.
R19	F	Verificación criptográfica	Debe	Cada vez que se presenta una VC, debe estar firmada digitalmente con la llave privada del *DID* correspondiente para garantizar su autenticidad.
R20	NF	Privacidad por diseño	Debe	Si se realiza una transacción, entonces el sistema deberá asegurar que solo se revele la información mínima y necesaria.
R21	NF	Confianza transitiva	Debe	Si una entidad confía en otra a través de una credencial verificable, entonces esa confianza puede ser extendida a terceras partes de manera transitiva.
R22	NF	Compatibiliad en navegadores	Debe	El *dashboard* deberá ser compatible con los principales navegadores web, incluyendo *Chrome*, *Firefox* y *Opera*. La experiencia del usuario debe ser coherente en todas las plataformas.

Tabla 4.4: Requerimientos para la implementación de la capa 3 para *ToIP* reformulados conforme al formato *EARS*. Adaptado de [268].

4.2.4.4 Requerimientos en la capa 4: Nivel de aplicación

Definición del marco de gobernanza que establece el nivel de persistencia, confidencialidad, privacidad e integridad de la información almacenada como *DID* y VC (ver sección 5.1). Este marco propenderá por garantizar estas características dado el diseño por privacidad aplicado y las propiedades intrínsecas de la tecnología de registro distribuido combinadas con un almacenamiento descentralizado. Los requerimientos asociados se listan en la Tabla 4.5.

N.	Tipo	Nombre	Prioridad	Descripción
R23	NF	Marco de gobernanza	Debe	Cuando se construye un sistema de identidad autogobernada, debe seguir un conjunto de procedimientos y reglas específicos que aseguren la confianza digital y la sostenibilidad a lo largo del tiempo para todos los participantes.
R24	NF	La confianza es direccional	Debe	Si la entidad X confía en la entidad Y, no implica automáticamente que Y confíe en X, a menos que se establezca explícitamente.

Continúa en la siguiente página

Tabla 4.5 – continuación de la página anterior

N.	Tipo	Nombre	Prioridad	Descripción
R25	NF	La confianza depende del contexto	Debe	Si se establece una relación de confianza, esta será válida solo dentro del contexto específico en el que fue creada.
R26	NF	La confianza tiene límites	Debe	Cuando se verifica una credencial, el marco de gobernanza debe establecer reglas claras para su validación.

Tabla 4.5: Requerimientos para la implementación de la capa 4 para *ToIP* reformulados conforme al formato *EARS*. Adaptado de [268].

4.2.5 Requerimientos tecnológicos

Para la implementación del caso de estudio, se dispone de un conjunto específico de requerimientos tecnológicos que garanticen la correcta configuración y desempeño del sistema. Estos requerimientos abarcan tecnologías de registro distribuido como una blockchain privada tipo *ethereum*, sistemas de almacenamiento descentralizado como *IPFS*, y herramientas de desarrollo especializadas incluyendo librerías y *frameworks*. Además, se especifican las configuraciones de *hardware* necesarias para soportar las operaciones y procesos involucrados. La Tabla 4.6 presenta una lista detallada que enumera cada uno de estos componentes tecnológicos, indicando sus respectivas versiones.

Requerimiento	Descripción
Tecnología de registro distribuido	*Blockchain* privada tipo *ethereum*, desplegada en un entorno para pruebas simulado mediante *Ganache* Versión 2.7.1 [272].
Sistema de almacenamiento descentralizado	*InterPlanetary File System* (*IPFS*) [20] desplegado a través del servicio ofrecido por Pinata [273].
Docker	Versión 27.2.1 [274]. Despliegue rápido de *Mysql*, Versión 8.0.33 y *Remote Dictionary server*, versión 7.4.2 [275].
Web3.js	Librería Javascript para interacción con la *blockchain* de *ethereum* [276].
Nodejs	Entorno de ejecución de *JavaScript* Versión 21.7.1 [277].
Smart contracts	Se desarrollarán en *Solidity* Versión 0.8.0 [278].
Librería *DidKit*	Se utilizarán los métodos *DID-Key* para la generación de identificadores descentralizados. Además se tomará como la base la demo de *Chapi Wallet* y de aplicación con *spring boot* generadas para esta libreria [279].
Frontend	Svelte Versión 3.0.0 [280], *Spring Boot* [281].
Sistema Operativo	Ubuntu 22.04.3 LTS (*Jammy Jellyfish*)
CPU	*AMD Ryzen* 7 2700 o superior
RAM	16 GB o superior.
Almacenamiento	8 GB o superior.

Tabla 4.6: Requerimientos tecnológicos para el desarrollo de caso de estudio. Fuente: Elaboración propia.

4.3 Aletheia: Modelo de identidad digital autogobernada

La arquitectura general de Aletheia se presentó en la Figura 4.3, su diseño propende por garantizarle al titular de los derechos de identidad el control sobre el acceso a su información personal y que sea la máxima autoridad sobre esta. La seguridad y privacidad de la información se basa en la aplicación de la criptografía asimétrica, siendo su utilización transparente para cada entidad. El modelo dispone de una billetera digital denominada Aletheia *Wallet* que permite la interacción de los usuarios en el caso de uso, gestiona los identificadores descentralizados y posibilita la administración de las credencias verificables. Además, la arquitectura esta compuesta por cuatro capas conforme a la propuesta de *Trust Over IP* [266]. Los requerimientos de cada una de las capas se presentaron en la sección 4.2.

4.3.1 Descripción general

El modelo se fundamenta en la interacción de tres entidades principales: Poseedor, Emisor y Verificador, cuyas características se detallan en la sección 4.2.1. Para participar en el caso de uso, cada entidad debe configurar previamente su billetera digital. Este proceso implica: Crear un nombre de usuario y una contraseña de acceso, que se almacenan localmente para prevenir el uso no autorizado del dispositivo, generar el *DID* de la entidad y permitir la realización de una copia de seguridad de las llaves criptográficas asociadas. Es crucial que cada entidad posea un *DID* único, ya que este garantiza su identificación inequívoca en el sistema. La Figura 4.3 muestra el modelo de almacenamiento de datos que utilizan las capas de la arquitectura. La persistencia se realiza *on-chain* y *off-chain*. La cadena de bloques funciona como un registro verificable donde se dispone de un directorio de *DID* de las entidades habilitadas y se realice el anclaje de los datos sensibles almacenados fuera de esta. El almacenamiento *off-chain* utiliza un sistema de archivos descentralizado como *IPFS* para guardar la información cifrada asociada a las credenciales verificables y que se accede a través del *hash* notarizado en la *blockchain* por medio de contratos inteligentes.

4.3.2 Descripción de la arquitectura

El caso de uso se basa en una arquitectura multicapa, donde los componentes se organizan según sus responsabilidades. Cada capa interactúa únicamente con su capa adyacente, lo que favorece una mayor mantenibilidad, escalabilidad y facilidad para la ejecución de pruebas.

Aletheia-Dapp está formada por las siguientes capas:

1. Capa de Presentación: Compuesta por las vistas y los controladores. Las vistas representan la interfaz gráfica de usuario para la interacción con el sistema y los controladores procesan las solicitudes HTTP, invocan los servicios y utilidades necesarios y preparan los datos para su envío a las vistas.

2. Capa de Servicios: Contiene la lógica de negocio conforme al marco de gobernanza establecido, y actúa como un intermediario para coordinar los requerimientos de información por parte de los controladores hacia los repositorios de datos.

3. Capa de Acceso a Datos: Contiene los repositorios encargados de la interacción con las bases de datos y los sistemas de persistencia de la información. Esta capa se encuentra compuesta por: una base de datos relacional *MySQL* para la gestión de usuarios en el caso de uso ya que no se dispone de un modelo descentralizado de reputación, un servicio de caché (*REDIS*) para mejorar el rendimiento de la aplicación reduciendo la latencia al procesar datos en memoria

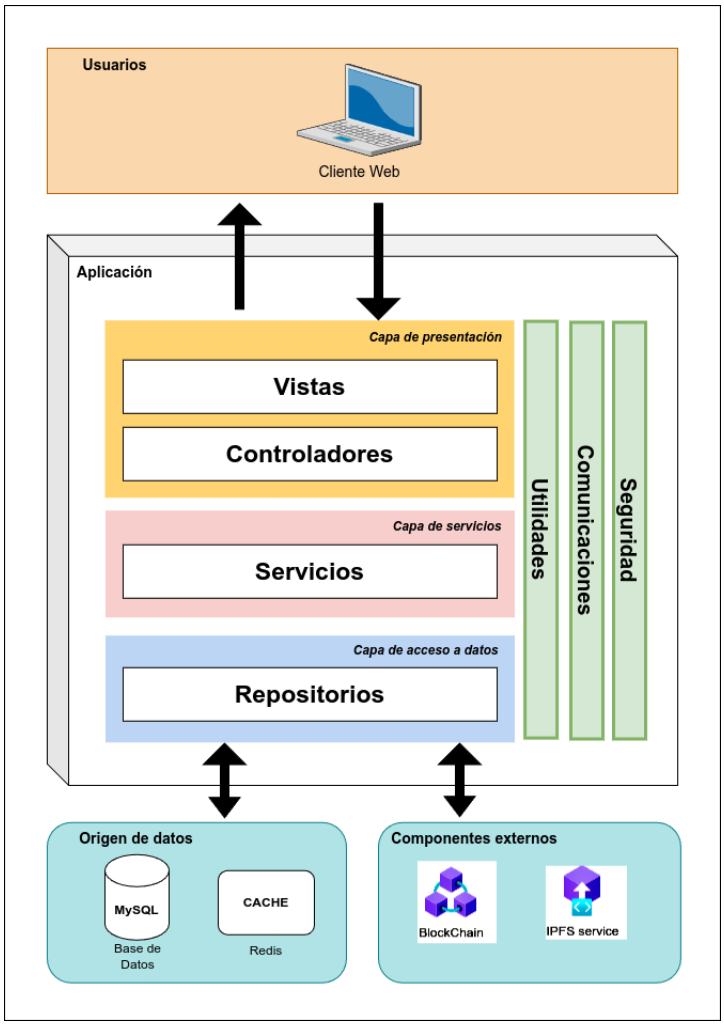


FIGURA 4.5: Diagrama de componentes para Aletheia-Dapp.
Fuente: Elaboración propia.

principal, una *blockchain* para el registro inmutable y trazable de transacciones, y por último, un sistema de almacenamiento descentralizado basado en contenido como *IPFS*, que permite preservar la información bajo un esquema eficiente y descentralizado.

4. Capa de Utilidades: Contiene funciones y clases de apoyo que pueden ser utilizadas a través de las diferentes capas de la aplicación. Estas pueden incluir validaciones, conversiones de formato, manejo de excepciones, librerías criptográficas, entre otros.

El diagrama de la arquitectura se ilustra en la Figura 4.5, en la cual se observa un diseño modular y escalable, que facilitará el mantenimiento y evolución de la aplicación. *Blockchain*, *IPFS*, *Redis* son tecnologías que le ofrecen al modelo eficiencia, seguridad y gestión de grandes volúmenes de datos, bajo un ambiente descentralizado y de alta disponibilidad.

4.3.3 Diagramas de flujo para credenciales verificables

El modelo planteado se basa en un intercambio confiable de credenciales verificables. Esta sección presenta cuatro diagramas de flujo que explican el comportamiento del caso de uso en los procesos críticos referentes a la creación de VC, su visualización y persistencia, la construcción de una

presentación verificable dirigida a un verificador y la comprobación de la misma por parte de esta entidad. Estos diagramas proporcionan una visión clara de cómo Aletheia gestiona de forma segura y privada las VC. En la sección 5.3 se elabora un seguimiento detallado del flujo de información con el objeto de validar el modelo.

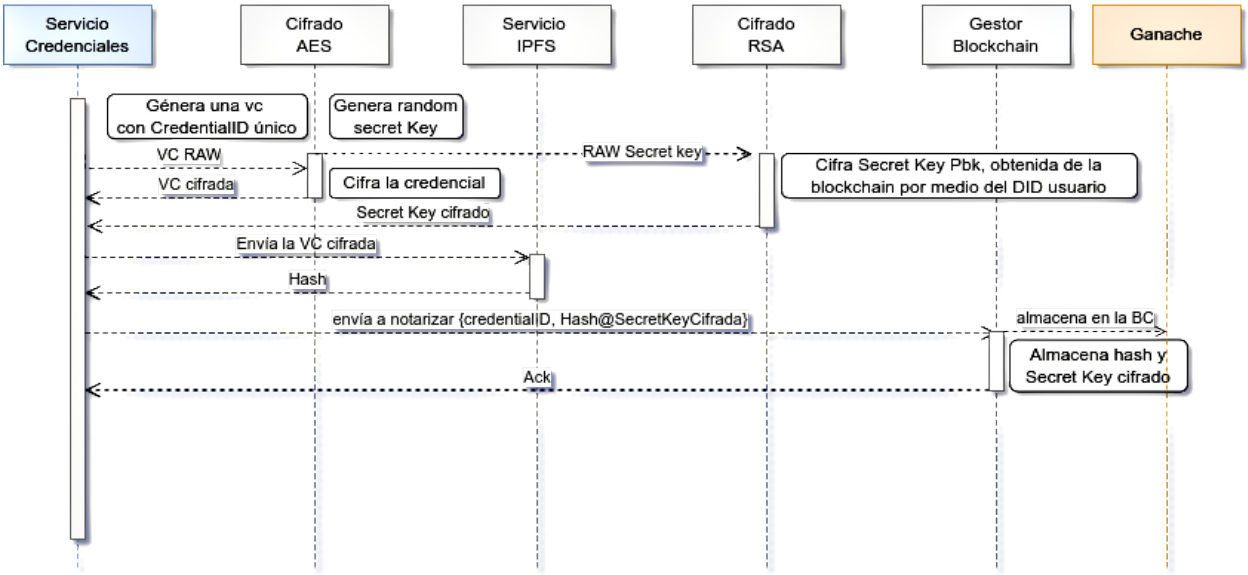


FIGURA 4.6: Generación de una credencial verificable.
Fuente: Elaboración propia.

1. Emisión de una credencial verificable: El diagrama de flujo de la Figura 4.6 ilustra el proceso necesario para que una entidad Emisor pueda generar correctamente una petición de emisión de una VC realizada por un usuario Poseedor. El flujo inicia con una solicitud de emisión, se valida el requerimiento conforme al marco de gobernanza y se genera la VC con la afirmación (*claim*) solicitada. Luego, se cifra la VC para su carga en el servicio *IPFS*, y por último, se notariza en la *blockchain* mediante el llamado a un contrato inteligente.

   A continuación se analiza cada paso involucrado en la emisión de una VC:

   (a) El proceso comienza con el "Servicio Credenciales", donde un emisor selecciona una solicitud realizada por un posible Poseedor, verifica el cumplimiento del marco de gobernanza y genera la VC con un UUID único (CredentialID).

   (b) El servicio de "Cifrado AES" genera una clave secreta aleatoria mediante el algoritmo AES.

   (c) El "Servicio Credenciales" envía la VC sin cifrar (VC *RAW*) al servicio de "Cifrado *AES*".

   (d) El "Cifrado *AES*" cifra la credencial utilizando la clave secreta generada y retorna la VC cifrada al "Servicio Credenciales".

   (e) El "Cifrado *AES*" envía la clave secreta sin cifrar al servicio de "Cifrado *RSA*".

   (f) El "Cifrado *RSA*" cifra la clave secreta AES con la llave pública del usuario, la cual es recuperada de la *blockchain* por medio del *DID*. La clave cifrada es retornada al "Servicio Credenciales".

   (g) El "Servicio Credenciales" envía la VC cifrada al "Servicio *IPFS*".

   (h) El "Servicio *IPFS*" genera un *hash* de la VC cifrada.

(i) El "Servicio de Credenciales" envía el identificador de la VC, el *hash* obtenido y la clave secreta cifrada al "Gestor *Blockchain*".

(j) El "Gestor *Blockchain*" almacena el *hash* y la clave secreta cifrada en la *blockchain*. En este caso se comunica con la red privada de pruebas desplegada con *Ganache*.

(k) Finalmente, el "Gestor *Blockchain*" envía una confirmación (*ACK*) de vuelta al "Servicio *IPFS*", que a su vez lo transmite al "Servicio Credenciales", completando así la emisión.

Este enfoque permite que solo el usuario autorizado pueda acceder a la información, lo que es fundamental en un entorno de identidad autogobernada, donde los usuarios tienen el control completo sobre sus datos. Al utilizar tanto cifrado asimétrico (*RSA*) como simétrico (*AES*), el sistema maximiza la seguridad en todo el proceso, desde la emisión hasta la visualización de la credencial. La combinación de *IPFS* para almacenamiento descentralizado y *blockchain* para el registro de transacciones, asegura que los datos se mantengan íntegros y verificables en todo momento.

2. Visualización y Almacenamiento: La Figura 4.7 es un diagrama de secuencia del proceso de recuperación y visualización de una credencial verificable. En primer lugar, se procede a la recuperación de la VC desde *IPFS*, su descifrado y la presentación al Poseedor. Y, en segundo lugar, se realiza su almacenamiento seguro en Aletheia *wallet*, según los pasos indicados en la Figura 4.8.

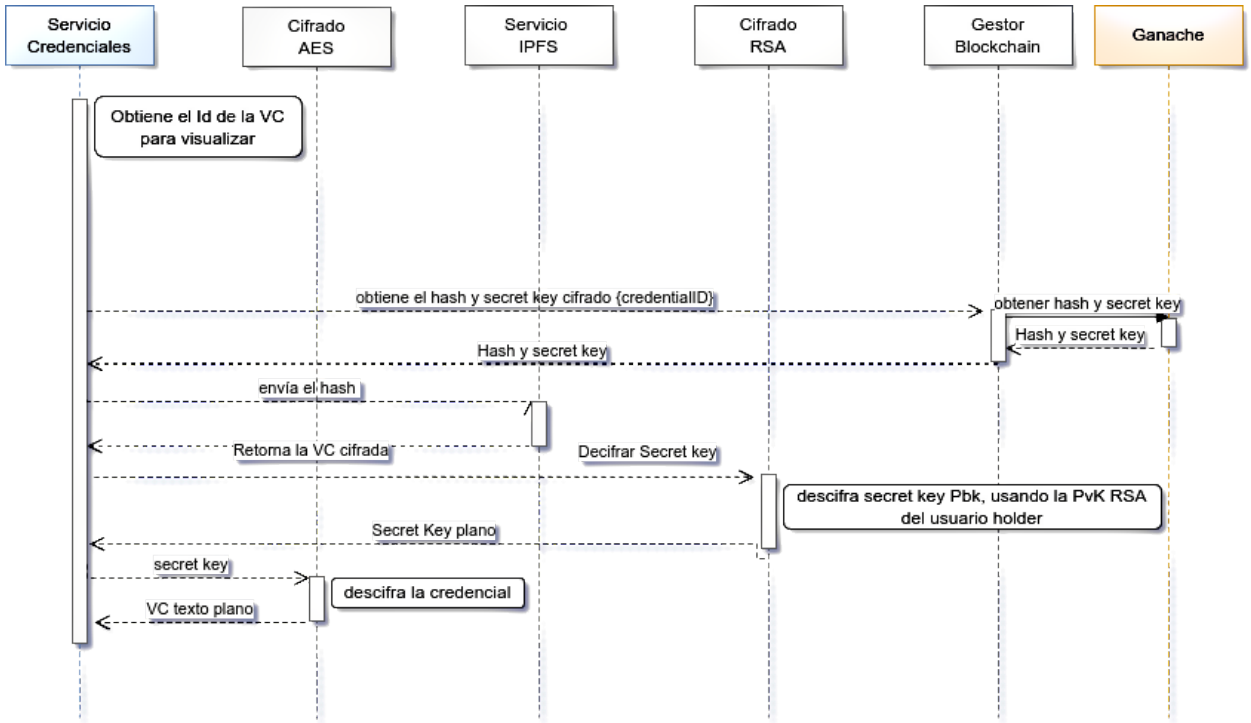


FIGURA 4.7: Visualización de una credencial verificable.
Fuente: Elaboración propia.

La Figura 4.7 contiene el proceso para recuperar credenciales, que involucra desde la obtención del ID hasta la visualización en texto plano, pasando por varios servicios involucrados en el proceso de cifrado y almacenamiento:

(a) El "Servicio Credenciales", inicia el proceso obteniendo el Token de certificado de la VC que se desea visualizar. Este identificador actúa como referencia para acceder a la VC

almacenada en *IPFS* de forma cifrada.

(b) El "Servicio Credenciales" se comunica con "*Ganache*" para obtener el *hash IPFS* y la *secret key* AES cifrada, utilizando el ID de la credencial. Esta información se encuentra en la transacción de creación de la VC. "*Ganache*" devuelve el *hash IPFS* y la *secret key* AES al "Servicio Credenciales".

(c) El "Servicio de Credenciales" envía el *hash IPFS* obtenido al "Servicio *IPFS*". Luego, el "Servicio *IPFS*" devuelve la VC cifrada al "Servicio de Credenciales".

(d) 'El "Servicio de Credenciales" envía la clave secreta *AES*, cifrada con la clave pública *RSA* del usuario "estudiante.1-Dapp", al módulo de "Cifrado *RSA*". Este módulo se encargará de descifrarla utilizando la clave privada *RSA* del usuario. Una vez descifrada, la clave secreta en su forma de texto plano es enviada de vuelta al "Servicio de Credenciales". Este proceso garantiza que solo el titular pueda acceder a la clave secreta AES.

(e) El "Servicio de Credenciales" utiliza esta clave secreta para descifrar la VC, que en este punto todavía está cifrada.

(f) El proceso concluye con el "Servicio Credenciales" con una VC descifrada y convertida en un formato de texto plano, haciendo que el contenido de la credencial sea legible y accesible para el usuario.

La visualización de una VC en Aletheia se basa en un modelo de seguridad que combina eficientemente mecanismos de cifrado simétrico y asimétrico, potenciando tanto la confidencialidad como la integridad de las credenciales en todo el proceso. El diagrama de la Figura 4.8 presenta el proceso de almacenamiento de la VC en Aletheia *Wallet*, la billetera digital del usuario. En esta tarea interactúan dos componentes principales: el "Servicio de Credenciales" y "Aletheia *Wallet*". A continuación, se describen los pasos involucrados:

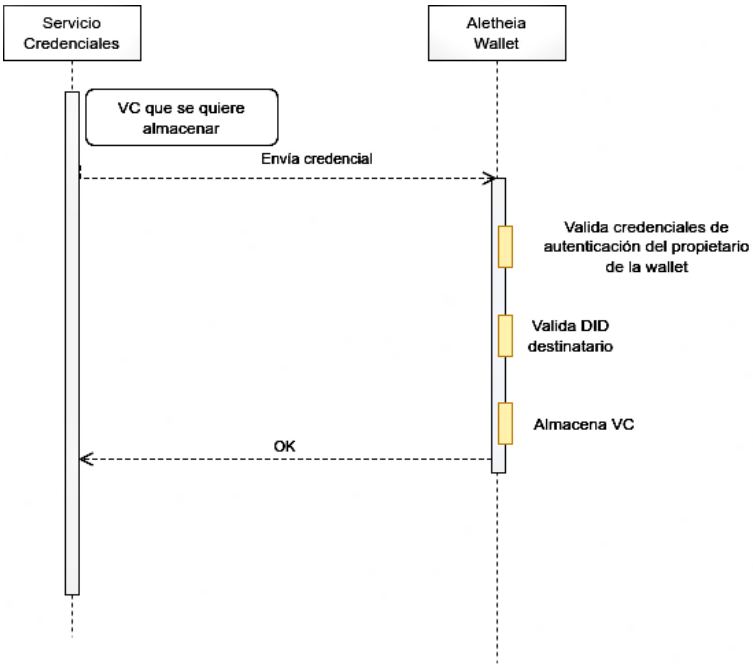


FIGURA 4.8: Almacenamiento de una VC en Aletheia *wallet*.
Fuente: Elaboración propia.

(a) El proceso se inicia en el "Servicio de Credenciales", que dispone de la VC que se requiere almacenar. Esta credencial ya ha sido emitida, y se encuentra en formato *RAW*. La VC es enviada a "Aletheia *Wallet*".

(b) "Aletheia *Wallet*" recibe la VC, y realiza una validación de las credenciales de autenticación del propietario de la billetera. Este paso es crucial para garantizar que solo el legítimo propietario pueda almacenar credenciales en la *wallet*.

(c) Después de verificar la autenticación, la *wallet* valida el *DID* del destinatario. Esto asegura que la credencial se está almacenando en la *wallet* correcta.

(d) Una vez que se han completado las validaciones anteriores, la "Aletheia *Wallet*" procede a almacenar la VC de manera segura. Si el proceso finaliza exitosamente, "Aletheia *Wallet*" envía una confirmación al "Servicio Credenciales", indicando que el proceso se ha completado satisfactoriamente.

En resumen, la credencial verificable emitida por el "Servicio Credenciales", se almacena exitosamente en la "Aletheia *Wallet*" del Titular, asegurando que este pueda acceder y gestionar sus VC. El diagrama 4.8 muestra un proceso seguro y verificado para almacenar VC, asegurando la autenticidad del propietario de la *wallet* y la correcta asignación de la credencial antes de su almacenamiento. Este paso es esencial en la gestión de credenciales verificables en entornos de identidad autogobernada.

3. Generación de Presentación Verificable: El tercer diagrama (ver Figura 4.9) describe el proceso de generación de una presentación verificable. El flujo presentado en el diagrama se centra tanto en la autenticidad de la información presentada como en la protección de la privacidad del titular. En este esquema, el usuario puede seleccionar las VC que desea incluir en la presentación, revelando solo los datos necesarios para cada contexto, conforme a los principios de minimización de datos inherentes a los sistemas de Identidad autogobernada. Esta flexibilidad permite que el usuario mantenga el control sobre la información compartida.

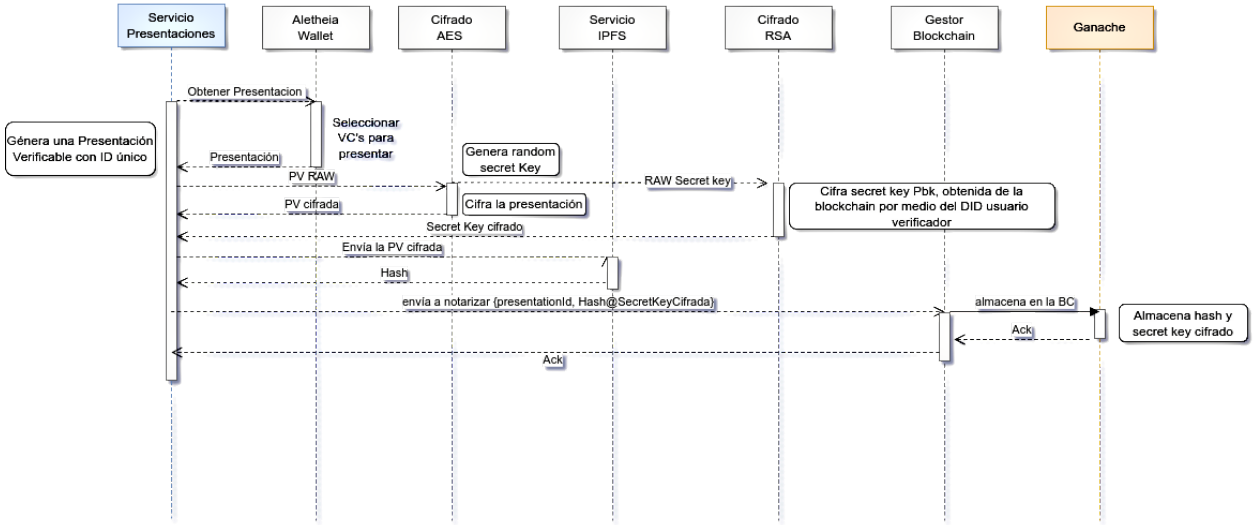


FIGURA 4.9: Generación de una presentación verificable.
Fuente: Elaboración propia.

La Figura 4.9 ilustra la secuencia completa del proceso para generar, cifrar y almacenar una PV, así como su posterior registro en la *blockchain*. A continuación, se presenta una descripción detallada de cada uno de los pasos involucrados:

(a) El proceso inicia en el "Servicio Presentaciones", que genera una PV con un identificador único. Para lo cual se requiere que el Titular se autentique en "Aletheia *Wallet*" y seleccione las VC que desea incluir en la presentación. Este proceso sigue los principios

de minimización de datos, donde solo la información estrictamente necesaria es revelada para cumplir con el propósito de verificación.

(b) "Aletheia *Wallet*" envía la PV en formato *RAW* al componente de "Cifrado AES".

(c) El servicio de "Cifrado AES" genera una clave secreta aleatoria.

(d) El "Cifrado AES" utiliza esta clave para cifrar la presentación y devuelve la PV cifrada al "Servicio Presentaciones". Esto permite que solo el verificador autorizado pueda acceder y validar el contenido de la PV, preservando así la privacidad del titular.

(e) La clave secreta *EAS* en formato *RAW* se envía al componente "Cifrado *RSA*".

(f) El módulo de "Cifrado *RSA*" se encarga de cifrar la clave secreta *EAS* utilizando la clave pública (Pbk) del usuario verificador, que es obtenida de la *blockchain* mediante una consulta asociada a su *DID*. Este proceso asegura que solo el verificador autorizado, a través de su clave privada correspondiente, pueda descifrar y acceder a la clave secreta utilizada para cifrar la presentación.

(g) "Cifrado *RSA*" retorna la clave cifrada al "Servicio Presentaciones"

(h) El "Servicio Presentaciones" envía la PV cifrada al "Servicio *IPFS*". A partir de la PV cifrada, se genera un *hash IPFS*, el cual es devuelto al "Servicio Presentaciones".

(i) La clave secreta cifrada, junto con el *hash* de la PV cifrada, son enviados al "Gestor *Blockchain*", donde se lleva a cabo el proceso de registro de la PV en la *blockchain*. El *hash* es usado como evidencia de la integridad de la PV sin requerir exponer datos sensibles. Este paso es crítico para garantizar la inmutabilidad y trazabilidad de la presentación.

(j) El "Gestor *Blockchain*" se comunica con "*Ganache*" para almacenar estos datos. En la *blockchain* se almacena el *hash* y la clave secreta cifrada, y se envía una confirmación (Ack) al "Gestor *Blockchain*".

(k) El "Gestor *Blockchain*" reenvía esta confirmación al "Servicio Presentaciones".

Este proceso facilita que la PV sea emitida y cifrada de manera segura, almacenada en un sistema de archivos distribuido como *IPFS*, y registrada en una *blockchain*, resguardando tanto su existencia como su acceso, mientras se preservan la privacidad y la integridad de los datos. El diagrama 4.9 ilustra un flujo centrado en la seguridad, privacidad y control de las PV dentro de un sistema descentralizado de identidad autogobernada. En este contexto, el modelo Aletheia se adhiere a principios fundamentales de la SSI, tales como el control descentralizado de los datos, la minimización en la divulgación de información y la preservación de la privacidad mediante el uso de técnicas criptográficas. Nuevamente, la integración de tecnologías como *IPFS* y *blockchain* refuerza la descentralización y la transparencia del proceso, garantizando que el usuario mantenga el control total sobre sus VC y PV. Al igual que en la emisión de una VC, el cifrado de la PV y de la clave secreta AES que la protege, junto con el almacenamiento del *hash* y de las claves cifradas en la *blockchain*, proporcionan niveles elevados de seguridad, inmutabilidad y verificabilidad, sin comprometer la privacidad del titular de las credenciales.

4. Verificación de la Presentación Verificable: El último diagrama de secuencia se presenta en la Figura 4.10, y esquematiza el proceso de verificación de una PV. Este flujo abarca desde la recepción de la presentación por parte del verificador hasta la validación de su autenticidad aplicando las pruebas criptográficas establecidas. El proceso de verificación implica varias fases, cada una de las cuales garantiza la seguridad y la autenticidad de la información presentada. Primero, se recuperan la PV cifrada y la clave secreta AES desde *IPFS* y la *blockchain*, respectivamente. Posteriormente, la clave secreta es descifrada utilizando un sistema de cifrado asimétrico (*RSA*), lo cual asegura que solo el verificador autorizado pueda acceder a la información de la presentación. Luego, la PV descifrada es validada con la librería *DidKit*

para confirmar la autenticidad de las credenciales. De esto modo, la PV se recupera de manera segura, se descifre correctamente, y se valida, manteniendo la integridad y la confidencialidad de los datos en todo momento.

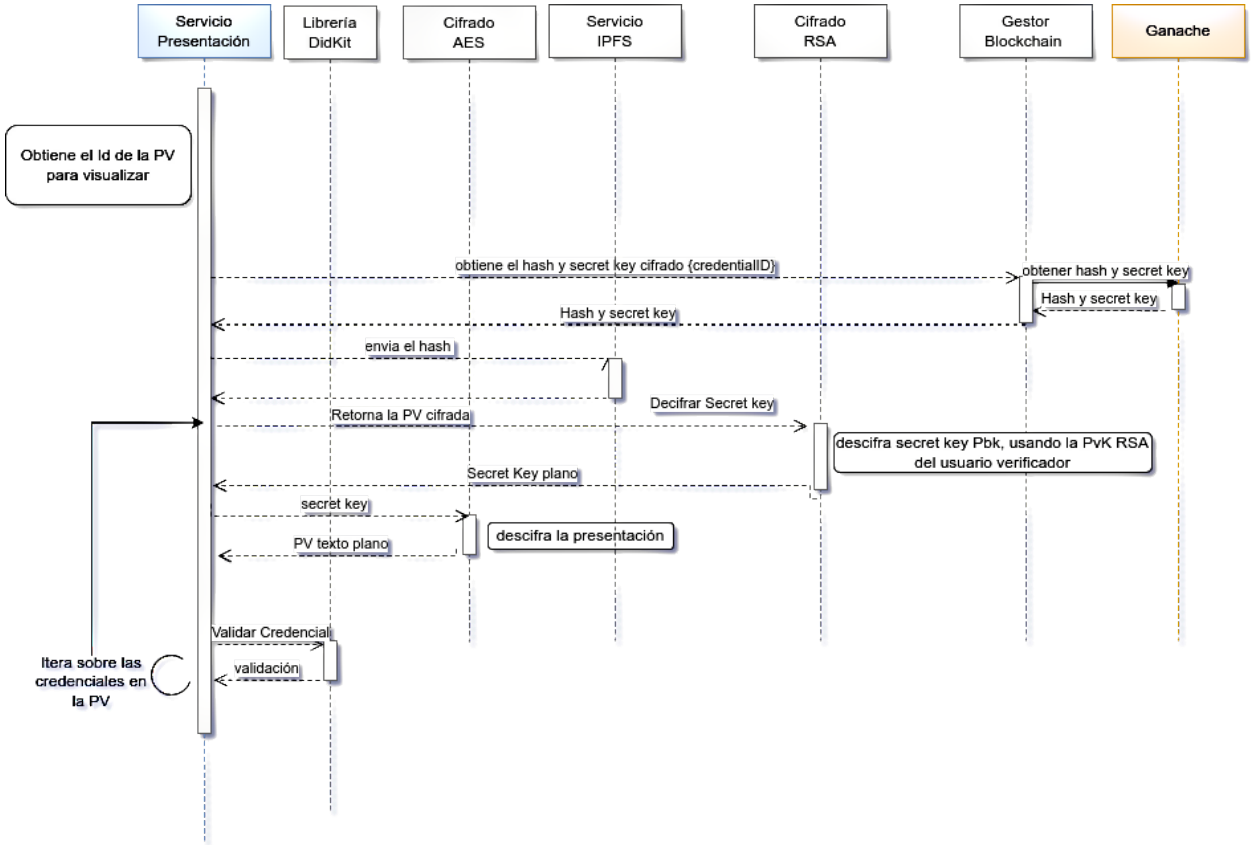


FIGURA 4.10: Verificación de una presentación verificable.
Fuente: Elaboración propia.

A continuación, se describe cada uno de los pasos requeridos:

(a) El proceso comienza en el "Servicio Presentación", cuando un usuario verificador obtiene el ID de la PV que se desea visualizar. Este ID es requerido para acceder a la PV almacenada y proceder con su verificación.

(b) El "Servicio Presentación" se comunica con el "Gestor *Blockchain*", el cual interactúa con "*Ganache*" para obtener dos elementos: el *hash* de la PV almacenada y la clave secreta AES cifrada. Estos elementos se obtienen transacción que notarizó la presentación.

(c) El "Gestor *Blockchain*" devuelve el *hash* y la clave secreta AES cifrada al "Servicio Presentación". Estos dos valores permiten asegurar la autenticidad e integridad de la PV durante la verificación.

(d) El "Servicio Presentación" envía el *hash* obtenido al "Servicio *IPFS*".

(e) El "Servicio *IPFS*", utilizando el *hash* recibido, recupera la PV cifrada y la devuelve al "Servicio Presentación".

(f) Paralelamente, el "Servicio Presentación" envía la clave secreta AES cifrada al componente de "Cifrado *RSA*".

(g) El "Cifrado *RSA*" se encarga de descifrar la clave AES secreta utilizando la clave privada *RSA* del usuario verificador. Esta operación se asegura que solo el verificador pueda descifrar la clave secreta utilizada para proteger la presentación.

(h) La clave secreta *AES* en formato *RAW* se devuelve al "Servicio Presentación".

(i) El "Servicio Presentación" recibe la clave secreta AES descifrada en texto plano y la envía al módulo "Cifrado AES".

(j) El "Cifrado AES" utiliza esta clave secreta AES para descifrar la PV. La PV descifrada se devuelve al "Servicio Presentación".

(k) Con la PV descifrada, el "Servicio Presentación" interactúa con la "Librería DidKit". Esta funcionalidad se utiliza para validar la autenticidad y la integridad de las credenciales verificables contenidas en la presentación.

(l) La "Librería DidKit" realiza el proceso de validación y devuelve el resultado al "Servicio Presentación".

(m) Finalmente, el "Servicio Presentación" itera sobre las VC contenidas en la PV, para realizar las verificaciones requeridas.

Este paso de verificación de la PV completa el triángulo de la confianza, cerrando el ciclo de comunicación entre Poseedor, Emisor y Verificador, un flujo de información fundamental en una aplicación de identidad digital autogobernada.

El Capítulo 5 lleva a cabo una validación tanto académica (ver sección 5.2) como dinámica (ver sección 5.3) del modelo Aletheia, lo cual permite corroborar la validez de este flujo de información y, en consecuencia, verificar la hipótesis propuesta en esta investigación.

Capítulo 5

Validación del modelo Aletheia

El presente capítulo aborda la validación del modelo Aletheia descrito en la sección 4.3. Se estructura de la siguiente manera: primero se define el marco de gobernanza aplicado en la construcción del caso de prueba, luego se realiza una validación académica tomando como referencia el marco de evaluación establecido en [2], y por último, se realiza una validación estática sobre la implementación realizada, compuesta por Aletheia-Dapp y Aletheia *Wallet*. Esta validación técnica permitió comprobar la funcionalidad y seguridad del sistema en un entorno simulado, analizando el flujo de información en la creación, emisión y verificación de credenciales y presentaciones verificables a través de una infraestructura de llaves criptográficas, almacenamiento descentralizado e interacción entre diferentes entidades como emisores, titulares y verificadores, probando como el modelo respalda la privacidad, integridad y verificabilidad de las credenciales.

5.1 Marco de gobernanza

A continuación se presenta el marco de gobernanza propuesto para Aletheia-Dapp, el cual sirve de referente para la implementación de este caso de prueba.

5.1.1 Capa 1: Utilidad pública

Esta capa se encarga de la infraestructura requerida para preservar la privacidad en la comunicación de las entidades de Aletheia. El modelo utiliza los siguientes estándares técnicos para la conectividad e interacción entre su entidades:

- *JSON Web Key* (JWK). Es una estructura de datos basada en JSON que permite representar claves criptográficas, facilitando la compatibilidad con multiples protocolos de seguridad [282].
- *Universally Unique Identifier,* versión 4 - *UUIDv4*: Este identificador aleatorio debe ser usado para generar identificaciones únicas a recursos, por ejemplo, enlaces web. *UUIDv4* es aleatorio pero no garantiza su unicidad pero presenta una probabilidad muy baja de colisiones (4×10^{-18}), por cada millón de identificadores generados) [224].
- Creación de identificadores descentralizados [221].
  - DID en Aletheia Wallet: La billetera digital utiliza la función *generateEd25519Key()* disponible en la librería *DIDKit* [279]. *DIDKit* provee las primitivas necesarias para la implementación de sistemas con identidades descentralizadas y credenciales verificables. Ed25519 en un algoritmo de firma digital de clave pública eficiente y seguro [283], características que han influido en su aplicación en los ecosistemas basados en *blockchain*,

como *Solana*, *Ethereum* o *Stellar*. No es considerado un algoritmo post-cuántico por lo cual los sistemas que lo utilicen deberán ser actualizados cuando la computación cuántica logre el grado de madurez que implique un riesgo de seguridad [284]. Por último, el DID se genera mediante el método *keyToDID*, utilizando la llave ED25519 transformada a formato JWK.
  - DID en Aletheia-Dapp: El caso de estudio permite la creación de un DID adicional para cada entidad. La generación de este DID se realiza de la misma manera que en la Wallet, para lo cual invoca la función *generateEd25519Key()* y crea un archivo JWK para las llaves.
- *Credential Handler API -CHAPI-*: Es una interfaz de programación diseñada para el manejo de credenciales verificables. *CHAPI* permite la emisión, almacenamiento y verificación de VC, de manera segura y eficiente, mejorando la interoperabilidad entre sistemas de identidad digital [270].
- El *Framework* de seguridad de *Spring* proporciona autenticación y autorización para aplicaciones en *JAVA* [285]:
  - Las contraseñas son almacenadas aplicando el algoritmo de cifrado *bcrypt* (función de *hashing* de contraseñas) implementado en el método *BCryptPasswordEncoder*.
- Cifrado de información sensible: El modelo utiliza un sistema de almacenamiento descentralizado [286] que preserva la privacidad y control de la información mediante un algoritmo de cifrado. Se aplicó la implementación *RSA* (Rivest, Shamir y Adleman) disponible en la *API* de seguridad de *Java* [287] con una longitud de la clave de 2048 bits, que permite un cifrado y descifrado seguro de datos. La selección de *RSA* se fundamenta en la seguridad del algoritmo y la versatilidad en el cifrado de datos usando la llave pública o para la firma digital de documentos por medio de la llave privada. *RSA* no demanda un intercambio previo de llaves por lo cual es aplicado en entornos de una infraestructura de llave pública para la emisión y validación de certificados [283].
- Tecnología de registro distribuido: Aletheia, por su diseño agnóstico a *blockchains*, es capaz de operar sobre diversas plataformas de DLT. En esta prueba se utilizó una instancia privada de *ethereum*, provisionada con *Ganache*, para simular un entorno de DLT. *Truffle* se utilizó como herramienta para compilar y desplegar los contratos inteligentes sobre esta *blockchain* [272]. Por último, el despliegue de Aletheia en un caso de uso industrial requiere seleccionar la *blockchain* conforme a las necesidad del caso, definir las reglas para adición de nodos validadores, el algoritmo de consenso junto con la recompensa a los mineros y las políticas para monitoreo y arbitraje del registro.

5.1.2 Capa 2: Infraestructura técnica de confianza

En esta capa, se deben definir los mecanismos y condiciones para la construcción de identidades verificables, junto con la comunicación necesaria a través de los identificadores descentralizados establecidos en la capa inferior. La interacción de cada entidad en Aletheia estará mediada por su billetera digital a través de *CHAPI* para gestionar las credenciales verificables de manera eficiente.

La Figura 5.1 muestra la interacción de una entidad en la Aletheia Wallet, destacando las dos acciones principales: creación de una billetera e inicio de sesión. Un nuevo usuario debe proporcionar credenciales de acceso (nombre de usuario y contraseña), que serán almacenadas localmente. La billetera generará un UUIDv4, el cual podrá utilizarse para crear referencias únicas a objetos, como enlaces, junto con el DID de la entidad correspondiente. El segmento izquierdo de la Figura 5.1 ilustra el proceso de habilitación de la Wallet y muestra un ejemplo en formato *JWK* de las llaves asociadas al DID. Este esquema sigue una estructura de pares clave-valor, donde la clave “kty” indica

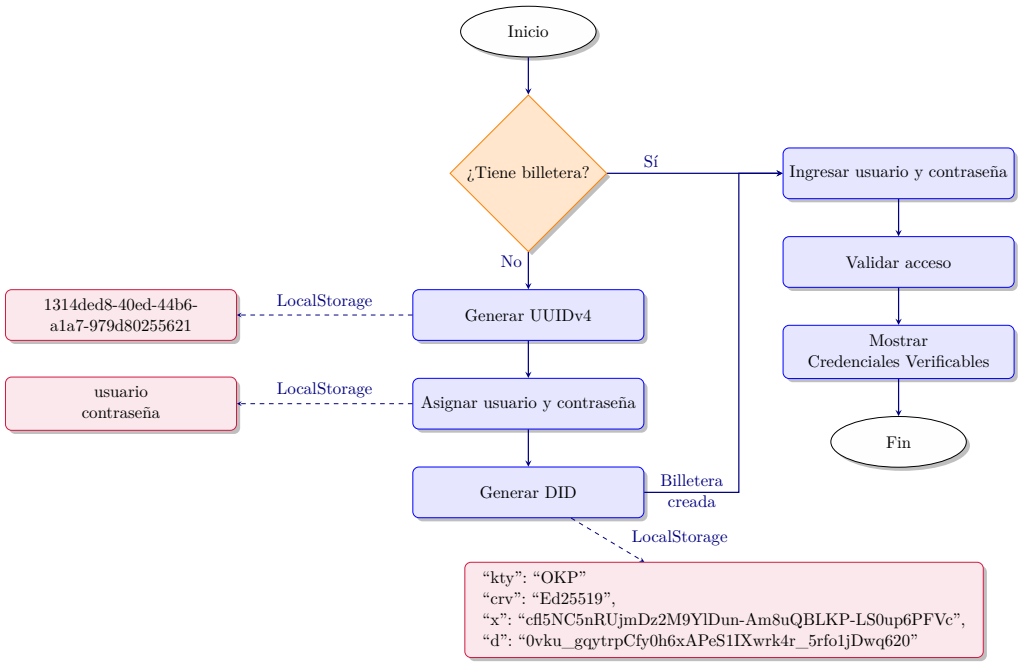


FIGURA 5.1: Flujo de información para la creación de un usuario e inicio de sesión en Aletheia Wallet. Fuente: Elaboración propia.

el tipo de clave y tiene el valor "OKP" (*Operation Key Pair*). La entrada "crv" especifica la curva utilizada, con el valor Ed25519, que corresponde a una curva elíptica. Los dos últimos elementos, "x" y "d", contienen, respectivamente, la coordenada x del punto público en la curva elíptica y la clave privada asociada a dicho punto. Ambos valores están codificados en formato base64url. Cada entidad es responsable de la gestión de sus propias claves.

Una vez el usuario dispone de una billetera, puede comunicarse con Aletheia-Dapp y crear o iniciar sesión, según el flujo presentado en la Figura 5.2. La definición de este caso de uso no incluye medidas para mitigar ataques Sybil ni contempla un modelo de reputación (ver sección 5.4); por lo tanto, Aletheia-Dapp requiere una gestión de usuarios respaldada por una base de datos relacional. En este esquema se debe implementar un mecanismo de auditoría sobre los emisores para mantener su acreditación. La creación de un usuario en Aletheia-Dapp requiere el suministro de credenciales de acceso, el DID de la billetera y se producirán dos llaves, una *RSA* para el cifrado y descifrado de información sensible y la otra para el DID de la aplicación. El *hash* de la credencial de acceso se registra en la *blockchain* mediante un contrato inteligente.

5.1.3 Capa 3: Diamante de la confianza

El diamante de la confianza está formado por la interacción entre Emisor - Titular - Verificador, conocida como el triángulo de la confianza, junto con las normas que la gobiernan. Estas reglas le otorgan estructura y fundamento al diamante.

Las condiciones para el flujo de información establecido por credenciales verificables son:

- Se cuenta con un conjunto de esquemas predefinidos para las credenciales verificables. Para este caso de uso se utilizó el esquema definido por la *W3C* en su versión 1.0 [288], que proporciona una estructura estándar para la emisión y verificación de credenciales. Este esquema provee ejemplos prácticos [289] para la emisión y verificación de credenciales.
- Cada entidad, poseedor, emisor o verificador, deberá estar registrada tanto en Aletheia Wallet

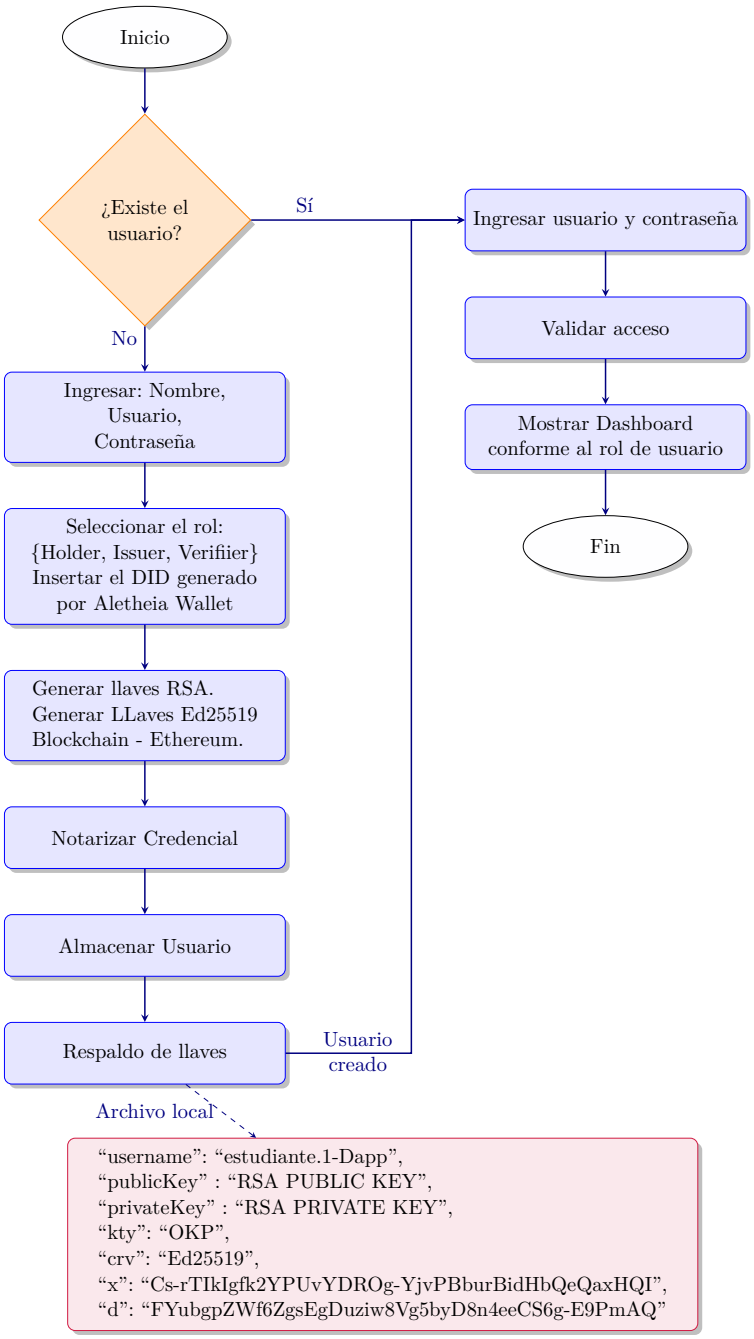


FIGURA 5.2: Flujo de información para la creación e inicio de sesión en Aletheia-Dapp.
Fuente: Elaboración propia.

como en Aletheia-Dapp.

- Cuando un Poseedor (*Holder*) inicia sesión en Aletheia-Dapp, tiene acceso a un panel de control que le permite acceder a las siguientes acciones:
  - Solicitud de credenciales verificables:
    - Realizar solicitud: Es necesario seleccionar el Emisor al cual se desea dirigir la solicitud, especificando el tipo de credencial requerida.
    - Consultar solicitud: Se muestra el total de credenciales solicitadas, junto con su estado actual. El Titular puede visualizar la credencial que le ha sido emitida y decidir si desea conservarla en su billetera digital. Para almacenar la credencial, se

requiere un llamado a Aletheia Wallet, seguido de un proceso de autenticación y una confirmación de aceptación por parte del Titular.

  - Presentación de credenciales verificables:
    * Realizar una presentación verificable: Se debe determinar el verificador al cual se desea enviar la solicitud, junto con una etiqueta que refleje la intención de la presentación. Además, se debe conectar la billetera digital para seleccionar el conjunto de credenciales verificables que se desea incluir.
    * Consultar las presentaciones realizadas: Se muestra un listado de las peticiones enviadas, junto con su estado actual y el token asignado a cada VC, una vez ha sido emitida.

- Cuando un emisor inicia sesión en Aletheia-Dapp tendrá de un *dashboard* con las siguientes acciones:
  - Generación de credenciales verificables: El emisor tiene acceso a un listado de todas las credenciales que le han sido solicitadas. Este analiza cada solicitud y puede optar por emitir, rechazar o descartar la credencial requerida. Una vez que la VC es generada, el estado de la solicitud se actualiza para que el Titular correspondiente pueda consultarlo.
- Cuando un verificador inicia sesión en Aletheia-Dapp, dispondrá de un *dashboard* con las siguientes acciones:
  - Consulta de credenciales verificables presentadas: El verificador tiene acceso a un listado de todas las credenciales que le han sido presentadas. Luego, ejecuta un proceso de verificación criptográfica y registra el resultado de dicha comprobación.

5.1.4 Capa 4: Nivel de aplicación

La última capa se concibe como la responsable de la confianza humana, abarcando las reglas de contexto social y jurídico que buscan asegurar la transparencia y seguridad en las relaciones entre las entidades del modelo.

Este caso de prueba tiene como objetivo principal evaluar la funcionalidad del modelo Aletheia, probando que el sistema SSI esta diseñado para la generación y validación automática de credenciales verificables. El diseño del caso se centra en probar el flujo de información en un escenario controlado, permitiendo una evaluación precisa de las capacidades del sistema.

El caso de uso contempla las siguientes acciones:

1. Solicitud de Credenciales: El Titular de los derechos de identidad, como un estudiante, inicia el proceso solicitando credenciales a un Emisor previamente registrado y autorizado, como la secretaría académica de una institución educativa.

2. Emisión de Credenciales: El Emisor analiza la solicitud recibida y, si la aprueba, genera la credencial verificable correspondiente y la envía al solicitante mediante una comunicación segura.

3. Recepción y Almacenamiento: Al recibir las credenciales, el estudiante verifica su estado y, posteriormente, puede optar por almacenarlas de forma segura en Aletheia Wallet, la billetera digital diseñada específicamente para este propósito.

4. Presentación de Credenciales: Cuando surge la necesidad, el Titular puede presentar una o varias de sus credenciales almacenadas en su billetera digital a un verificador. Por ejemplo, podría presentarlas a la unidad de investigaciones de su institución para solicitar la aprobación de un trámite, como una movilidad académica.

5. Verificación y Aprobación: El verificador, utilizando las herramientas proporcionadas por Aletheia, comprueba criptográficamente la autenticidad e integridad de las presentaciones recibidas. Con base en esta verificación, emite las aprobaciones correspondientes para el trámite solicitado.

Este flujo de trabajo demuestra la capacidad de Aletheia para facilitar un ecosistema de identidad digital seguro y eficiente, donde las credenciales pueden ser emitidas, almacenadas, presentadas y verificadas de manera confiable y automatizada. Este caso de prueba permite evaluar la seguridad y la privacidad del sistema en cada etapa del proceso, desde la emisión inicial hasta la verificación final de las credenciales.

5.2 Adherencia a los principios de identidad digital autogobernada

La sección 2.2.1.2 describe los principios de identidad digital autogobernada propuestos por Allen [223], los cuales han sido seleccionados como las variables necesarias para evaluar el comportamiento de Aletheia. En la sección 3.10 se presentó la escala utilizada para medir el nivel de cumplimiento de estos principios en los diferentes *frameworks* de SSI identificados en esta investigación 3. La escala de medición junto, con los resultados obtenidos, han sido publicados en [2]. Este artículo ha permitido establecer una base de comparación y análisis para sistemas de identidad autogobernada.

La Tabla 5.1 muestra y analiza el nivel de cumplimiento de los principios en el modelo Aletheia, de acuerdo con la escala previamente definida.

Principio	**Puntaje**	**Descripción**
Existencia	1.0	Un usuario puede habilitarse en Aletheia Wallet sin ninguna restricción y generar su propio DID para comunicarse con un proveedor de servicios, como Aletheia-Dapp en este caso de uso.
Control	1.0	Como titular de los derechos de identidad, el usuario tiene control sobre sus claves criptográficas y total autonomía para gestionar sus credenciales verificables.
Consentimiento	1.0	Gracias al diseño centrado en la privacidad, que incluye la implementación de la billetera *CHAPI* y el almacenamiento cifrado de información sensible, el titular tiene la capacidad de otorgar su consentimiento sobre el uso de atributos de su identidad digital.
Minimización	1.0	La billetera digital contiene un conjunto de afirmaciones sobre una entidad. Dado que el usuario tiene control total sobre su billetera, puede seleccionar un subconjunto específico de esta información para presentarlo a un Verificador, lo que permite divulgar únicamente la información requerida en cada proceso.
Persistencia	1.0	La información sensible se almacena fuera de la cadena de bloques y en un dispositivo externo a la billetera digital. Esta característica permite preservar la privacidad del usuario, ya que los datos se registran y cifran en un sistema de almacenamiento descentralizado, como *IPFS*.

Continúa en la siguiente página...

Continuación de la tabla...

Principio	Puntaje	Descripción
Protección	1.0	El modelo permite la integración con múltiples DLT, ya sea en entornos públicos, privados o federados. En todos los casos, la información del usuario permanece bajo su control, gracias al esquema utilizado en Aletheia Wallet y a los procedimientos de cifrado y descifrado implementados para acceder a los datos almacenados.
Acceso	1.0	el Titular siempre podrá acceder a su billetera digital y, por lo tanto, a sus atributos de identidad, independientemente del proveedor de servicios.
Transparencia	1.0	El modelo aplica estándares abiertos como DID [221], VC [222] y *CHAPI* [270]. Además, en el caso de prueba se utilizó software de código abierto, como Didkit [279].
Portabilidad	0.75	Aletheia implementa los estándares mencionados anteriormente, lo cual posibilita una portabilidad derivada de esta estandarización. Sin embargo, la mayor ventaja se encuentra en su Wallet, que permite la adaptación y el uso de los atributos de identidad digital en diferentes plataformas. Es importante señalar que cada caso puede requerir un esfuerzo de programación para su integración.
Interoperabilidad	1.0	Permite una interacción con plataformas que implementen el estándar DID, como se ilustra en la Tabla 3.10. Además, Aletheia Wallet amplía esta interoperabilidad mediante la implementación de la interfaz *CHAPI*.

Tabla 5.1: Nivel de Adherencia del Modelo Aletheia a los Principios de Identidad autogobernada. Fuente: Elaboración del autor.

La Figura 3.2 incluida en la página 57, exhibe el nivel de cumplimiento de los principios SSI en los nueve *frameworks* analizados. La Figura 5.3 añade el modelo Aletheia, lo cual facilita la comparación de su nivel de adherencia con respecto a estos *frameworks*. El modelo propuesto se alinea con los principios de SSI y ofrece ventajas en cuanto a persistencia, gracias a su almacenamiento descentralizado y cifrado, comparable al de ION pero sin depender de una *blockchain* pública como *bitcoin*. Además, las credenciales verificables están protegidas, ya que se almacenan en la Wallet y son controladas directamente por el Titular. La billetera digital implementa *CHAPI*, lo que fomenta la portabilidad y la interoperabilidad, características clave de esta propuesta. Para concluir, La mayoría de los *frameworks*, como *Aletheia*, *ION*, *Kilt*, *Uport* y *Jolocom*, alcanzan una puntuación alta y relativamente uniforme en la mayoría de los principios de SSI. Esto sugiere que estos modelos están bien alineados con los estándares de identidad autogobernada. Por su parte, Aletheia, sobresale por su adaptabilidad y enfoque en la persistencia, interoperabilidad y portabilidad. Esto hace que Aletheia sea adecuado para implementaciones en sistemas SSI que requieren altos niveles de control y acceso, junto con la capacidad de operar en un entorno diverso de plataformas.

5.3 Análisis del escenario de validación

El propósito de esta sección es analizar y validar el flujo de información propuesto en Aletheia, el cual se basa en un modelo respaldado por DLT para la gestión de una identidad digital autogobernada. Este enfoque está diseñado para preservar la privacidad y la integridad de los atributos

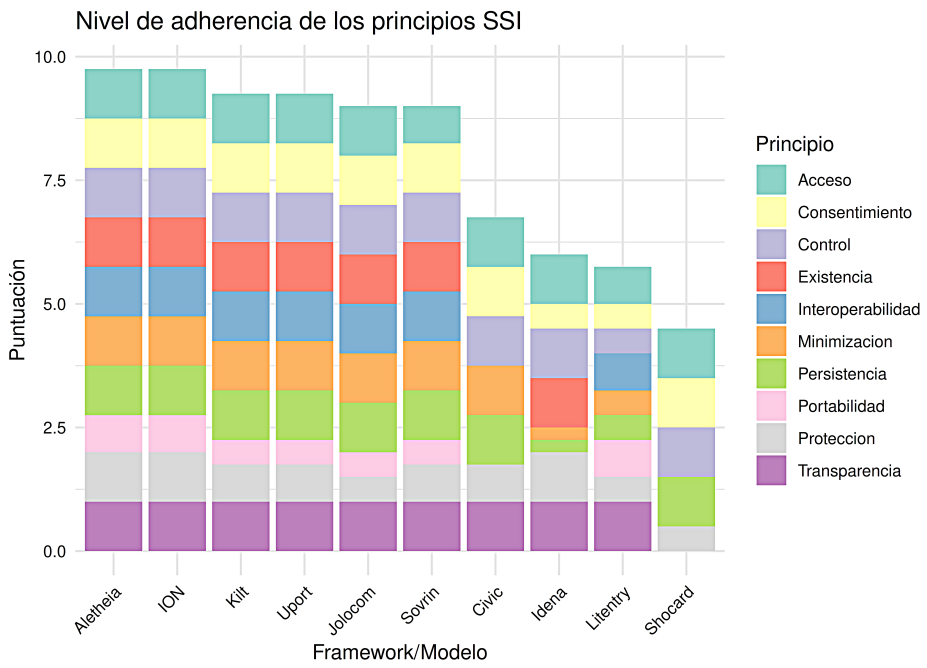


FIGURA 5.3: Cumplimiento de los principios SSI en el modelo Aletheia.
Fuente: Elaboración del autor

de identificación personal, así como para permitir su intercambio seguro entre las entidades (ver sección 4.2.1): Titular, Emisor y Verificador. La implementación de una identidad autogobernada en un entorno que combina DLT y servicios de almacenamiento descentralizado permite a los usuarios gestionar sus identidades de manera autónoma, reduciendo o eliminando la dependencia de terceros de confianza y mitigando riesgos de vulnerabilidad, como la manipulación de datos.

Para validar la hipótesis (ver sección 1.2.2), se ha implementado el caso de uso Aletheia-Dapp (ver sección 4.2.3), el cual integra una billetera digital para la gestión de credenciales verificables (ver sección 4.2.2). Este modelo se basa en los principios de SSI (ver sección 2.2.1.2), utilizando DID (ver sección 2.2.1.4), VC (ver sección 2.2.1.6), y almacenamiento tanto dentro (*on-chain*) como fuera (*off-chain*) de la cadena de bloques (ver sección 2.2.1.7). Este escenario simula la interacción necesaria entre las diferentes entidades para un intercambio seguro, permitiendo así evaluar la capacidad de Aletheia para garantizar la privacidad, integridad de los datos y seguridad en el intercambio de información.

5.3.1 Aspectos generales de la implementación

La implementación de Aletheia-Dapp es una aplicación descentralizada diseñada para gestionar identidades digitales autogobernada, su función principal es proporcionar una plataforma segura y eficiente para la creación, almacenamiento, verificación y presentación de credenciales verificables, utilizando tecnologías de identidad descentralizada, estándares de credenciales verificables, *Svelte* para *frontend* de la billetera digital y *Spring Boot* para el *backend*.

Funcionalidad principal:

1. Gestión de identidades descentralizadas: Aletheia-Dapp permite a los usuarios crear y gestionar su identificador descentralizado. Este DID es autogobernado, lo que significa que los usuarios tienen control total sobre su identidad sin depender de una autoridad central.

2. Gestión de credenciales verificables: se permite a los usuarios emitir, almacenar y gestionar credenciales verificables. Estas credenciales pueden ser utilizadas para demostrar atributos específicos de una identidad, como el título académico. Aletheia-Dapp utiliza *DIDKit* para manejar DID y VC, con sus funciones para verificar presentaciones y credenciales, así como para interactuar con servicios de identidad descentralizada.
   - Emisión de credenciales: Los emisores pueden crear y emitir VC a los usuarios.
   - Almacenamiento Seguro: Las VC se almacenan de manera segura en la billetera del usuario.
   - Verificación de Credenciales: Los verificadores pueden comprobar la autenticidad y validez de las credenciales presentadas por los poseedores.
3. Presentación de credenciales: Un poseedor esta habilitado para presentar sus VC a terceros de manera segura y privada.
   - Presentación selectiva: Los usuarios pueden elegir las VC que desean compartir desde su billetera digital.
4. Interacción con servicios externos: Aletheia-Dapp puede interactuar con servicios externos y otros sistemas descentralizados para soportar su funcionalidad.
   - Integración con DLT: La aplicación puede interactuar con la blockchain de *ethereum* para registrar y verificar transacciones relacionadas con identidades y credenciales.
   - Servicios de mediación: Utiliza este servicio para facilitar la comunicación entre la billetera digital y la aplicación eb diferentes partes en el ecosistema de identidad descentralizada.

El código fuente y la documentación técnica de Aletheia-Dapp y Aletheia *Wallet* se encuentra disponibles en los repositorios: `https://github.com/devapp2/AletheiaDappV1.git` y `https://github.com/devapp2/AletheiaWalletV1.git`, respectivamente.

5.3.2 Contexto del escenario de validación

El caso de prueba y validación ha sido desplegado en una máquina virtual alojada en el *CECAD* [290], con la siguiente configuración: 16 procesadores, 32 GB de memoria *RAM*, 100 GB de almacenamiento y *Ubuntu 22.04.03 LTS* como sistema operativo. Los requisitos de software necesarios para el funcionamiento de Aletheia se detallan en la Tabla 4.6 de la sección 4.2.5 y han sido instalados en este entorno.

La Tabla 5.2 detalla la configuración adoptada para la red *blockchain* de *Ethereum*. En esta tabla se incluyen las direcciones específicas asignadas al *smart contract*, utilizado tanto para la creación de usuarios como para la gestión de VC, así como la dirección de la cuenta de usuario encargada de cubrir las comisiones de las transacciones en la red. Las pruebas se llevaron a cabo en este entorno controlado, utilizando tres navegadores web en sus versiones más recientes al momento del experimento: *Firefox* versión 130.0, *Chromium* versión 128.0.6613.113 y *Opera One* versión 114.0.5282.21. Este enfoque de múltiples versiones garantiza la compatibilidad del sistema y valida su correcto funcionamiento en diversas plataformas y versiones de navegadores. Cabe destacar que, para cada prueba, se monitorearon las transacciones en la *blockchain*, verificando tanto el comportamiento del *smart contract* como la correcta gestión de las VC.

Este escenario de validación implica la interacción de tres entidades principales: el Poseedor, el Emisor y el Verificador, cada una con roles claramente definidos. En primer lugar, el Poseedor, identificado como “estudiante.1”, actúa como un alumno dentro de una institución universitaria y

Información de la *Blockchain*	
Tipo	*Ethereum* privada, modo simulación
Puerto	7545
Identificador de la red	5777
Hardfork	Merge
Workspace	Aletheia
Precio por unidad de gas	800.000 gwei (0.008) (1 ETH = 10^9 gwei)
Limite de gas	200 unidades (0.16 ETH)
Algoritmo de minado	Proof of Stake (proceso de Auto minado simulado)
Dirección de la cuenta	0x4AfF5efC82C625b1D6Ed2f653C9560D79b10D7A6
Dirección del *smart contract*	0xbB127E3CeF2b0b561EaabB64044cEEDd96047034

Tabla 5.2: Configuración de la *blockchain* tipo *ethereum* simulada con *Ganache*.
Fuente: Elaboración propia.

es responsable de gestionar sus credenciales verificables. En segundo lugar, el Emisor, representado por "secretario.1", corresponde a la secretaría académica, encargada de generar y emitir certificaciones oficiales a solicitud del estudiante. Finalmente, el Verificador, como la unidad de investigaciones ("unidadInvestigacion.1-Dapp") de una facultad, desempeña un papel crucial al conceder incentivos económicos a los estudiantes, pero solo después de validar automáticamente una Presentación Verificable (PV) proporcionada por el Poseedor.

Entidad	**Nombre**	**DID y UUIDv4**
Poseedor	estudiante.1	did:key:z6Mkn8AkWKht7hqfvo47JH3nYjV4CUjBYMmDAT7NrDuzSyux UUIDv4:6d5e71ab-3eca-44aa-bbf3-99e37a0d91c7
Emisor	secretario.1	did:key:z6MkwBM4imMSUNs7awm1mbrWcJuPmPYwRFpaq44sL1HyHVYW UUIDv4:81022134-d076-48b5-8970-7d027298eda9
Verificador	unidadInvestigacion.1-Dapp	did:key:z6MkwNa2U9pmjVJXekV4Thbo71VYxuRPHCqqP48QLXi8QHxU UUIDv4:b3ad3064-1eef-4a53-9b13-b3f716b8ec42

Tabla 5.3: Entidades creadas en Aletheia *Wallet*.
Fuente: Elaboración propia.

La Tabla 5.3 detalla la información relacionada con la creación de estas tres entidades, de acuerdo con el procedimiento descrito en la Figura 5.1. Durante este proceso, se generó una billetera digital para cada entidad, estando inicialmente vacía pero habilitada para almacenar las credenciales verificables correspondientes al usuario (Ver Figura 5.4). Es importante aclarar que la creación de estas billeteras digitales es un paso fundamental para garantizar el almacenamiento seguro y la gestión eficiente de las credenciales verificables. Además, esta estructura permite que las interacciones entre las tres entidades se realicen sin la necesidad de intermediarios de confianza, promoviendo un ecosistema descentralizado.

Una vez que el usuario ha creado su billetera digital, comienza el proceso de habilitación de su cuenta en Aletheia-Dapp, siguiendo el procedimiento descrito en la Figura 5.2. Cada usuario dispone de dos pares de llaves: un par de tipo *RSA*, destinado al cifrado de archivos y a la firma digital de credenciales, y un par de tipo Ed25519, utilizado específicamente para las interacciones dentro de la red *Ethereum*. Esta dualidad en el uso de llaves aporta una ventaja significativa en la gestión de datos y en la seguridad de las transacciones. Aletheia-Dapp proporciona un servicio de gestión en *blockchain*, que incluye la invocación de un contrato inteligente responsable de registrar la creación del usuario en la red. Este registro no solo establece la identidad del usuario, sino que también genera una credencial verificable que incluye el identificador descentralizado. El DID se deriva de las llaves Ed25519, mientras que las llaves *RSA* se emplearán para cifrar la información sensible.

El resultado de la ejecución del método que almacena la credencial verificable, tal como se define en

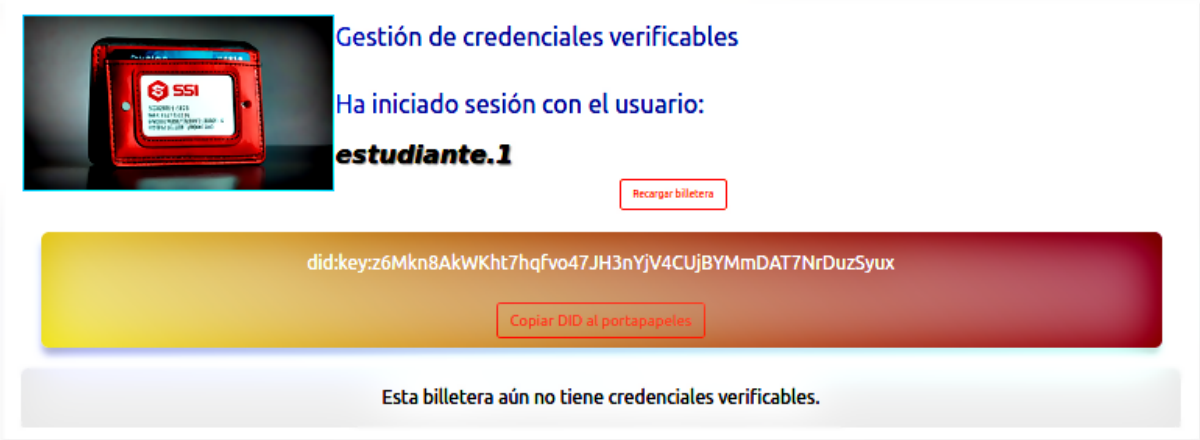


FIGURA 5.4: Inicialización Aletheia *Wallet* para el poseedor estudiante.1.
Fuente: Elaboración propia.

el contrato inteligente, se presenta en la Figura 5.5. Además, en la Figura 5.5a se pueden observar los detalles de la transacción relacionada con la creación del usuario "estudiante.1-Dapp", mientras que la Figura 5.5b agrupa todas las transacciones correspondientes a los tres usuarios involucrados en el sistema: estudiante, secretario académico y unidad de investigaciones. El gas consumido durante la creación de un usuario asciende a 464 369 gwei, equivalente a 0,000 464 369 ETH. Este valor refleja no solo el costo de ejecutar la transacción en la red *Ethereum*, sino que también sirve como indicador del consumo de recursos y la eficiencia del proceso de creación de usuarios en Aletheia-Dapp. Optimizar este costo es un aspecto fundamental para mejorar la sostenibilidad económica de la plataforma a largo plazo, aunque requiere un análisis adicional en un entorno de producción o de ejecución no simulado.

Una vez finalizado el proceso de creación de los usuarios, la entidad Poseedor tendrá la capacidad de llevar a cabo las siguientes acciones: solicitar la emisión de una VC, realizar una Presentación Verificable (PV) y consultar el estado tanto de la emisión de VC como de la validación de PV. En las secciones siguientes, se detallará el proceso correspondiente a cada una de estas acciones.

5.3.2.1 Generación de una credencial verificable

El proceso de emisión de una credencial verificable se ilustra en la Figura 4.6. Esta tarea consta de varias etapas, comenzando con la solicitud de emisión por parte de un usuario.

En la Figura 5.6a se muestra como un futuro Poseedor, identificado como "estudiante.1-Dapp", realiza la solicitud. En esta etapa, el solicitante lleva a cabo dos acciones: (a) selecciona un Emisor autorizado, en este ejemplo, "secretario.1-Dapp"; y (b) especifica el tipo de credencial verificable que desea obtener, en este caso, una constancia de pertenencia a un proyecto curricular. Es importante destacar que el sistema está diseñado para ofrecer flexibilidad y transparencia a lo largo del proceso. La Figura 5.6b ilustra como el usuario puede consultar el estado de sus VC, lo que permite un seguimiento continuo del progreso en la emisión. La posibilidad de monitorear el estado de las credenciales no solo mejora la experiencia del usuario, sino que también incrementa la confiabilidad y transparencia del sistema de gestión de VC, ya que los usuarios pueden verificar si su solicitud está en proceso, si se ha emitido la credencial o si se requiere alguna acción adicional de su parte. Este enfoque en la emisión de credenciales verificables habilita un proceso confiable, característica fundamental en el contexto de la identidad digital autogobernada.

(A) Transacción en la *blockchain* asociada al registro del estudiante.1 en Aletheia-Dapp.

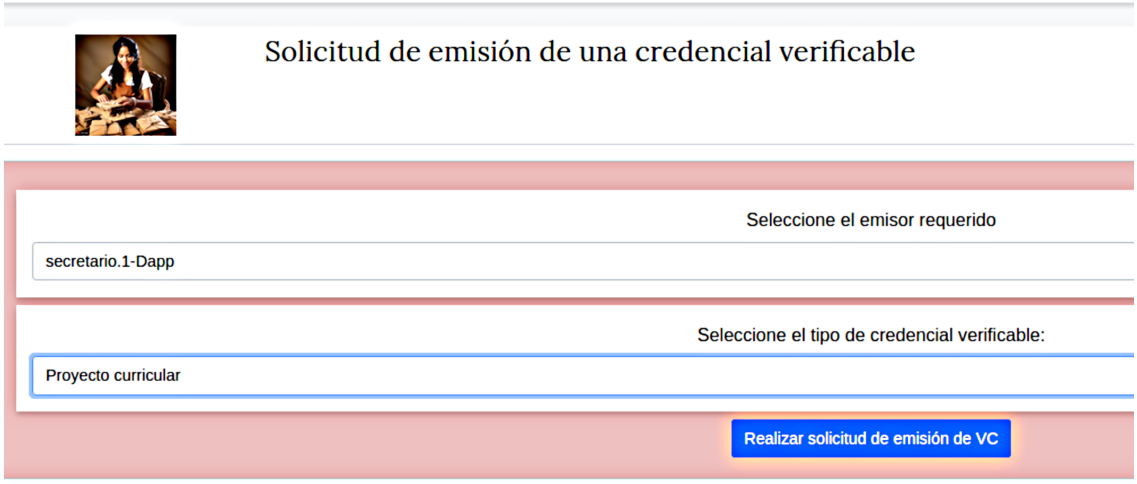
(B) Transacciones asociadas a la creación de los usuarios para el caso de prueba en Aletheia-Dapp.

FIGURA 5.5: Transacciones asociadas a la creación de usuarios en Aletheia-Dapp.
Fuente: Elaboración propia.

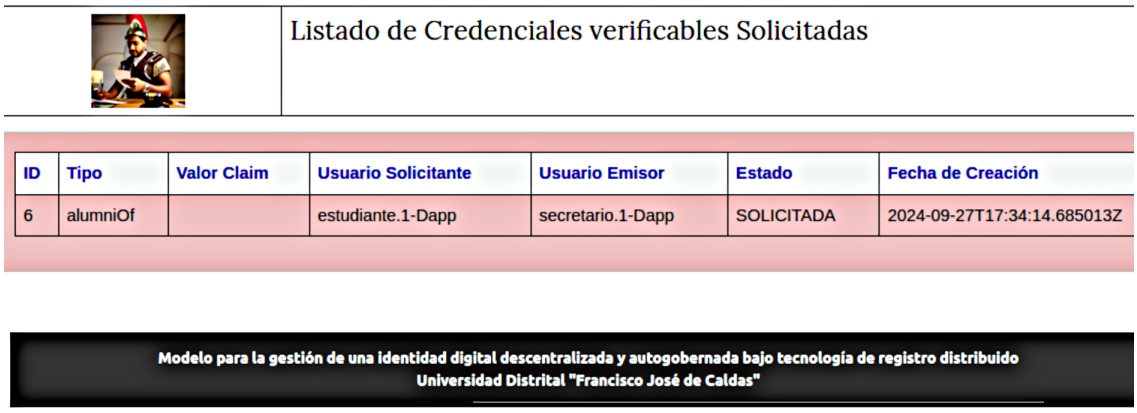
El backend de Aletheia-Dapp cuenta con un servicio de credenciales que se integra con una base de datos relacional para almacenar y gestionar el ciclo de vida de las solicitudes de emisión de VC. La Tabla 5.4, presenta el esquema aplicado para almacenar los datos de una solicitud, incluyendo el estado de la solicitud, los datos del usuario y los detalles de la VC a emitir. La Figura 5.6, presenta la petición realizada por el usuario "estudiante.1-Dapp".

Los campos que conforman la Tabla 5.4 son:

- Identificador: Un atributo interno que permite enumerar las solicitudes recibidas.
- Marca de tiempo: Indica el momento en que se realizó la solicitud.
- Estado inicial: Se establece por defecto como "Solicitada". Los otros estados pueden ser: "Generada" o "Rechazada".
- Tipo de credencial: En este caso, se especifica como "*alumniOf*". El sistema permite un total de cinco tipos diferentes de credenciales: *University Degree Credential* ("Título Universitario"), *Alumni Credential* ("Facultad a la que pertenece"), *alumni Of* ("Proyecto curricular"), *current Status* ("Estado académico del estudiante"), *status Reason* ("Descripción del estado académico"). Estos tipos de credenciales se encuentran definidos en la plantilla definida por la *W3C* [289].



(A) Solicitud de emisión de una credencial verificable.



(B) Listado de solicitudes de emisión de VC realizadas por el usuario estudiante.1-Dapp.

FIGURA 5.6: Solicitud de emisión de una credencial verificable.
Fuente: Elaboración propia.

- Nombre del usuario emisor, “secretario.1-Dapp”.
- Nombre de usuario receptor o solicitante, “estudiante.1-Dapp”.

La estructura de esta tabla no solo facilita la gestión de las solicitudes de emisión, sino que también asegura la trazabilidad y la integridad de los datos relacionados con las credenciales verificables emitidas.

A continuación, el usuario emisor (“secretario.1-Dapp”) selecciona la solicitud a procesar, en este caso identificada con el número 6. El Emisor verifica el cumplimiento de las condiciones según la lógica de negocio definida en el marco de gobernanza y procede a construir una credencial genérica, cuya estructura se detalla en el código fuente 5.1. Esta VC genérica incluye los siguientes elementos: (a) un identificador único universal asignado de forma aleatoria para garantizar la unicidad de la credencial; (b) la especificación del tipo como “credencial verificable”; (c) el DID del emisor asignado por Aletheia-Dapp; (d) la fecha de emisión, que corresponde al momento de inicio del proceso; (e) la fecha de vencimiento, e establecida por defecto seis meses después de la emisión. Es importante señalar que este período de validez debe ser un parámetro configurable en el sistema acorde con el marco de gobernanza; (f) información específica de la credencial compuesta por el DID del futuro poseedor, que debe coincidir con el identificador de la Aletheia *Wallet* donde se almacenará la

identificador	6
Fecha de creación	2024-09-27T17:34:14.685013Z
DID solicitante	did:key:z6Mkn8AkWKht7hqfvo47JH3nYjV4CUjBYMmDAT7NrDuzSyux Debe coincidir con el DID de la billetera del Poseedor.
Estado	Solicitada
Tipo de credencial	alumniOf
Usuario emisor	secretario.1-Dapp
Usuario solicitante	estudiante.1-Dapp

Tabla 5.4: Datos incluidos en la solicitud de emisión de una VC.
Fuente: Elaboración propia.

VC, junto con el valor de la afirmación, que en este ejemplo corresponde al proyecto curricular de ingeniería electrónica. Es importante mencionar que este caso de prueba se adhiere al contexto definido por el *World Wide Web Consortium* para las Credenciales Verificables, en su versión 1.0 [288], y sigue la plantilla de ejemplo proporcionada [289] por esta misma organización.

Código fuente 5.1: Inicialización de una credencial verificable genérica

```
1 {
2     "id": "urn:uuid:35d29c00-2239-43e2-9541-71265d2d60ed",
3     "type": [
4         "VerifiableCredential"
5     ],
6     "issuer": "did:key:z6MkvsDVd6yyk4paoFFKCbtyYYu1qUcuLY7Jru1aBxTf4kZG",
7     "issuanceDate": "2024-09-27T15:18:49.969243Z",
8     "expirationDate": "2025-03-27T15:18:49.969243Z",
9     "credentialSubject": {
10        "id": "did:key:z6Mkn8AkWKht7hqfvo47JH3nYjV4CUjBYMmDAT7NrDuzSyux",
11        "alumniOf": "Ingenieria electronica"
12    },
13    "@context": [
14        "https://www.w3.org/2018/credentials/v1",
15        "https://www.w3.org/2018/credentials/examples/v1"
16    ]
17 }
```

Para la emisión de la credencial verificable, se adiciona un mecanismo de verificación basado en llaves criptográficas a la VC genérica presentada en el código fuente 5.1. Este mecanismo se implementa mediante la invocación del método "*keyToVerificationMethod*", el cual convierte una clave criptográfica en formato *JWK* en un método de verificación para la VC. La información de claves de la cuenta del Emisor, "secretario.1-Dapp", se muestra en el código fuente 5.2. El método "*keyToVerificationMethod*" está integrado en la librería *DIDKit* y genera una estructura que define como se usará una clave para verificar la credencial, eliminando así la dependencia de una autoridad centralizada. Esta funcionalidad es fundamental para el desarrollo del modelo, ya que protege la privacidad y otorga a los usuarios un mayor control sobre su identidad.

Código fuente 5.2: Configuración de las cuentas de Emisor, Verificador y Poseedor

```
1 {
2     "Issuer" :"{
3     "did:key":"z6MkvsDVd6yyk4paoFFKCbtyYYu1qUcuLY7Jru1aBxTf4kZG",
4     "username": "secretario.1-Dapp",
5     "publicKey": "-----BEGIN RSA PUBLIC KEY-----
          MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxjuoqzalrrjaZF2LTmfxFs2RYSdPZ3gJmz61L0DkLCNW
          TAqT4MxFd9iHOP17jGy59rH8PlgJPIs7i/vs/yqaRhfGYSBbesHVls5vOJdivMTpbfHCj4cKdioX/Ga68Mjc52ch
          Bxx0yPKel85ogdT+fsDWyc/xHuNZxjIeXxuk9zca+FaMXOod0Cvv7Esh/MP4mBDcnwR8GB/cbfW+LWUG3HdQzPJ
          ri4IPWGjX1fD6R72vDKuxwS+KDmXhE2Z+ddey86HpLWX8gPZsReCQqXO8I/M57ZLCNlnL8+DUA8mR4CyDVpFivVc
          E6kAe4e0xRvmSwL+j2kcR10ZdVpLL+gp/RwIDAQAB -----END RSA PUBLIC KEY-----",
6     "jwk_key": "{
7             "kty":"OKP",
8             "crv":"Ed25519",
```

```
9               "x":"894LrcIZdc7edW7NBFL_OKhymTlMsIfmKpS2pb8o9zM",
10              "d":"HvQJnnSOmcbBIiLYuxeEym6eFlLZ41PphZk0uhj6pks"
11              }"
12      }",
13
14      "Holder": "{
15      "did:key":"z6MkfBTnYg5SK4XcNkdtrMVzwTNTNvk1F8aYo7cFvsTPn5N9",
16      "username":"estudiante.1-Dapp",
17      "publicKey":"-----BEGIN RSA PUBLIC KEY-----
            MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsytWuBFeNcFX/aOc7Cvx6MEcJE6+5ggACCyWM
            EKr0GMc5Ht5SBkV8TfZHut9h5G3A2sAfZPmifd6S41axHgTU2q+8sEUOnu7dUj+ydXz959w/ElXcWpmc4AYbJK0
            c4xsb1stg7HOqmQdqQv3y7JyMEI5UNok8Ke2gRSYT9mx6CMgVIibvDJ1dbWju7QHAs1s+jNujW5IBX0728FQn510
            ROJE8hUNahmU08r8KicVDW9aRJFbLyg6F0O6zvkt5EpfXcjzQOIHvbDiHcBi4O2eGAodntYNznjFNfl6HNxc/aG1
            JmY+YIxbJycTJf1Q8kRmnycza3XH82n9zFivZuIB9wIDAQAB-----END RSA PUBLIC KEY-----",
18      "jwk_key":"{
19              "kty":"OKP",
20              "crv":"Ed25519",
21              "x":"Cs-rTIkIgfk2YPUvYDROg-YjvPBburBidHbQeQaxHQI",
22              "d":"FYubgpZWf6ZgsEgDuziw8Vg5byD8n4eeCS6g-E9PmAQ"
23              }"
24      }",
25
26      "Verifier": "{
27      "did:key":"z6MkpDLhiEm2gtSsGUKBeFN97nReaJ1FXxJiy2JTenPHTP8g",
28      "username":"unidadInvestigacion.1-Dapp",
29      "publicKey":"-----BEGIN RSA PUBLIC KEY-----
            MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqSY8pSRwY8BElrLEy3wOPUsB5DrXnwiiYe87UI71Zt1w
            tpZdyQ8V2xdlfYsHzzQN59IOjoCGs5AHmbnnpL3cCqnI3VJfXpDBXnAdLA/eI6dm/+Z2zNdaJng30tfeHbz1DP5J
            HR+sz2pH0ToMXlJI2ULcGxkNcRO6G/C3x4rMXJgrNpF5bFOucfJ2TI2QRQrfqsiHsSsTjImJutvTNCVGp3KrMxdd7
            UNdiNa8mG368XkCnUrVhwQ4JV07+VsODREQZX5fzmO71Y/R0t/VqAdAJaOrEGnhxKOTSyEvp6syiempuD2EDXZVm
            WSK9hwe10+3ffttliejiAdMD9McFgY84QIDAQAB-----END RSA PUBLIC KEY-----",
30      "jwk_key":"{
31              "kty":"OKP",
32              "crv":"Ed25519",
33              "x":"kQQBAAd4dBsmKbc8bknGBiGrwdBA_WS5YWteNY_YHWU",
34              "d":"Fx_hqIkHPqeVkxpqXvvaxMW3MzSGFKgO2Xu8A09G-Jw"
35              }"
36      }"
37}
```


Una vez establecido el mecanismo de verificación, se procede a emitir la VC utilizando la función "*issueCredential*" de la misma librería. Este método permite crear una credencial verificable resistente a manipulaciones, que puede ser verificada criptográficamente mediante el método previamente definido. La credencial emitida se visualiza en el código fuente 5.3, se encuentra en un formato de texto plano, y está lista para ser cifrada y almacenada de manera segura en un sistema de archivos descentralizado.

CÓDIGO FUENTE 5.3: Credencial verificable emitida por secretario.1-Dapp


```
1{
2       "@context": [
3               "https://www.w3.org/2018/credentials/v1",
4               "https://www.w3.org/2018/credentials/examples/v1"
5       ],
6       "id": "urn:uuid:35d29c00-2239-43e2-9541-71265d2d60ed",
7       "type": [
8               "VerifiableCredential"
9       ],
10      "credentialSubject": {
11              "id": "did:key:z6Mkn8AkWKht7hqfvo47JH3nYjV4CUjBYMmDAT7NrDuzSyux",
12              "alumniOf": "Ingenieria electronica"
13      },
14      "issuer": "did:key:z6MkvsDVd6yyk4paoFFKCbtyYYu1qUcuLY7Jru1aBxTf4kZG",
15      "issuanceDate": "2024-09-27T15:18:49.969243Z",
16      "proof": {
17              "type": "Ed25519Signature2018",
18              "proofPurpose": "assertionMethod",
19              "verificationMethod": "did:key:z6MkvsDVd6yyk4paoFFKCbtyYYu1qUcuLY7Jru1aBxTf4kZG#
                    z6MkvsDVd6yyk4paoFFKCbtyYYu1qUcuLY7Jru1aBxTf4kZG",
```

```
20        "created": "2024-09-27T20:18:49.971779Z",
21        "jws": "eyJhbGciOiJFZERTQSIsImNyaXQiOlsiYjY0Il0sImI2NCI6ZmFsc2V9..FPbO5tVn6u6O2tTv
              ArFjk6zD7Mo8RMvsEdUtDr68tQBpJyPr0MfSh3WjiaLCFy1a2mkJPTix8rUd2fTUyHYFBg"
22    },
23    "expirationDate": "2025-03-27T15:18:49.969243Z"
24 }
```


En el siguiente paso, el servicio de "Cifrado AES" genera una clave secreta de 256 bits para aplicar el algoritmo *Advanced Encryption Standard* -AES-. La elección de AES como método de cifrado se fundamenta en factores críticos para la seguridad de la información, por ejemplo: (a) resistencia a ataques: AES ha demostrado resiliencia frente a diversos tipos de criptoanálisis y vectores de ataque; (b) eficiencia en el cifrado de datos: alto rendimiento tanto para el cifrado de datos, permitiendo un procesamiento eficiente de grandes volúmenes de datos; (c) Alto nivel de adopción: Su uso generalizado por organizaciones gubernamentales, instituciones financieras y empresas tecnológicas líderes respalda su uso estandarizado, confiabilidad y eficacia; (d) Estandarización: AES fue seleccionado por el Instituto Nacional de Estándares y Tecnología de Estados Unidos como estándar de estatal de cifrado [291]. Una vez generada, esta clave secreta se utiliza para cifrar la VC emitida, garantizando su confidencialidad. Posteriormente, para asegurar la integridad del proceso, la propia clave secreta es cifrada utilizando la llave pública *RSA* del futuro Poseedor, la cual se obtiene del registro distribuido. Este enfoque de doble cifrado proporciona una capa adicional de seguridad, asegurando que solo el destinatario autorizado pueda acceder a la clave secreta y, por ende, a la VC cifrada. El resultado del proceso de cifrado se ilustra en el código fuente 5.4.

CÓDIGO FUENTE 5.4: Credencial verificable cifrada con la llave secreta AES


```
1 "Credencial verificable Cifrada": "ZKQuE8YdVAP7pJd/5rx0kQgsUHRSHZhFZWNIsBdy9hBvYWZGNh93WPq9CBf
    seI3kNgYd9ySovS/eDqpCnu3HpPmmIRpa8SqWALQ1cSH8VJn3oDuayvjdSqJnXYnNsVuT1F13wHo71lOUE/hAReJGZ+
    J7DclSCO+QhPosc9QadgSd+Fj7hNNEMm/qaiKbp4Dk3uxquVnwaayMLGeuw/WEx52kteXoLtWARsK4SfyRc1N9KkP2
    frHhJAAfQAkRUGbYtypmeNiW8yCCf1jGy7SV88XiYEZ+6i7YkIC7adj+vnoPjIcbQ3YHn1I/iWxWGmAQlzUP0vbwHHq
    d57ymW3BZu/3Jp80DPeX4PXGYmZ6lW+rTzfJeIC2dUWg0ZM6tBgTtt7LJ7/z5JIwtSzSLM9b0fMJWPVgR4nu9yQSOLC/
    nBhlITQzB/EmKz96kEiX5UY/mJXwqo8xBmg0VOZ9vJfyXcD1dNoiwGPQgjItYHAPmcz8XLMVjDqNAyBH07zQWnvB9s
    T0Hg5KFDO/6T7awMvieB5ivGQ5vLv/0/StMmnlIXX1AxoLbtCp7+nQ7Gd1mn1lJ1APLmKMEa5LJszz0UJV+EZXfML+/
    gI1y+XU8v4wgd1T2xmxjdvb6JM8dvX47fo5fS/fm5jBgTXOzQjZUCypwn19f9uZyDIuIwN1XH7opZX5QqS1n+o+ohI3
    i9V/Uto0O2U5M0PpRvl41DUnnA2kOh0f1sLephBeNsxes/0qu62TWMyqzMn0oo1djvmTr7Nm1hb4/ESKaM9+DWNXyY
    y7qaIQk8+mGPsl1eMjCzpdxvvxn+iiddG8Ug5rAQz7H2r1nlcWmHJpFdXHkUzFUyYbS4M6gTEVKGefqcwgRqIgVOR
    xE147O+9t3GjMu3MSi/MwovwuSzthHpoYifc9P67SMQFZl9tilH6nQOW5cSYVZyHqXmxFzT2rHToMBiwgHU40j74XUP
    YlfUGRmwpPA699837v4rckcwdmwLI2ERcOqz7rCIBGY1N1ZNaZtjb7bk8lr9yX3qDGlSaIWZ7B81U3q9PZA1pN/0jX8O
    Attod1bswnNuP5C0hgz9Ou6uFndy1sZfmJYpD7QtfGOZBJD6LKT/02qo5bl3C06iqEwhTqa3bSI4pNdGnyLjpuWKaN4Q
    G8bnTqagYv47IktZaAVu/g=="
```


La clave secreta *EAS*, junto con la Credencial Verificable, ambas debidamente cifradas, son enviadas al "Servicio de Credenciales" para su posterior procesamiento. La VC es remitida al "Servicio *IPFS*", el cual, para este caso particular, está conectado a *Pinata Cloud*. Este servidor se encarga de calcular el *hash* de la credencial, obteniendo un identificador único para el archivo, que en este ejemplo ha sido: bafkreihae3bxxhgrc3ziylbjdlq6g3kagsur4zb5bqrqfldtbzhycb4x2a. Este *hash* actúa como un marca inmutable del contenido y asegura su integridad. Una vez calculado el *hash*, la VC es almacenada en *IPFS*, lo que permite su consulta pública y verificación futura. El documento cargado a *IPFS* dispone de una referencia que proporciona un acceso directo permitiendo verificar su existencia y contenido en cualquier momento [1]. Finalmente, tanto el *hash* generado en *IPFS* como la clave *EAS* cifrada son registrados de manera segura en la *blockchain*. Esta operación garantiza la inmutabilidad y trazabilidad de la credencial, protegiendo tanto la privacidad del usuario como la integridad de los datos a lo largo del tiempo.

La información de la transacción donde se realizó la notarización de la VC se puede ver en el

[1] https://emerald-quiet-tortoise-545.mypinata.cloud/ipfs/bafkreihae3bxxhgrc3ziylbjdlq6g3kagsur4z4b5bqrqfldtbzhycb4x2a?pinataGatewayToken=A_KWFBIDSBDgLeUhP_SmM6ZqQzYZAFt9IlufnNHzcHtYBg3_Hwyp891PZJHKFLRt

documento JSON presentado en el código fuente 5.5.

CÓDIGO FUENTE 5.5: Datos de la transacción en blockchain relacionada con la notarización de la credencial verificable emitida


```
1{
2    "TX Hash": "0x1ebf8dbfb5fda4166d48b9dcd817f6526ee2e898bb96b8af386b6857fb59f43a",
3    "Gas Used": "349317 gwei",
4    "urn:uuid": "35d29c00-2239-43e2-9541-71265d2d60ed",
5    "IPFS Hash": "bafkreihae3bxxhgrc3ziylbjdlq6g3kagsur4zb5bqrqfldtbzhycb4x2a",
6    "Clave EAS Cifrada": "lTX6gR58PhQh8H9IVNLyEUmTvLU1/hT3cqzAOiE4CwilBOxk78D+zOYJvhY7gJZyX1ZoW
         L7Q0ELpS88/xaeJRbHw6dCVxg8xvharOFuSgYclUffzSzW7h9/d35rdVTlAXcxDsPVdJBGOigLTnZGIxgI1MRIE
         KLjxUhDtyYG9fFUIBxYW4m8+MuOEJByBJe9KAatwrJM/0juZCWQlVn3ht6TWlvcG5zwlnzKDVczNK5LCuH
         WKMPoNQJxFqs8Tzy92gXnzWE3BsTEFxdGBQrV6AGfGgd2J7TttuKQiCM2zsinA77voUr36XeN91icZcTBahI
         tM172o4v5pkeVz1q9VCA=="
7}
```


Finalizado el proceso de emisión de la VC, el usuario solicitante podrá visualiza el estado de la solicitud desde su *dashboard*, como se muestra en la Figura 5.7. La tabla que contiene esta figura, proporciona información detallada sobre cada credencial solicitada. La columna Tipo contiene el tipo de credencial usado, que en este caso es "*alumniOf*", señalando la pertenencia a una institución académica. La columna *Valor Claim* especifica el valor de la afirmación como "Ingeniería Electrónica", vinculando al usuario con este programa curricular. El Usuario Solicitante se identifica como "estudiante.1-Dapp", mientras que el Usuario Emisor es "secretario.1-Dapp". La credencial se encuentra en el estado "Generada", lo que indica que ha sido procesada y está disponible para el solicitante. El Token de Certificado es un identificador único en formato URN, en este caso urn:uuid:35d29c00-2239-43e2-9541-71265d2d60ed, que permite rastrear la credencial emitida. La Fecha de Actualización muestra el último momento en que la credencial fue actualizada, marcado como 2024-09-27T20:18:49.484807Z. Finalmente, la columna Acción proporciona un enlace "Ver Credencial" para que el usuario pueda acceder a los detalles completos de la credencial emitida.

Listado de Credenciales verificables Solicitadas

Tipo	Valor Claim	Usuario Solicitante	Usuario Emisor	Estado	Token de Certificado	Fecha de Actualización	Acción
alumniOf	Ingenieria electrónica	estudiante.1-Dapp	secretario.1-Dapp	GENERADA	urn:uuid:35d29c00-2239-43e2-9541-71265d2d60ed	2024-09-27T20:18:49.484807Z	Ver Credencial

Modelo para la gestión de una identidad digital descentralizada y autogobernada bajo tecnología de registro distribuido
Universidad Distrital "Francisco José de Caldas"

FIGURA 5.7: Credencial Verificada emitida para el usuario estudiante.1-Dapp.
Fuente: Elaboración propia.

5.3.2.1.1 Visualización de una credencial verificable: La visualización de una VC se realiza conforme al diagrama de secuencia presentado en la Figura 4.7. Este flujo involucra múltiples servicios que colaboran para recuperar y descifrar la VC de manera segura. el "Servicio de Credenciales" actúa como intermediario, obteniendo el Token del Certificado y consultando el sistema distribuido para recuperar el *hash IPFS* y la clave secreta *AES* cifrada. Esta clave secreta está protegida por cifrado asimétrico, utilizando una clave pública *RSA* del usuario, lo que garantiza que solo el Titular pueda descifrarla con su clave privada. La clave *AES* es utilizada para proteger

FIGURA 5.8: Visualización de la credencial verificable emitida.
Fuente: Elaboración propia.

la credencial mediante cifrado simétrico, lo que aporta una capa adicional de seguridad, dado que *AES* es altamente eficiente para el cifrado de grandes volúmenes de datos, como en este caso. A través del Servicio *IPFS*, la credencial cifrada se recupera de un almacenamiento descentralizado. Posteriormente, el sistema descifra la clave secreta AES mediante el módulo de Cifrado *RSA*, y una vez recuperada la clave secreta en texto plano, se procede a descifrar la credencial.

Se procede de la siguiente manera, al consultar el listado de solicitudes de emisión de credenciales verificables, el usuario "estudiante.1-Dapp" observará que se ha emitido una VC, como se muestra en la Figura 5.7. Al seleccionar el enlace "Ver Credencial", se obtendrá desde el registro distribuido el token del certificado "35d29c00-2239-43e2-9541-71265d2d60ed", el *hash* de *IPFS* "bafkreihae3bxxhgrc3ziylbjdlq6g3kagsur4zb5bqrqfldtbzhycb4x2a" y la clave AES cifrada. Esta información está contenida en la transacción de creación de la VC, la cual puede consultarse en el código fuente 5.5. Dado que ya se conoce el *hash IPFS*, se procede a la recuperación de la VC cifrada, obteniendo el *digest* que se muestra en el código fuente 5.4. El siguiente paso consiste en descifrar la clave secreta *AES* (ver código fuente 5.5) utilizando la llave privada *RSA* de "estudiante.1-Dapp". Como resultado de este proceso, se obtiene la cadena "o6oQ uYyd Xzk7 OnPx JHqB yFh1 NoAi LVvt /5O8 59dN 5kI=". Finalmente, utilizando la clave secreta *AES* en texto plano, es posible descifrar la credencial verificable y proceder a su visualización, tal como se presenta en la Figura 5.8. Ahora, el poseedor podrá revisar la VC emitida en su totalidad y, si está de acuerdo con la información, proceder a almacenarla en su billetera digital.

5.3.2.1.2 Almacenamiento de una credencial verificable: El almacenamiento de la VC se lleva a cabo siguiendo el diagrama de secuencia presentado en la Figura 4.8.

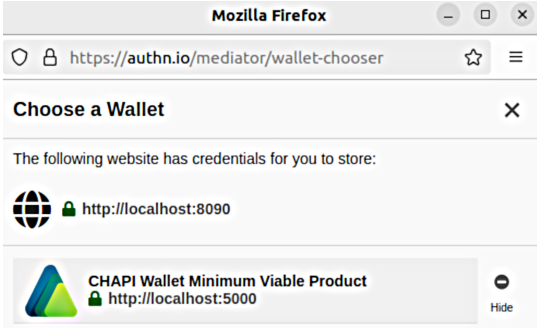


FIGURA 5.9: Mediador para la comunicación entre Aletheia-Dapp y Aletheia *Wallet*.
Fuente: Elaboración propia.

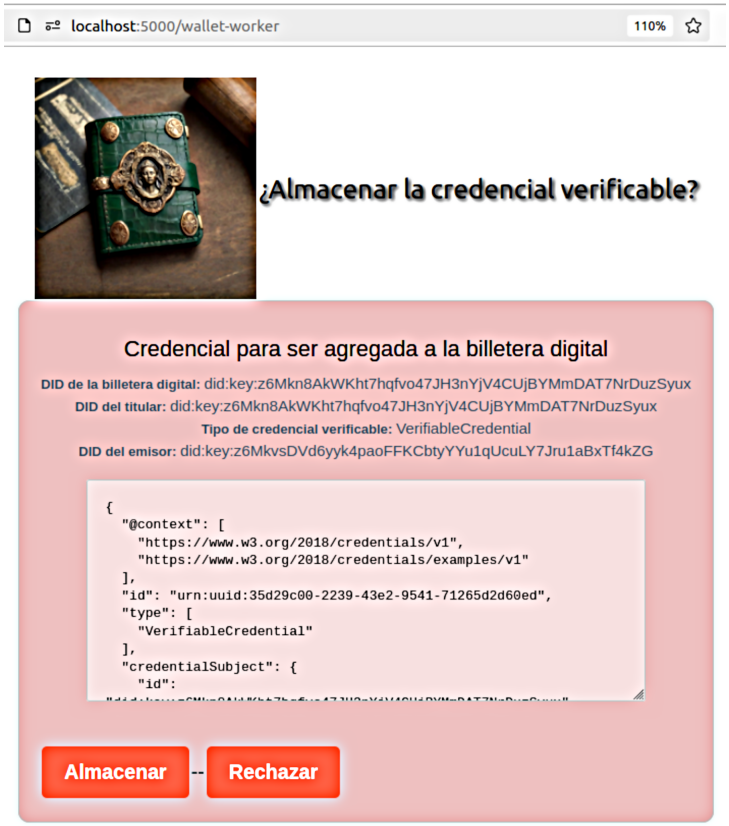


FIGURA 5.10: Interface de Aletheia *Wallet* para el almacenamiento de una credencial verificable emitida.
Fuente: Elaboración propia.

Una vez que la VC está lista para ser enviada a la billetera digital, el usuario inicia el flujo invocando a "Almacenar en Aletheia *Wallet*". Esto genera una comunicación con la billetera digital utilizando un servicio de mediación de conexiones proporcionado por el W3C [292]. Este servicio facilita la interacción entre Aletheia-Dapp, disponible en la dirección `localhost:8080`, y Aletheia *Wallet*, desplegada en `localhost:5000`. El llamado al mediador se ilustra en la Figura 5.9. El poseedor debe iniciar sesión con sus credenciales de acceso, y se valida que el Identificador Descentralizado de Aletheia *Wallet* coincida con el DID del titular de la VC. Si esta condición se cumple, el proceso abre la interfaz en la billetera para permitir el almacenamiento de la credencial, como se muestra en la Figura 5.10.

Finalmente, la Credencial Verificable se transforma en un string en formato JSON para facilitar

su manipulación. Luego, se realiza una validación adicional de la propiedad de la VC mediante la comparación del Identificador Descentralizado, asegurando que la credencial esté efectivamente vinculada al titular correspondiente. Tras esta comprobación exitosa, el estado de la billetera digital se actualiza para incorporar la nueva VC. Este proceso permite que la VC esté automáticamente disponible para su uso, como se detalla en la Figura 5.11. Aletheia se enfoca en la emisión de Credenciales Verificables con un fuerte enfoque en la preservación de la privacidad del titular de los derechos de identidad. Este modelo permite que el usuario mantenga el control total sobre sus VC, ya que estas se almacenan en una billetera digital, donde el propietario es la máxima autoridad sobre sus datos. De esta manera, Aletheia garantiza que solo el titular tiene la capacidad de administrar, compartir o revocar su información, reforzando los principios fundamentales de la Identidad autogobernada referentes a existencia, control, protección y privacidad. Este modelo no solo protege la información sensible, sino que también otorga a los individuos una mayor capacidad para gestionar su identidad en múltiples contextos sin depender de terceros de confianza.

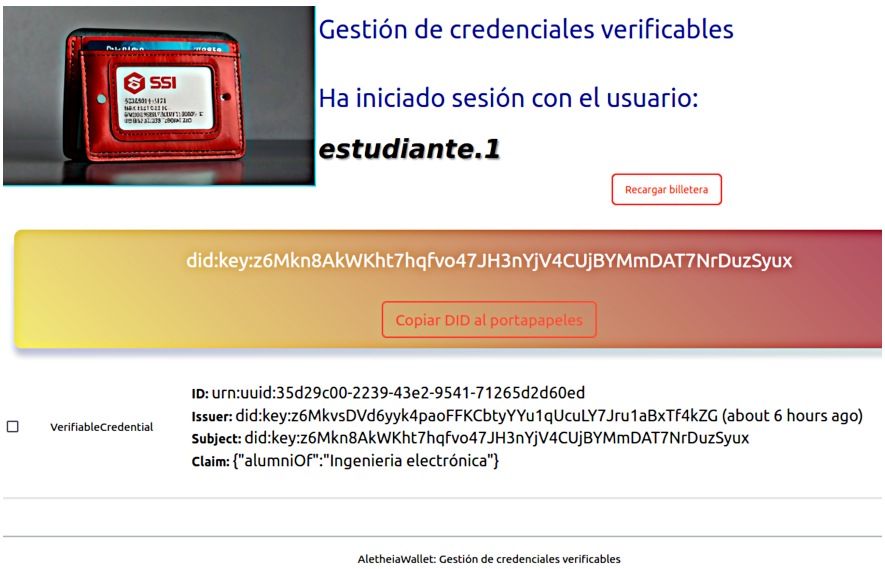


FIGURA 5.11: Vista actualizada de Aletheia *Wallet* para el usuario estudiante.1-Dapp incluyendo la credencial verificable recién adicionada.
Fuente: Elaboración propia.

5.3.2.2 Realización de una presentación verificable

La Figura 4.9 muestra la secuencia de pasos necesarios para la construcción de una presentación verificable. La PV es generada por un titular de los derechos de identidad, quien debe iniciar sesión en Aletheia-Dapp para comenzar el proceso. Como se mencionó en secciones previas, un usuario con rol de Titular (Poseedor o *Holder*) puede generar PV o consultar el estado de las solicitudes presentadas. La Figura 5.12 visualiza el panel de control de un titular, en este caso, para el usuario "estudiante.1-Dapp". El proceso de generación de la PV se inicia seleccionando la opción "Realizar una Presentación Verificable".

La preparación del envío de una PV requiere de la siguiente información: primero, determinar el verificador al cual se desea realizar la presentación. De acuerdo con el marco de gobernanza establecido (ver sección 5.1), para este caso de prueba se dispone de una lista de verificadores aprobados, de la cual el Poseedor selecciona un verificador destino. En segundo lugar, se debe incluir un atributo informativo que oriente al verificador sobre la intención de la solicitud. Finalmente, se

FIGURA 5.12: *Dashboard* en Aletheia-Dapp para el estudiante.1-Dapp.
Fuente: Elaboración propia.

debe seleccionar el conjunto de VC que se desea incluir en la PV.

La Figura 5.13 muestra la interfaz de Aletheia-Dapp, que facilita el ingreso de estos datos. La selección de las credenciales verificables preserva la privacidad y el control por parte del titular, ya que, al estar almacenadas en Aletheia *Wallet*, la DApp no tiene acceso directo a ellas. Por este motivo, es obligatorio realizar un proceso de autenticación en la billetera para permitir su uso. La petición de comunicación desde Aletheia-Dapp:8090 hacia Aletheia *Wallet*:5000 se puede observar en la Figura 5.14, con subsecuente ingreso de las credenciales de acceso por parte de "estudiante.1-Dapp", ilustrado en la Figura 5.15. Se resalta nuevamente, que esta interacción se lleva a cabo mediante el servicio mediador proporcionado por la W3C [292].

Inmediatamente después de validar el acceso a la billetera digital, se consultan y listan todas las credenciales verificables del titular, las cuales quedan habilitadas para ser incluidas en la PV. En este momento, el usuario "estudiante.1-Dapp" dispone únicamente de una VC, como se observa en la Figura 5.16, también se visualiza que la solicitud de recuperación de la VC fue realizada desde Aletheia-Dapp. El proceso de consulta de la VC que involucra el descifrado de la misma se discutió en la sección 5.3.2.1.1. En este punto el usuario selecciona todas las VC que desee incluir y solicita la generación de la PV.

La presentación verificable creada se encuentra en formato *RAW*, y se incluye en el código fuente 5.6. Este formato *JSON* representa una PV según el estándar de la W3C. Contiene una estructura de credenciales verificables, en donde la presentación incluye una lista de credenciales (*verifiableCredential*), cada una emitida por una entidad específica (*issuer*). La credencial tiene un sujeto (*credentialSubject*), identificado por un DID, que detalla atributos como "*alumniOf*", indicando que pertenece a un proyecto curricular (en este caso, "Ingeniería Electrónica"). Cada credencial cuenta con una prueba de autenticidad (proof), que se genera utilizando el esquema de firma Ed25519Signature2018, lo cual garantiza la integridad y autenticidad de la información. Este objeto *proof* proporciona una firma digital que autentica el documento o mensaje, y se puede verificar utilizando la clave pública especificada en el campo *verificationMethod*. Además, la inclusión de campos como *proofPurpose*, *created* y *domain* ayuda a contextualizar y restringir el uso de la firma, incrementando la seguridad y la integridad del proceso de validación. La PV también incluye una prueba a nivel de presentación que valida la autenticación del titular (*holder*) y el método de verificación correspondiente. Asimismo, se especifican fechas de emisión (*issuanceDate*) y expiración (*expirationDate*) tanto para la credencial como para la presentación, asegurando un ciclo de vida bien definido de la información presentada.

CÓDIGO FUENTE 5.6: Credencial verificable seleccionada para la realización de la presentación verificable

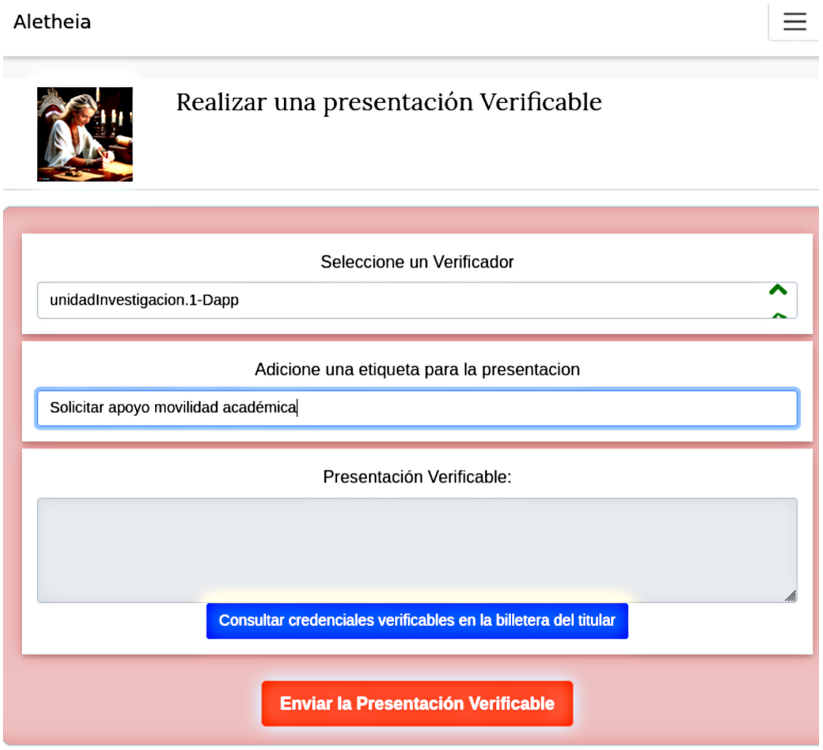


FIGURA 5.13: Información requerida para la elaboración de una presentación verificable. Fuente: Elaboración propia.


```
1 {
2 "holder": "did:key:z6Mkn8AkWKht7hqfvo47JH3nYjV4CUjBYMmDAT7NrDuzSyux"
3 "id": "urn:uuid:f2ae6d5e-84a8-47cb-a7cb-ac226028e0a6",
4 "proof": {
5         "type": "Ed25519Signature2018",
6         "proofPurpose": "authentication",
7         "verificationMethod": "did:key:z6Mkn8AkWKht7hqfvo47JH3nYjV4CUjBYMmDAT7NrDuzSyux#
              z6Mkn8AkWKht7hqfvo47JH3nYjV4CUjBYMmDAT7NrDuzSyux",
8         "created": "2024-10-08T17:19:58.919Z",
9         "domain": "localhost:8090",
10        "jws": "eyJhbGciOiJFZERTQSIsImNyaXQiOlsiYjY0Il0sImI2NCI6ZmFsc2V9..v3VgYNYYRdVQT_d4U
              Aosi449UlpDKfN7Z2NUKKYrbmMpoT_Y0H1wN2JG6rr9_yiIEpeN9Fm5I9vNoixhPqzxKCw"
11        },
12 "type": [
13        "VerifiablePresentation"
14        ],
15 "@context": [
16        "https://www.w3.org/2018/credentials/v1"
17        ],
18 "verifiableCredential": [
19        {
20        "credentialSubject": {
21                "id": "did:key:z6Mkn8AkWKht7hqfvo47JH3nYjV4CUjBYMmDAT7NrDuzSyux",
22                "alumniOf": "Ingenieria electrónica"
23        },
24        "issuanceDate": "2024-09-27T15:18:49.969243Z",
25        "id": "urn:uuid:35d29c00-2239-43e2-9541-71265d2d60ed",
26        "proof": {
27                "type": "Ed25519Signature2018",
28                "proofPurpose": "assertionMethod",
29                "verificationMethod": "did:key:z6MkvsDVd6yyk4paoFFKCbtyYYu1qUcuLY7Jru1aBxTf4kZG#
                      z6MkvsDVd6yyk4paoFFKCbtyYYu1qUcuLY7Jru1aBxTf4kZG",
30                "created": "2024-09-27T20:18:49.971779Z",
31                "jws": "eyJhbGciOiJFZERTQSIsImNyaXQiOlsiYjY0Il0sImI2NCI6ZmFsc2V9..FPbO5tVn6u6O2t
                      TvArFjk6zD7Mo8RMvsEdUtDr68tQBpJyPr0MfSh3WjiaLCFy1a2mkJPTix8rUd2fTUyHYFBg"
```

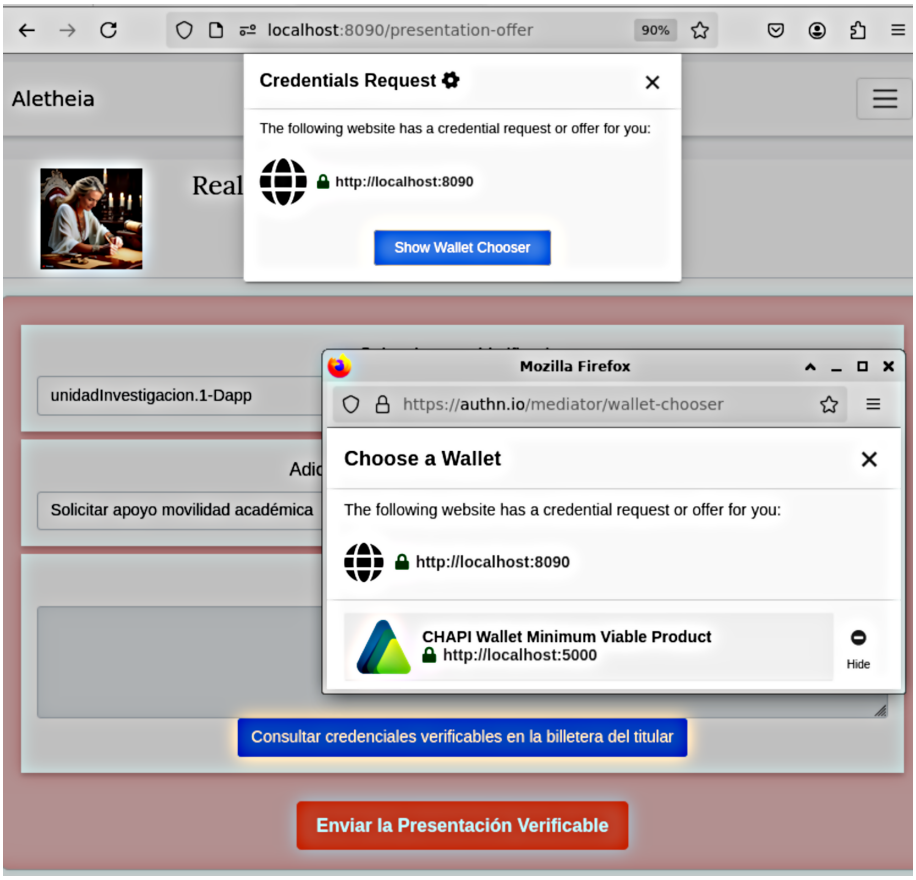


FIGURA 5.14: Llamado al servicio de mediación para la comunicación entre Aletheia-Dapp y Aletheia *Wallet*.
Fuente: Elaboración propia.

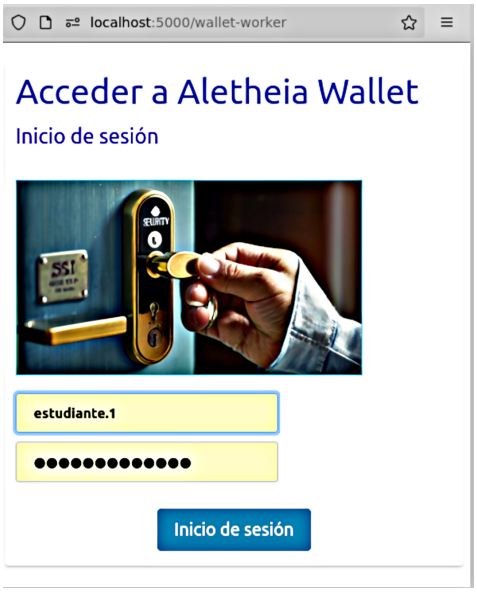


FIGURA 5.15: Autenticación en Aletheia *Wallet*, requerida desde el servicio de presentaciones.
Fuente: Elaboración propia.

```
32                      },
33        "type": [
```

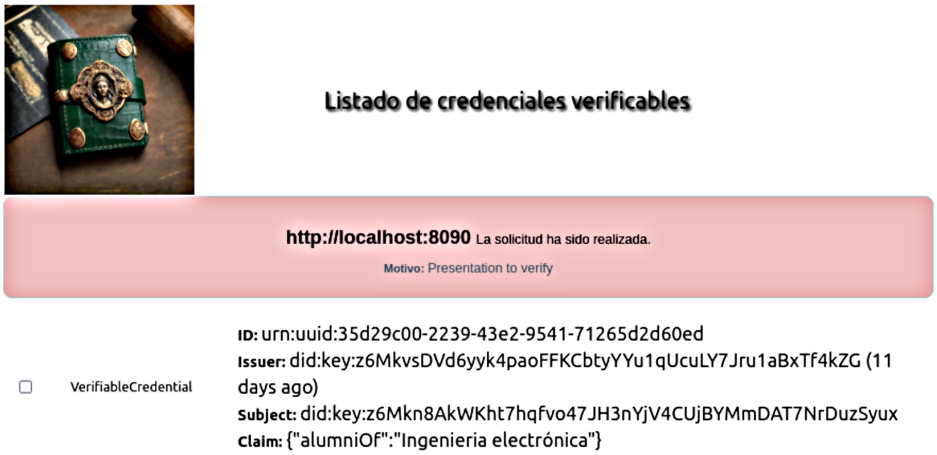


FIGURA 5.16: Listado de VC del estudiante.1-Dapp disponibles para la generación de una PV. Fuente: Elaboración propia.

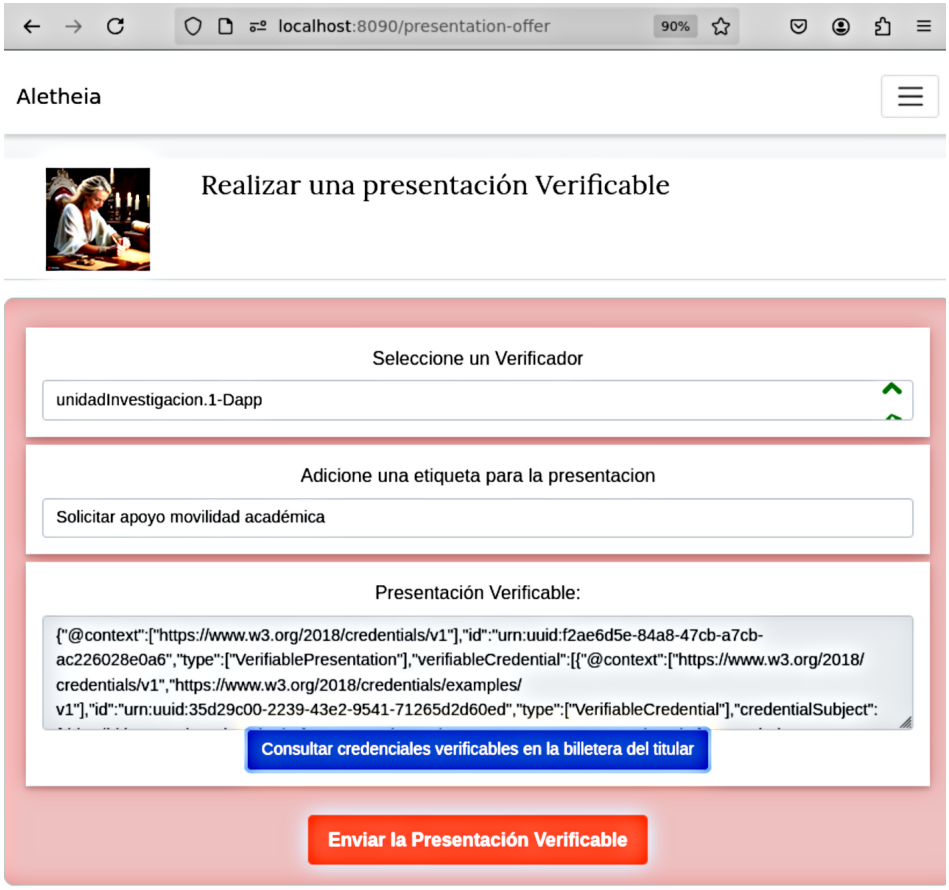


FIGURA 5.17: Estructura final para la generación de la presentación verificable. Fuente: Elaboración propia.

```
34                              "VerifiableCredential"
35                          ],
36          "@context": [
37                  "https://www.w3.org/2018/credentials/v1",
38                  "https://www.w3.org/2018/credentials/examples/v1"
39          ],
40          "issuer": "did:key:z6MkvsDVd6yyk4paoFFKCbtyYYu1qUcuLY7Jru1aBxTf4kZG",
```

```
41          "expirationDate": "2025-03-27T15:18:49.969243Z"
42          }
43          ],
44 }
```

La presentación verificable contenida en el código fuente 5.6 está lista para ser cifrada y notarizada en el registro distribuido. La información de la cuenta del verificador destino, "unidadInvestigacion.1-Dapp", se presentó en el código fuente 5.2. La creación del usuario registra la información en la *blockchain*. Para esta cuenta en particular, dicha información se encuentra en la transacción 0x20ff3cae1b0bc8d76185d5e9e37f7358ae1f9330a77122ff893a2c509409f4f2 (ver Figura 5.5b). La PV se cifra de forma análoga a como se realiza con una credencial verificable. Para ello, se genera una llave AES que se utiliza para cifrar la PV, y esta llave secreta AES se cifra a su vez con la llave pública *RSA* del verificador. El identificador de la credencial (f2ae6d5e-84a8-47cb-a7cb-ac226028e0a6), el *hash IPFS* (bafkreihhtiyddsdzml7wyebt2lu4ybdkudqnmk3ymg64gp75wfdshb6iui) para recuperar la PV cifrada y la clave secreta AES cifrada son incluidos en la transacción en la *blockchain*. La operación fue ejecutada en la TX número 0x7a30 6350 1b1e f3dd 7e51 550b 2d9b 3323 962f fe6c 1c07 86ca 6a52 86b9 f7ec 9783 (ver Figura 5.18).

← BACK
TX 0x7a3063501b1ef3dd7e51550b2d9b3323962ffe6c1c0786ca6a5286b9f7ec9783
SENDER ADDRESS
0x4AfF5efC82C625b1D6Ed2f653C9560D79b10D7A6
TO CONTRACT ADDRESS
0xbB127E3CeF2b0b561EaabB64044cEEDd96047034
CONTRACT CALL
VALUE
0.00 ETH
GAS USED
349317
GAS PRICE
4100000000
GAS LIMIT
9000000
MINED IN BLOCK
44
TX DATA
0x5e5652ac0000000000000000000000000000000000000000000000000000000000000000400000000000000000000000000000000000000000000000000000000000000000000a00
000000000000000000000000000000000000000000000000000000000000002d75726e3a757569643a663261653664356 52d383461382d343763622d613763622d6163323236
303238653061360000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001946261666b726569686874697
9646473647a6d6c37777965627432 6c7534796264 6b7564716e6d6b33796d67363467703735776664736862366975694048 4e356c566b774d483539663264316430454b4454
714d445857462b66354e7573464a73722b59524b5075507146726c38766f5350734e586d517474752f307462346136772b45644d56535a37494252375 64a4c4631306675367
253614e47584367432b6a2b532f4366336b6b567a573069334e574752444d63674c366856334745734163654638333533324137336739486231395 56358382b704b38395034
4b7464392b45754a366e42496b4869413048 2f49685637767a52416930614b636a34644a576f7866785a466c4a4a4a637a2b5a4869484378 4e414c7a58376475444a356e525
2693756465133747979314 44b6e413375385132 6d7649556c4167314d2b44544342556e486f4173366c4b617938685974 4a77434b436f4a6539544e7032672b44314b4a4f51
70794f796d35416e49543353334c36374e7157415034477a714654706d566d557238417a32354f543969413d3d000000000000000000000000
```

Figura 5.18: Notarización de la presentación verificable recién construida.
Fuente: Elaboración propia.

| | |
|---|---|
| Identificador | 4 |
| Token del certificado | urn:uuid:f2ae6d5e-84a8-47cb-a7cb-ac226028e0a6 |
| Fecha de creación | 2024-10-08T17:21:54.145866Z |
| Estado | Generada |
| Objeto | Solicitar apoyo movilidad académica |
| Usuario quién presenta | estudiante.1-Dapp |
| Usuario verificador | unidadInvestigacion.1-Dapp |
| Presentación verificable | urn:uuid:f2ae6d5e-84a8-47cb-a7cb-ac226028e0a6 |

Tabla 5.5: Datos asociados a la presentación verificable realizada por estudiante.1-Dapp

Como último paso se tiene la actualización del registro que gestiona Aletheia-Dapp sobre credenciales y presentaciones verificables. La Tabla 5.5 describe los datos asociados a la presentación verificable realizada por el usuario "estudiante.1-Dapp" que se almacenarán en la base de datos relacional para consulta de la Dapp y generación de la páginas web dinámicas requeridas.
```

5.4 Verificación de la presentación

La verificación de una PV se realiza conforme al procedimiento establecido en la Figura 4.10. En primer lugar, un usuario tipo verificador inicia sesión en Aletheia-Dapp para acceder a su *Dashboard*. En este caso de prueba, la única acción disponible para este tipo de usuarios es consultar y validar PV recibidas (Figura 5.19 y Figura 5.20).

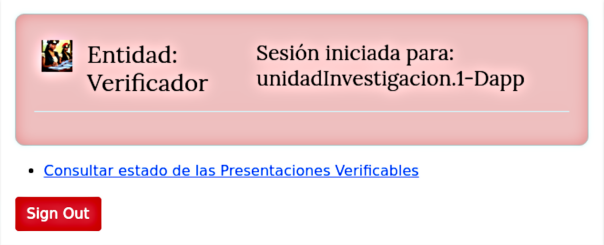


FIGURA 5.19: *Dashboard* en Aletheia-Dapp para el verificador unidadInvestigacion.1-Dapp. Fuente: Elaboración propia.

ID	Tipo	Usuario Solicitante	Usuario Vericador	Estado	Token de Certificado	Fecha de Creación	Acción
4	Solicitar apoyo movilidad académica	estudiante.1-Dapp	unidadInvestigacion.1-Dapp	GENERADA	urn:uuid:f2ae6d5e-84a8-47cb-a7cb-ac226028e0a6	2024-10-08T17:21:54.145866Z	Ver Presentacion

FIGURA 5.20: Listado de presentaciones verificables del verificador unidadInvestigacion.1-Dapp. Fuente: Elaboración propia.

En la Figura 5.20 se detalla la información obtenida de la Tabla 5.5 referente a la PV presentada por el usuario "estudiante.1-Dapp" al verificador "unidadInvestigacion.1-Dapp". Este panel proporciona una visión organizada de las presentaciones verificables disponibles, destacando los detalles esenciales que permiten a los verificadores tomar acción sobre ellas, asegurando así un flujo de trabajo correcto y una trazabilidad precisa del proceso de verificación. En este momento, se puede proceder con la verificación de la PV y modificar su estado conforme al resultado de la evaluación criptográfica.

La lectura de una PV, al igual que la de una VC, comienza con la recuperación de los elementos necesarios almacenados en la *blockchain*: el *UUID*, el *hash IPFS* y la llave secreta AES cifrada mediante la clave pública *RSA* del verificador. A continuación, se procede a descifrar la llave secreta AES utilizando la clave privada correspondiente, la cual está bajo el control del verificador respectivo. Una vez descifrada la llave AES, se utiliza para recuperar la PV en su formato *JSON* (texto *RAW*). Este proceso permite que la PV, ahora descifrada, esté lista para su verificación.

La verificación de la PV se realiza mediante la función *verifyPresentation*, implementada en la "librería *DIDKit*". Este método es crucial para validar la autenticidad e integridad de una PV, requiriendo dos argumentos: una cadena JSON que representa la PV y un objeto de opciones que especifica los parámetros de verificación. Estos parámetros incluyen el propósito de la prueba, el desafío asociado, el dominio relevante y la fecha de creación. "DIDKit.verifyPresentation" ejecuta las verificaciones criptográficas necesarias para garantizar que la presentación no ha sido alterada desde su emisión y que la entidad emisora es confiable y verificable. El proceso de verificación se desarrolla en dos etapas principales: primero, se verifica la presentación en su conjunto utilizan-

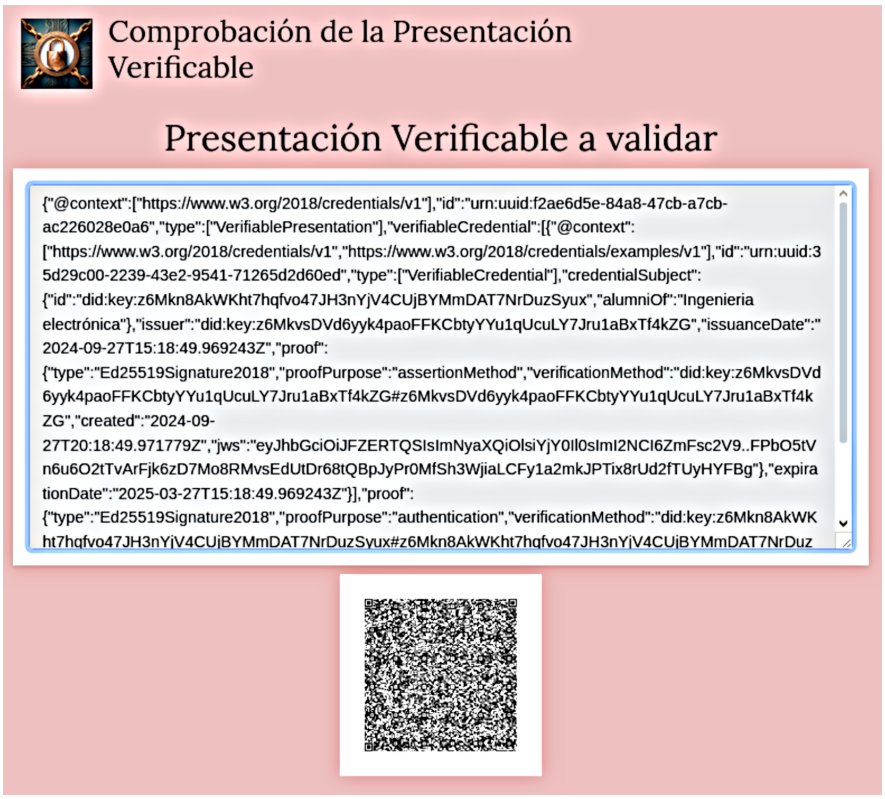


FIGURA 5.21: Visualización y comprobación de la presentación verificable.
Fuente: Elaboración propia.

do “DIDKit.verifyPresentation”, y luego se valida individualmente cada credencial contenida en la presentación mediante “DIDKit.verifyCredential”. El método devuelve un resultado en formato JSON que incluye el estado general de la verificación, detalles sobre el proceso de validación y cualquier error encontrado. En caso de detectar irregularidades, el sistema lanza una excepción, indicando explícitamente la invalidez de la presentación. La ejecución de este método constituye un paso fundamental en la validación de presentaciones verificables dentro de sistemas de identidad descentralizada. Su importancia radica en establecer una entorno de confianza en las VC presentadas, prevenir la aceptación de información no verídica, y garantizar la integridad del ecosistema de identidad digital autogobernada. El resultado de esta verificación es determinante para establecer la validez de la presentación y sus credenciales asociadas, siendo crucial para la toma de decisiones basadas en estas identidades y atributos verificados. El estado de la PV se actualiza en Aletheia-Dapp como se muestra en la Figura 5.22, donde la PV ha sido marcada como “Aceptada”. Este caso de prueba finaliza con la verificación de una PV ya que en este punto se ha logrado completar el flujo de información en el triángulo de la confianza, dando por comprobada la integridad y privacidad de la información bajo el modelo planteado.

En conclusión, la validación del modelo Aletheia ha mostrado de manera contundente que el flujo de información diseñado para la gestión de una identidad digital autogobernada es seguro, verificable y eficiente. A lo largo de la prueba de concepto, se comprobó que cada etapa, desde la creación de la identidad digital en Aletheia *Wallet* hasta la emisión, almacenamiento y verificación de credenciales verificables, cumple con los principios fundamentales de identidad digital autogobernada: existencia, control, privacidad y protección de los atributos de identidad del Poseedor. El uso de identificadores descentralizados, credenciales verificables, almacenamiento descentralizado y tecnología de registro distribuido permite un intercambio seguro de información, minimizando la dependencia de terceros y manteniendo un total control por parte del usuario. Asimismo, la implementación de algoritmos

Presentacion y credenciales verificadas correctamente

Dashboard de Presentaciones Verificables

Listado de Presentaciones Verificables

ID	Tipo	Usuario Solicitante	Usuario Vericador	Estado	Token de Certificado	Fecha de Creación
4	Solicitar apoyo movilidad académica	estudiante.1-Dapp	unidadInvestigacion.1-Dapp	ACEPTADA	urn:uuid:f2ae6d5e-84a8-47cb-a7cb-ac226028e0a6	2024-10-08T17:21:54.145866Z

FIGURA 5.22: Aprobación de la presentación verificable por parte del verificador unidadInvestigacion.1-Dapp.
Fuente: Elaboración propia.

criptográficos como Ed25519 para la firma digital y *RSA* para el cifrado de información sensible refuerza la protección de la privacidad del Poseedor, propendiendo por asegurar que la información compartida sea únicamente accesible a los participantes autorizados. La verificación criptográfica de las presentaciones verificables muestra que el modelo es resiliente frente a intentos de manipulación de datos y está alineado con los estándares de interoperabilidad establecidos por la W3C. En resumen, el flujo de información en Aletheia preserva la privacidad del Poseedor y cumple con los principios de identidad autogobernada, evidenciando su capacidad para operar en un entorno seguro y confiable, sin comprometer la autonomía y seguridad de un titular de los derechos de identidad.

Conclusiones

- La identidad digital autogobernada es un esquema de gestión de atributos de identidad personal que responde a las necesidades de gestión de identidad en el contexto digital actual (ver sección 1.1). La adopción de tecnologías como los registros distribuidos y los identificadores descentralizados puede establecer un sistema seguro y confiable que permite a los individuos mantener el control sobre sus atributos de identidad. Este modelo, que garantiza privacidad y autonomía, representa un paso esencial hacia el empoderamiento de los usuarios en un entorno digital cada vez más complejo (ver sección 1.2).
- El análisis de la literatura que fue realizado mostró que la identidad digital autogobernada requiere la adopción de tecnologías basadas en registros distribuidos, arquitecturas descentralizadas, y un enfoque centrado en el usuario para garantizar el control, la seguridad, y la privacidad de los datos (ver sección 2.2.1). Las diversas arquitecturas propuestas tienden a asegurar que el usuario mantenga el control sobre sus datos personales, promoviendo la interoperabilidad y el cumplimiento de normativas regulatorias (ver sección 2.2.2).
- El modelo propuesto Aletheia contribuye al desarrollo de una infraestructura segura y transparente para la gestión de la identidad digital, brindando a los usuarios el control de su privacidad y permitiendo la minimización de la información divulgada. La combinación de tecnologías descentralizadas, como *blockchain* e *IPFS*, y la utilización de mecanismos criptográficos asegura la integridad, confidencialidad y verificabilidad de los datos (ver sección 4.2).
- La arquitectura del modelo propuesto permitió separar la billetera digital del caso de uso específico (ver sección 4.3). Esta característica ha posibilitado, por un lado, el diseño de Aletheia *Wallet* (ver sección 4.2.2) centrado únicamente en la gestión de las credenciales verificables otorgando al modelo un mejor desempeño en los principios de identidad digital referentes a persistencia, protección, acceso, portabilidad e interoperabilidad, y por otra parte, la posibilidad de aplicación o diseño de un caso de uso no dependientes de un determinado *DLT* (ver sección 4.2.3).
- Aletheia no realiza el almacenamiento de información sensible en el dispositivo donde se despliegue la billetera digital, sino que realiza un proceso de persistencia soportado en un sistema de almacenamiento descentralizado como *IPFS*, pero bajo un flujo de información que cifra/-descifra los datos, lo que permite preservar la privacidad del usuario y la existencia de la identidad (ver sección 4.3).
- El proceso de generación y visualización de una VC en Aletheia se caracteriza por su enfoque en la seguridad mediante el uso de criptografía avanzada, la eliminación de intermediarios centralizados y el aprovechamiento de tecnologías descentralizadas. Este modelo asegura que solo los titulares de las credenciales tengan acceso a sus datos, preservando la privacidad y la integridad en todas las etapas del proceso (ver sección 4.3.3).
- Aletheia es funcional para la gestión de una identidad digital autogobernada, preservando la privacidad y la seguridad de los atributos de identidad a lo largo de todo el proceso de interacción entre las entidades. El uso de identificadores descentralizados y credenciales verificables

permite a los usuarios mantener el control total sobre sus datos, mientras que el almacenamiento en *IPFS* y la integración con *blockchain* garantizan la inmutabilidad y trazabilidad de las credenciales emitidas y verificadas. El modelo se compara favorablemente con otros *frameworks* SSI (ver sección 3.10.11), especialmente en términos de portabilidad y persistencia, debido principalmente a la utilización de almacenamiento descentralizado y protocolos de interoperabilidad avanzados como *CHAPI*, lo cual representa una ventaja para aplicaciones de identidad digital a largo plazo y el uso en diversas plataformas (ver sección 5.2).

Trabajo Futuro

Este proyecto de investigación ha permitido fortalecer la línea de trabajo alrededor de *Blockchain* e identidad digital autogobernada en los grupos de investigación: Laboratorio de Investigación y Desarrollo en Electrónica y Redes - LIDER[2] de la Universidad Distrital "Francisco José de Caldas" y en el Laboratorio de Investigación en Sistemas Inteligentes - LISI[3] de la Universidad Nacional de Colombia.

A continuación se proponen las siguientes direcciones para continuar con esta investigación:

- Diseñar e implementar una versión de Aletheia *Wallet* para dispositivos móviles que integre un mecanismo para recuperación social de llaves. Esta actividad se puede realizar a partir del trabajo desarrollado en [293].
- Integrar un modelo de reputación basado en *Blockchain* que permita la descentralización en la creación de los usuarios en Aletheia-Dapp y mitigue el ataque Sybil. Este modelo se podría definir a partir de los resultados que se obtengan de los proyectos en curso planteados en [294], [295].
- Mejorar la seguridad y control de la identidad digital tanto en la *Wallet* como en la Dapp agregando métodos de control biométricos descentralizados. La investigación llevada a cabo en [296] permite la gestión de un perfil biométrico con una DLT.
- Ampliar el caso de estudio sobre la Universidad Distrital "Francisco José de Caldas" con el objeto de tener en el mediano plazo una solución funcional que abarque diferentes aspectos del modelo operativo de la institución, definiendo un conjunto personalizado de esquemas para las credenciales verificables. Este prototipo podría incluir los trabajos previos realizados sobre control de inventario asignado a funcionarios [297], gestión de notas [298], emisión de certificación para grados [299] y evaluación docente [295]. Además, la generación de un contexto de credenciales verificables ajustado a la universidad.
- Preparar la migración del proyecto de *Ganache* [272] a *Hardhat* [300], y así poder realizar la transición de *Ganache*, entorno simulado de una *blockchain* privada tipo *Ethereum*, a un ambiente de desarrollo profesional, más cercano a un contexto real, robusto y personalizable.

[2] https://rita.udistrital.edu.co/lider/
[3] http://www.hermes.unal.edu.co/pages/Consultas/Grupo.xhtml?idGrupo=409&opcion=1

Principales contribuciones

La presente investigación ha desarrollado un modelo de identidad digital descentralizada y autogobernada aplicable a cualquier contexto donde se requiera la administración de atributos de identidad personal, con independencia de una tecnología de registro distribuido o de almacenamiento descentralizado. El modelo propuesto se adhiere a los principios de identidad digital autogobernada, presentando un diseño basado en la privacidad, la persistencia y el control por parte del titular de los derechos de identidad.

Las principales contribuciones de esta investigación son:

- Una conceptualización de la identidad digital centrado en el usuario, fundamentado en identificadores descentralizados y credenciales verificables. Además, se realiza una presentación de las capacidades de la *DLT* para asegurar la privacidad, integridad y seguridad de los datos personales, abordando de manera integral tanto los desafíos tecnológicos como los principios de inclusión y derechos humanos, fundamentales para la implementación de una identidad digital adecuada en la era contemporánea. Estas contribuciones permiten vislumbrar un futuro en el que los individuos tengan total control sobre sus identidades digitales, facilitando la creación de un ecosistema seguro, inclusivo y respetuoso de la privacidad.
- Se resalta la aplicación de un enfoque metodológico, reproducible y automatizado para la revisión sistemática de la literatura. Esta metodología aporta un análisis bibliométrico riguroso (por ejemplo: [58], [59], [220]) que promueve la selección objetiva de las fuentes y publicaciones de mayor relevancia en un área de investigación. La aplicación de este método de análisis y selección de publicaciones, permitió identificar los atributos y requerimientos de información para el diseño de una aplicación SSI (ver sección 2.2.1), además de establecer la complejidad y diversidad del panorama actual en la gestión de identidades digitales autogobernadas, subrayando la necesidad de establecer estándares claros que faciliten la interoperabilidad y la seguridad en la gestión de los atributos de identidad.
- El Capítulo 2 introduce un marco de evaluación para *frameworks* de identidad digital autogobernada, basado en el nivel de adherencia a los principios de SSI (ver sección 2.2.1.2). Este marco ofrece un mecanismo para evaluar y comparar diversas soluciones de SSI, lo cual es fundamental para determinar su capacidad de garantizar la soberanía del usuario, la seguridad y la interoperabilidad de las identidades. Además, su aplicación permite identificar fortalezas y debilidades en los *frameworks*, orientando así la toma de decisiones para la implementación de soluciones de identidad que aseguren la protección de datos. La aplicación de este marco ha generado uno de los análisis comparativos más completos hasta la fecha sobre *frameworks* de SSI (ver artículo [2] y sección 3.10).
- Diseño de una arquitectura modular para la identidad digital autogobernada, alineada principalmente con los principios de control, privacidad y minimización de datos. Aletheia no solo integra tecnologías emergentes para asegurar la autenticidad de las credenciales digitales, sino que también involucra un marco de gobernanza que refuerza la confianza entre las partes involucradas. Este modelo aporta una solución novedosa y aplicable para la gestión de la identidad

digital, promoviendo la interoperabilidad y el control individual sobre la información personal (ver sección 4.3).

- La implementación del caso de prueba facilitó la comprensión y concreción de la abstracción del modelo planteado. Además de permitir su validación experimental en un entorno simulado, el código fuente desarrollado constituye un valioso aporte que puede ser usado como una base importante para la implementación del modelo Aletheia en otros escenarios que permitan seguir validando las bondades del modelo propuesto (ver sección 5.3).

5.5 Socialización de resultados

A lo largo del desarrollo de esta investigación, se han realizado diversas publicaciones en distintos ámbitos de divulgación científica. En primer lugar, es importante destacar que este proceso ha generado una serie de productos, que se clasifican en ponencias en congresos internacionales, artículos, una estancia de pasantia, un proyecto de investigación registrado en la oficina de investigaciones de la universidad Distrital, trabajos de grado tanto de maestría como de pregrado, y la participación como ponente en el tour *blockchain* en Colombia.

5.5.1 Ponencias en congresos internacionales

1. VII Congreso Internacional de Ingeniería CIIUDEC-2018. **"*Blockchain* Perspectiva y Futuro"**. Octubre 18 y 19 de 2018, Universidad de Cundinamarca, Bogotá D.C, Colombia.

2. II Convención Científica Internacional UCLV 2019. **"Perspectiva de un cuidado integral de la salud soportado en *Blockchain* e *IoT*".** Junio 23 al 30 de 2019, Universidad Central de las Villas, Santa Clara, Cuba.

3. IV Congreso Internacional Avances de Investigación en Ingeniería 2022. **"Evaluación de *Frameworks* para identidad digital auto-soberana"**. Octubre 18 al 21 de 2022, Universidad Ecci, Bogotá D.C, Colombia.

4. I Conferencia Internacional de Innovación e Investigación. **"Modelo de almacenamiento cifrado y descentralizado basado en identidad digital autogobernada integrando *blockchain* e *IPFS*"**. Noviembre 2 y 3 de 2023, Universidad Militar Nueva Granada, Cajicá, Bogotá D.C, Colombia.

5. 2nd International Symposium on "Generation and Transfer of Knowledge for Digital Transformation" SITIC2023. **IoT and Blockchain applied to the food supply chain: A systematic literature review.** Noviembre del 13 al 17 de 2023, Universidad Central de las Villas, Santa Clara, Cuba.

6. 2nd International Symposium on "Generation and Transfer of Knowledge for Digital Transformation" SITIC2023. **"Platform to preserve and verify documents applying self-sovereign identity supported on blockchain: case study requirements to obtain an academic certification."** Noviembre del 13 al 17 de 2023, Universidad Central de las Villas, Santa Clara, Cuba.

5.5.2 Artículos realizados

1. R. A. Pava-Díaz, J. N. Perez Castillo, y L. F. Niño-Vasquez, **"Perspectiva para el uso del modelo P6 de atención en salud bajo un escenario soportado en IoT y *blockchain*"**, Tecnura, vol. 25, n.º 67, pp. 112–130, ene. 2021 [301].

2. R. A. Pava-Díaz, D. A. López-Sarmiento, L. F. Niño-Vasquez, y R.V Paez-Méndez, **"Tecnología de registro distribuido (DLT): Características y escenarios de aplicación: Blockchain, DLT, DLT-DAG, Tecnología de registro distribuido"**, Tecnol. Investig. Academia, vol. 9, n.º 1, pp. 74–90, feb. 2022 [302].

3. R. A. Pava-Díaz, R. V. Paez-Mendez, and L. F. Niño-Vasquez, **"*A Bibliometric Study of Scientific Production on Self-Sovereign Identity*"**, Ingeniería, vol. 28, no. Suppl, p. e19656, Feb. 2023 [59].

4. R. A. Pava-Díaz, Gómez-Almeyda Santiago, Hernández-Suarez Cesar A. **"Veridoc-Chain: un modelo de identidad digital autogobernada basado en *blockchain* para una gestión de credenciales académicas segura y privada."**. Revista Cubana de Ciencias Informáticas. vol. 18. No 2. 2024. [303].

5. R. A. Pava-Díaz, J. Gil-Ruiz y D. A. López-Sarmiento, **"*Self-sovereign identity on the blockchain: contextual analysis and quantification of SSI principles implementation*"**, Frontiers in Blockchain, vol. 7, 2024 [2].

5.5.3 Estancia de pasantia

La estancia de pasantia realizada en la Pontificia Universidad Javeriana, sede Bogotá D.C., dentro del grupo de investigación SIDRe (Sistemas de Información, Sistemas Distribuidos y Redes de Computadores), bajo la dirección del Ing. Rafael Vicente Páez Méndez, Ph.D., no solo fortaleció los vínculos de colaboración interinstitucional, sino que también facilitó el intercambio de conocimientos y experiencias en el área de investigación. Durante esta pasantia, el análisis sobre la identidad digital permitió identificar los atributos y requisitos esenciales para la definición de una identidad autogobernada. Esta colaboración se ve reflejada en las publicaciones [302] y [59].

5.5.3.1 Proyecto de investigación institucionalizado

El proyecto de investigación titulado "Modelo para la gestión de una identidad digital descentralizada y autogobernada bajo tecnología de registro distribuido" fue registrado en el Sistema de Información de Investigaciones de la Universidad Distrital "Francisco José de Caldas", con el código asignado 3 370 072 920. Este proyecto facilitó la organización de la generación de productos de investigación y la dirección de trabajos de grado, los cuales se detallan en las Tablas 5.6 y 5.7.

5.5.4 Trabajos de grado dirigidos

Durante el desarrollo de esta investigación, el proyecto fue registrado en la Oficina de Investigaciones de la Universidad Distrital "Francisco José de Caldas" con el código interno 3370072920. En el marco de este proyecto, se plantearon diversos trabajos de grado de estudiantes de pregrado y maestría que contribuyeron al desarrollo de la línea de investigación. La Tabla 5.6 presenta los trabajos de maestría, mientras que la Tabla 5.7 muestra los correspondientes a pregrado.

Código	Estudiante	Título del Proyecto
20212495007	Sandoval Mesa Nidia Helena	Modelo de Gestión para Control y Trazabilidad de la Cadena de Suministros de Medicamentos en el Sistema de Salud a Través de Tecnología *Blockchain*.
20182495003	Avendaño Abril Johon Fredy	Modelo para la Administración de Recursos Logísticos de Alimentos Soportado en *Blockchain* y IoT - Programa PAE.
20182495017	Castellanos Hernández Omar Ricardo	Modelo de Administración de Datos Personales Orientado al Propietario de los Datos Usando *Blockchain* en Colombia.
20181195014	Diego Fernando Zapata Muñoz	Modelo de reputación basado en *blockchain* e identidad digital autogobernada aplicado al proceso de evaluación docente.

Tabla 5.6: Trabajos de grado dirigidos a nivel de Maestría

Código	Estudiante	Título del Proyecto
20092020106	Daniel Ricardo Galván Torres	Prototipo de una aplicación descentralizada de apoyo a los procedimientos de gestión de inventarios de la Universidad Distrital usando *Blockchain* e *IPFS*.
20161020503	Santiago Gómez Almeyda	Sistema *Blockchain* para verificación automática de requisitos de grado en la Universidad Distrital.
20171005039 20171005056	Juan Castañeda Santiago Peña	Gestión de llaves criptográficas orientado a un respaldo seguro y su recuperación en redes distribuidas.
20151005057 20151005080	Diego Garzón Estefania Barrios	Diseño de un módulo para autenticación usando datos biométricos en un entorno descentralizado.
20171005098	Miguel Ángel Leguizamo Muñoz	Diseño e Implementación de un Nuevo Método para Mitigación de Ataque Sybil.

Tabla 5.7: Trabajos de grado dirigidos a nivel de Pregrado

5.5.5 Conferencista/Panelista invitado

- Ponencia: "Algoritmos y tecnología detrás de las criptomonedas". Tour Universitario: *Blockchain*, El Internet del Valor. Universidad Nacional de Colombia, Bogotá D.C. 5 de Noviembre de 2019. Organizado por Red de Universidades por las TIC (UxTIC) y Red Universitaria Metropolitana de Bogotá (Rumbo).
- Ponencia: "*Blockchain*: Perspectiva y Futuro". Tour Universitario: *Blockchain*, El Internet del Valor. Universidad Nacional de Colombia, Bogotá D.C. 20 de Noviembre de 2019. Organizado por Red de Universidades por las TIC (UxTIC) y Red Universitaria Metropolitana de Bogotá (Rumbo).
- Invitado como panelista al debate académico internacional. "*Blockchain*, identidad digital y custodia de datos". Modalidad virtual. 18 de Julio de 2023. Organizado por Red de Universidades por las TIC (UxTIC), coinEx, Fodesep, Obreal Global, Asociación Red universitaria de alta velocidad del Valle del Cauca (Ruav) y Open LMS.

Bibliografía

[1] N. Naik y P. Jenkins, "Does Sovrin Network Offer Sovereign Identity?", en *ISSE - IEEE Int. Symp. Syst. Eng., Proc.*, Institute of Electrical y Electronics Engineers Inc., 2021, ISBN: 9781665431682. DOI: 10.1109/ISSE51541.2021.9582472.

[2] R. Pava-Díaz, J. Gil-Ruiz y D. López-Sarmiento, "Self-sovereign identity on the blockchain: contextual analysis and quantification of SSI principles implementation", *Frontiers in Blockchain*, vol. 7, 2024, ISSN: 2624-7852. DOI: 10.3389/fbloc.2024.1443362. dirección: https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2024.1443362.

[3] F. Wang y P. De Filippi, "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion", *Front. Blockchain*, vol. 2, n.º January, págs. 1-22, 2020. DOI: 10.3389/fbloc.2019.00028.

[4] Q. Stokkink, G. Ishmaev, D. Epema y J. Pouwelse, "A Truly Self-Sovereign Identity System", en *LCN 2021*, 2021, págs. 1-8. DOI: 10.1109/LCN52139.2021.9525011.

[5] Homeland Security, *Real ID Act*, 2022. visitado 6 de mayo de 2022. dirección: https://www.dhs.gov/real-id.

[6] Y. A. De Montjoye, E. Shmueli, S. S. Wang y A. S. Pentland, "OpenPDS: Protecting the privacy of metadata through SafeAnswers", *PLoS One*, vol. 9, n.º 7, pág. 9, 2014, ISSN: 19326203. DOI: 10.1371/journal.pone.0098790.

[7] Identity2020 Systems, *We need to get digital ID right*, 2019. visitado 3 de abr. de 2022. dirección: https://id2020.org/.

[8] Identity2020 Systems, *ID2020 Alliance Manifesto*, 2020. visitado 6 de mayo de 2022. dirección: https://id2020.org/manifesto.

[9] T. Lyons, L. Courcelas y K. Timsit, "Blockchain and digital identity", The european union blockchain observatory y forum, 2019. visitado 10 de ene. de 2019. dirección: https://www.eublockchainforum.eu/reports/blockchain-and-digital-identity.

[10] P. J. Windley, "Sovrin: An Identity Metasystem for Self-Sovereign Identity", *Front. Blockchain*, vol. 4, 2021, ISSN: 2624-7852. DOI: 10.3389/fbloc.2021.626726.

[11] Y. Li, A. Yazdanmehr, J. Wang y H. R. Rao, "Responding to identity theft: A victimization perspective", *Decision Support Systems*, vol. 121, págs. 13-24, 2019, ISSN: 01679236. DOI: 10.1016/j.dss.2019.04.002.

[12] P. Dunphy y F. A. Petitcolas, "A first look at identity management schemes on the blockchain", *IEEE Secur. Priv.*, vol. 16, n.º 4, págs. 20-29, 2018, ISSN: 1558-4046. DOI: 10.1109/MSP.2018.3111247.

[13] Identity Foundation, *DIF - Decentralized Identity Foundation*, 2020. visitado 28 de abr. de 2020. dirección: https://identity.foundation/.

[14] O. J. Gstrein y D. Kochenov, "Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World?", *Front. Blockchain*, vol. 3, n.º March, págs. 1-8, 2020. DOI: 10.3389/fbloc.2020.00010.

[15] J. Bernal Bernabe, J. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno y A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges", *IEEE Access*, vol. 7, págs. 164 908-164 940, 2019. DOI: 10.1109/ACCESS.2019.2950872.

[16] Asamblea general de las Naciones Unidas, *Transformar nuestro mundo: La Agenda 2030 para el Desarrollo Sostenible*, 2015. visitado 5 de mayo de 2020. dirección: https://www.unfpa.org/sites/default/files/resource-pdf/Resolution_A_RES_70_1_SP.pdf.

[17] M. A. Sicilia y A. Visvizi, "Blockchain and OECD data repositories: opportunities and policymaking implications", *Libr. Hi Tech*, vol. 37, n.º 1, págs. 30-42, 2019, ISSN: 07378831. DOI: 10.1108/LHT-12-2017-0276.

[18] Kiva, *Kiva Protocol - Building the credit bureau of the future*, 2020. visitado 28 de abr. de 2020. dirección: https://www.kiva.org/protocol.

[19] G. Kondova y J. Erbguth, ""Self-Sovereign Identity on Public Blockchains and the GDPR"", en *SAC '20*, ép. SAC '20, Brno, Czech Republic: Association for Computing Machinery, 2020, págs. 342-345, ISBN: 9781450368667. DOI: 10.1145/3341105.3374066.

[20] J. Benet, *IPFS - Content Addressed, Versioned, P2P File System*, 2014. visitado 16 de mayo de 2022. dirección: https://arxiv.org/abs/1407.3561.

[21] Q. Xu, Z. Song, R. S. Mong Goh e Y. Li, "Building an Ethereum and IPFS-Based Decentralized Social Network System", en *ICPADS 2018*, 2018, págs. 1-6. DOI: 10.1109/PADSW.2018.8645058.

[22] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad y M. H. Rehman, "Decentralized document version control using ethereum blockchain and IPFS", *Comput. Electr. Eng.*, vol. 76, págs. 183-197, 2019, ISSN: 00457906. DOI: 10.1016/j.compeleceng.2019.03.014.

[23] M. Yu, S. Sahraei, S. Li, S. Avestimehr, S. Kannan y P. Viswanath, "Coded Merkle Tree: Solving Data Availability Attacks in Blockchains", en *FC 2020 Revised Selected Papers*, Berlin, Heidelberg: Springer-Verlag, 2020, págs. 114-134, ISBN: 978-3-030-51279-8. DOI: 10.1007/978-3-030-51280-4_8.

[24] R. K. Raman y L. R. Varshney, "Distributed Storage Meets Secret Sharing on the Blockchain", en *ITA 2018*, feb. de 2018, págs. 1-6, ISBN: 9781728101248. DOI: 10.1109/ITA.2018.8503089.

[25] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat y L. Njilla, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability", en *CCGRID 2017*, 2017, págs. 468-477, ISBN: 9781509066100. DOI: 10.1109/CCGRID.2017.8.

[26] F. Casino, T. K. Dasaklis y C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues", *Telematics and Informatics*, vol. 36, págs. 55-81, 2019, ISSN: 0736-5853. DOI: 10.1016/j.tele.2018.11.006.

[27] T. Lyons, L. Courcelas y K. Timsit, "Blockchain and the GDPR", The European Union Blockchain: Observatory y Forum, 2018. visitado 14 de jul. de 2019. dirección: https://www.eublockchainforum.eu/reports/blockchain-and-gdpr.

[28] T. McGhin, K. K. R. Choo, C. Z. Liu y D. He, "Blockchain in healthcare applications: Research challenges and opportunities", *J. Netw. Comput. Appl.*, vol. 135, n.º January, págs. 62-75, 2019, ISSN: 10958592. DOI: 10.1016/j.jnca.2019.02.027.

[29] X. Li, X. Wu, X. Pei y Z. Yao, "Tokenization: Open Asset Protocol on Blockchain", en *ICICT 2019*, IEEE, 2019, págs. 204-209, ISBN: 9781728133232. DOI: 10.1109/INFOCT.2019.8711021.

[30] N. Diallo et al., "eGov-DAO: a Better Government using Blockchain based Decentralized Autonomous Organization", en *ICEDEG 2018*, IEEE, 2018, págs. 166-171, ISBN: 9781538625194. DOI: 10.1109/ICEDEG.2018.8372356.

[31] R. Soltani, U. Nguyen y A. An, "A Survey of Self-Sovereign Identity Ecosystem", *Secur. Commun. Netw.*, vol. 2021, 2021. DOI: 10.1155/2021/8873429.

[32] G. Ishmaev, "Sovereignty, privacy, and ethics in blockchain-based identity management systems", *Ethics. Inf. Technol.*, vol. 23, n.º 3, págs. 239-252, 2021, ISSN: 13881957. DOI: 10.1007/s10676-020-09563-x.

[33] M. Lockwood, "Exploring Value Propositions to Drive Self-Sovereign Identity Adoption", *Front. Blockchain*, vol. 4, 2021, ISSN: 2624-7852. DOI: 10.3389/fbloc.2021.611945.

[34] S. Haataja, "The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach", *Law, Innovation and Technol.*, vol. 9, n.º 2, págs. 159-189, 2017, ISSN: 1757997X. DOI: 10.1080/17579961.2017.1377914.

[35] J. Priisalu y R. Ottis, "Personal control of privacy and data: Estonian experience", *Health Technol.*, vol. 7, n.º 4, págs. 441-451, 2017, ISSN: 21907196. DOI: 10.1007/s12553-017-0195-1.

[36] N. Naik y P. Jenkins, "Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity", en *Proc. IEEE Int. Conf. Behav. Soc. Comput., BESC*, Institute of Electrical y Electronics Engineers Inc., 2020, ISBN: 9781728186054. DOI: 10.1109/BESC51023.2020.9348298.

[37] R. Nokhbeh Zaeem y K. S. Barber, "How Much Identity Management with Blockchain Would Have Saved Us? A Longitudinal Study of Identity Theft", en *LNBIP 394*, 2020, págs. 158-168. DOI: 10.1007/978-3-030-61146-0_13.

[38] G. Chapron, "The environment needs cryptogovernance", *Nature*, vol. 545, n.º 7655, págs. 403-405, 2017, ISSN: 14764687. DOI: 10.1038/545403a.

[39] R. Klitgaard, *Controlando la corrupción: Una indagación práctica para el gran problema social de fin de siglo*. Sudamericana, 1988, pág. 227, ISBN: 9789500709460.

[40] OECD, *Bribery in Public Procurement: Methods, Actors and Counter-Measures*. The Organisation for Economic Co-operation y Development, 2007, vol. 9789264013, pág. 103, ISBN: 9789264013964. DOI: 10.1787/9789264013964-en. dirección: https://www.oecd.org/daf/anti-bribery/anti-briberyconvention/44956834.pdf.

[41] P. Fraga-Lamas y T. Fernández-Caramés, "Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality", *IT Professional*, vol. 22, n.º 2, págs. 53-59, 2020. DOI: 10.1109/MITP.2020.2977589.

[42] N. O. Nawari y S. Ravindran, "Blockchain technology and BIM process: Review and potential applications", *ITcon*, vol. 24, n.º May, págs. 209-238, 2019, ISSN: 18744753.

[43] M. E. Peck, "Blockchains: How they work and why they'll change the world", *IEEE Spectrum*, vol. 54, n.º 10, págs. 26-35, oct. de 2017, ISSN: 0018-9235. DOI: 10.1109/MSPEC.2017.8048836.

[44] H. Heng, "The Application of Blockchain Technology in E-Government in China", en *ICCCN) 2017*, jul. de 2017, págs. 1-4. DOI: 10.1109/ICCCN.2017.8038519.

[45] Y. Kurihara, "Self-Sovereign Identity and Blockchain-Based Content Management", en *HCC 2020*, vol. IFIP AICT 590, 2020, págs. 130-140, ISBN: 978-3-030-62802-4. DOI: 10.1007/978-3-030-62803-11.

[46] S. Manski, "Distributed Ledger Technologies, Value Accounting, and the Self Sovereign Identity", *Front. Blockchain*, vol. 3, 2020, ISSN: 2624-7852. DOI: 10.3389/fbloc.2020.00029.

[47] G. Golan Gueta et al., "SBFT: A Scalable and Decentralized Trust Infrastructure", en *DSN 2019*, IEEE, 2019, págs. 568-580, ISBN: 9781728100562. DOI: 10.1109/DSN.2019.00063. eprint: 1804.01626.

[48] T. Hardjono y N. Smith, "Decentralized Trusted Computing Base for Blockchain Infrastructure Security", *Front. Blockchain*, vol. 2, n.º i, págs. 1-27, 2019. DOI: 10.3389/fbloc.2019.00024.

[49] A. Mühle, A. Grüner, T. Gayvoronskaya y C. Meinel, "A survey on essential components of a self-sovereign identity", *Comput. Sci. Rev.*, vol. 30, págs. 80-86, 2018, ISSN: 15740137. DOI: 10.1016/j.cosrev.2018.10.002.

[50] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008. visitado 20 de mayo de 2022. dirección: http://bitcoin.org/bitcoin.pdf.

[51] A. M. Makarov, A. O. Golyakova, I. D. Osinin y S. S. Postovalov, "Fundamental Design of Blockchain – Hashchain Networks with a Decentralized Register Based on Cryptography Methods", en *ICT 2017*, Springer, 2017, págs. 620-629. DOI: 10.1007/978-3-319-90835-9_72.

[52] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey y S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review", *Inf. Softw. Technol.*, vol. 51, n.º 1, págs. 7-15, 2009. DOI: https://doi.org/10.1016/j.infsof.2008.09.009.

[53] V. Garousi, M. Felderer y M. V. Mäntylä, ""The Need for Multivocal Literature Reviews in Software Engineering: Complementing Systematic Literature Reviews with Grey Literature"", en *EASE '16*, ép. EASE '16, Limerick, Ireland: Association for Computing Machinery, 2016, ISBN: 9781450336918. DOI: 10.1145/2915970.2916008.

[54] R Core Team, *R: A Language and Environment for Statistical Computing*, R Foundation for Statistical Computing, 2020. visitado 2 de ene. de 2022. dirección: https://www.R-project.org/.

[55] M. Aria y C. Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis", *J. Informetr.*, vol. 11, n.º 4, págs. 959-975, 2017. DOI: 10.1016/j.joi.2017.08.007.

[56] Clarivate Analytics, *Web of Science*, 2022. visitado 3 de ene. de 2022. dirección: https://access.clarivate.com/login?app=wos.

[57] Elsevier, *Scopus*, 2022. visitado 1 de feb. de 2022. dirección: https://www.elsevier.com/solutions/scopus.

[58] R. Pava-Díaz, R. Paez-Méndez, L. Niño-Vasquez y D. Lopez, *Preprocesamiento de publicaciones acerca de indentidad digital descentralizada y autgobernada*, 2022. visitado 12 de abr. de 2022. dirección: https://doi.org/10.6084/m9.figshare.19579492.

[59] R. Pava-Díaz, R. Paez-Méndez y L. Niño-Vasquez, "A Bibliometric Study of Scientific Production on Self-Sovereign Identity", *Ing.*, vol. 28, n.º Suppl, feb. de 2023. DOI: 10.14483/23448393.19656.

[60] F. Wang y P. De Filippi, "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion", *Front. Blockchain*, vol. 2, 2020, ISSN: 2624-7852. DOI: 10.3389/fbloc.2019.00028.

[61] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez y K. Dahal, "DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network", *Appl. Sci.*, vol. 9, n.º 15, 2019, ISSN: 2076-3417. DOI: 10.3390/app9152953.

[62] S. E. Haddouti y M. D. Ech-Cherif El Kettani, "Analysis of Identity Management Systems Using Blockchain Technology", en *CommNet 2019*, vol. 10, 2019, págs. 1-7. DOI: 10.1109/COMMNET.2019.8742375.

[63] X. Zhu e Y. Badr, "A Survey on Blockchain-Based Identity Management Systems for the Internet of Things", en *iThings/ GreenCom/ CPSCom/ SmartData/ Blockchain/ CIT 2018*, 2018, págs. 1568-1573. DOI: 10.1109/Cybermatics_2018.2018.00263.

[64] K. Bendiab, N. Kolokotronis, S. Shiaeles y S. Boucherkha, "WiP: A Novel Blockchain-Based Trust Model for Cloud Identity Management", en *DASC- PICom- DataCom- CyberSciTec 2018*, IEEE, 2018, págs. 724-729. DOI: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00126.

[65] M. Kuperberg, "Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective", *IEEE T. Eng. Manage.*, vol. 67, n.º 4, págs. 1008-1027, 2020. DOI: 10.1109/TEM.2019.2926471.

[66] A. Othman y J. Callahan, "The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity", en *IJCNN 2018*, 2018, págs. 1-7. DOI: 10.1109/IJCNN.2018.8489316.

[67] M. S. Ferdous, F. Chowdhury y M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology", *IEEE Access*, vol. 7, págs. 103 059-103 079, 2019. DOI: 10.1109/ACCESS.2019.2931173.

[68] Z. Gao et al., "Blockchain-Based Identity Management with Mobile Device", en *CryBlock '18*, ép. CryBlock'18, Munich, Germany: Association for Computing Machinery, 2018, págs. 66-70, ISBN: 9781450358385. DOI: 10.1145/3211933.3211945.

[69] B. Faber, G. Michelet, N. Weidmann, R. Mukkamala y R. Vatrapu, ""BPDIMS:A blockchain-based personal data and identity management system"", en *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, B. T.X., ed., vol. 2019-January, IEEE Computer Society, 2019, págs. 6855-6864, ISBN: 9780998133126. DOI: 10.24251/HICSS.2019.821.

[70] C. Lin, D. He, X. Huang, M. Khurram Khan y K.-K. R. Choo, "A New Transitively Closed Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems", *IEEE Access*, vol. 6, 2018. DOI: 10.1109/ACCESS.2018.2837650.

[71] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan y K.-K. R. Choo, "Blockchain-based identity management systems: A review", *J. Netw. Comput. Appl.*, vol. 166, 2020. DOI: 10.1016/j.jnca.2020.102731.

[72] Q. Stokkink y J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity", en *iThings/ GreenCom/ CPSCom/ SmartData/ Blockchain/ CIT 2018*, 2018, págs. 1336-1342. DOI: 10.1109/Cybermatics_2018.2018.00230.

[73] N. Naik y P. Jenkins, "Sovrin Network for Decentralized Digital Identity: Analysing a Self-Sovereign Identity System Based on Distributed Ledger Technology", en *ISSE - IEEE Int. Symp. Syst. Eng., Proc.*, Institute of Electrical y Electronics Engineers Inc., 2021, ISBN: 9781665431682. DOI: 10.1109/ISSE51541.2021.9582551.

[74] N. Naik, P. Grace y P. Jenkins, "An Attack Tree Based Risk Analysis Method for Investigating Attacks and Facilitating Their Mitigations in Self-Sovereign Identity", en *IEEE Symp. Ser. Comput. Intell., SSCI - Proc.*, Institute of Electrical y Electronics Engineers Inc., 2021, ISBN: 9781728190488. DOI: 10.1109/SSCI50451.2021.9659929.

[75] N. Naik y P. Jenkins, "UPort Open-Source Identity Management System: An Assessment of Self-Sovereign Identity and User-Centric Data Platform Built on Blockchain", en *ISSE - IEEE Int. Symp. Syst. Eng., Proc.*, Institute of Electrical y Electronics Engineers Inc., 2020, ISBN: 9781728186023. DOI: 10.1109/ISSE49799.2020.9272223.

[76] N. Naik y P. Jenkins, "Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems", en *ISSE - IEEE Int. Symp. Syst. Eng., Proc.*, Institute of Electrical y Electronics Engineers Inc., 2020, ISBN: 9781728186023. DOI: 10.1109/ISSE49799.2020.9272212.

[77] N. Naik y P. Jenkins, "Self-Sovereign Identity Specifications: Govern Your Identity through Your Digital Wallet using Blockchain Technology", en *Proc. - IEEE Int. Conf. Mob. Cloud Comput., Serv., Eng., MobileCloud*, Institute of Electrical y Electronics Engineers Inc., 2020, págs. 90-95, ISBN: 9781728110356. DOI: 10.1109/MobileCloud48802.2020.00021.

[78] Y. Liu, Q. Lu, C. Zhu y Q. Yu, "A blockchain-based platform architecture for multimedia data management", *Multimedia Tools Appl.*, vol. 80, n.º 20, 2021, ISSN: 13807501. DOI: 10.1007/s11042-021-10558-z.

[79] Y. Liu, Q. Lu, H.-Y. Paik y X. Xu, "Design Patterns for Blockchain-based Self-Sovereign Identity", en *ACM Int. Conf. Proc. Ser.*, Association for Computing Machinery, 2020, ISBN: 9781450377690. DOI: 10.1145/3424771.3424802.

[80] Y. Liu, Q. Lu, H. .-. Paik, X. Xu, S. Chen y L. Zhu, "Design Pattern as a Service for Blockchain-Based Self-Sovereign Identity", *IEEE Software*, vol. 37, págs. 30-36, 2020. DOI: 10.1109/MS.2020.2992783.

[81] M. A. Bouras, Q. Lu, S. Dhelim y H. Ning, "A Lightweight Blockchain-Based IoT Identity Management Approach", *Future Internet*, vol. 13, n.º 2, 2021, ISSN: 1999-5903. DOI: 10.3390/fi13020024.

[82] R. Soltani, U. Nguyen y A. An, "Decentralized and privacy-preserving key management model", en *Int. Symp. Networks, Comput. Commun., ISNCC*, Institute of Electrical y Electronics Engineers Inc., 2020, ISBN: 9781728156286. DOI: 10.1109/ISNCC49221.2020.9297294.

[83] R. Soltani, U. Nguyen y A. An, "Practical key recovery model for self-sovereign identity based digital wallets", en *DASC-PICom- CBDCom- CyberSciTech 2019*, Institute of Electrical y Electronics Engineers Inc., 2019, págs. 320-325, ISBN: 9781728130248. DOI: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066.

[84] R. Soltani, U. Nguyen y A. An, "A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger", en *iThings/ GreenCom/ CPSCom/ SmartData/ Blockchain/ CIT 2018*, Institute of Electrical y Electronics Engineers Inc., 2018, págs. 1129-1136, ISBN: 9781538679753. DOI: 10.1109/Cybermatics_2018.2018.00205.

[85] E. Bandara, X. Liang, P. Foytik, S. Shetty y K. D. Zoysa, "A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform", en *ICCCN 2021*, IEEE, 2021, págs. 1-7. DOI: 10.1109/ICCCN52240.2021.9522184.

[86] E. Bandara, X. Liang, P. Foytik y S. Shetty, "Blockchain and Self-Sovereign Identity Empowered Cyber Threat Information Sharing Platform", en *Smartcomp 2021*, IEEE, 2021, págs. 258-263. DOI: 10.1109/SMARTCOMP52413.2021.00057.

[87] E. Bandara et al., "Connect - Blockchain and Self-Sovereign Identity Empowered Contact Tracing Platform", en *MobiHealth 2020*, vol. 362, Springer International Publishing, 2021, págs. 208-223, ISBN: 9783030705688. DOI: 10.1007/978-3-030-70569-5_13.

[88] A. Grüner, A. Mühle y C. Meinel, "ATIB: Design and Evaluation of an Architecture for Brokered Self-Sovereign Identity Integration and Trust-Enhancing Attribute Aggregation for Service Provider", *IEEE Access*, vol. 9, 2021, ISSN: 21693536. DOI: 10.1109/ACCESS.2021.3116095.

[89] K. Schmidt, A. Muhle, A. Gruner y C. Meinel, "Clear the Fog: Towards a Taxonomy of Self-Sovereign Identity Ecosystem Members", en *Int. Conf. Priv., Secur. Trust, PST*, Institute of Electrical y Electronics Engineers Inc., 2021, ISBN: 9781665401845. DOI: 10.1109/PST52912.2021.9647797.

[90] A. Gruner, A. Muhle y C. Meinel, "An Integration Architecture to Enable Service Providers for Self-sovereign Identity", en *IEEE Int. Symp. Netw. Comput. Appl., NCA*, Institute of Electrical y Electronics Engineers Inc., 2019, ISBN: 9781728125220. DOI: 10.1109/NCA.2019.8935015.

[91] A. Gruner, A. Muhle, T. Gayvoronskaya y C. Meinel, "A quantifiable trust model for blockchain-based identity management", en *iThings/ GreenCom/ CPSCom/ SmartData/ Blockchain/ CIT 201*, Institute of Electrical y Electronics Engineers Inc., 2018, págs. 1475-1482, ISBN: 9781538679753. DOI: 10.1109/Cybermatics_2018.2018.00250.

[92] A.-E. Panait, "Is the user identity perception influenced by the blockchain technology?", en *Proc. - IEEE Int. Conf. Intell. Secur. Inf., ISI*, Institute of Electrical y Electronics Engineers Inc., 2020, ISBN: 9781728188003. DOI: 10.1109/ISI49825.2020.9280530.

[93] A.-E. Panait, R. Olimid y A. Stefanescu, "Analysis of uPort Open, an Identity Management Blockchain-Based Solution", *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12395 LNCS, págs. 3-13, 2020, ISSN: 03029743. DOI: 10.1007/978-3-030-58986-8_1.

[94] A. Abraham, S. More, C. Rabensteiner y F. Hörandner, "Revocable and Offline-Verifiable Self-Sovereign Identities", en *TrustCom 2020*, 2020, págs. 1020-1027. DOI: 10.1109/TrustCom50675.2020.00136.

[95] A. Abraham, K. Koch, S. More, S. Ramacher y M. Stopar, "Privacy-Preserving eID Derivation to Self-Sovereign Identity Systems with Offline Revocation", en *TrustCom 2021*, oct. de 2021, págs. 506-513. DOI: 10.1109/TrustCom53373.2021.00080.

[96] D. Kirupanithi y A. Antonidoss, "Self-sovereign identity creation on blockchain using identity based encryption", en *Proc. - Int. Conf. Intell. Comput. Control Syst., ICICCS*, 2021, págs. 299-304, ISBN: 9781665412728. DOI: 10.1109/ICICCS51141.2021.9432099.

[97] N. Kirupanithi y A. Antonidoss, "Hierarchical Deterministic protocol for the defragmentation of identity in a blockchain-based framework", en *Proc. Int. Conf. I-SMAC (IoT Soc., Mob., Anal. Cloud), I-SMAC*, 2021, págs. 1497-1504, ISBN: 9781665426428. DOI: 10.1109/I-SMAC52330.2021.9640809.

[98] D. Kirupanithi y A. Antonidoss, "Self-Sovereign Identity Management System on blockchain based applications using Chameleon Hash", en *Proc. - Int. Conf. Smart Electron. Commun., ICOSEC*, Institute of Electrical y Electronics Engineers Inc., 2021, págs. 386-390, ISBN: 9781665433686. DOI: 10.1109/ICOSEC51865.2021.9591734.

[99] M. Alharbi y F. K. Hussain, "Blockchain-Based Identity Management for Personal Data: A Survey", en *LNNS, 346*, L. Barolli, ed., vol. 346 LNNS, Cham: Springer International Publishing, 2022, págs. 167-178, ISBN: 978-3-030-90072-4. DOI: 10.1007/978-3-030-90072-4_17.

[100] J. Kaneriya y H. Patel, "A comparative survey on blockchain based self sovereign identity system", en *Proc. Int. Conf. Intell. Sustain. Syst., ICISS*, 2020, págs. 1150-1155, ISBN: 9781728170893. DOI: 10.1109/ICISS49785.2020.9315899.

[101] K. Gilani, E. Bertin, J. Hatin y N. Crespi, "A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data", en *Conf. Blockchain Res. Appl. Innov. Networks Serv., BRAINS*, 2020, págs. 97-101, ISBN: 9781728170916. DOI: 10.1109/BRAINS49436.2020.9223312.

[102] A. Satybaldy, M. Nowostawski y J. Ellingsen, "Self-sovereign identity systems: Evaluation framework", en *IFIP 2020*, vol. 576 LNCS, 2020, págs. 447-461. DOI: 10.1007/978-3-030-42504-3_28.

[103] B. N. Eddine, A. Ouaddah y A. Mezrioui, "Exploring blockchain-based Self Sovereign Identity Systems: Challenges and comparative analysis", en *BRAINS 2021*, 2021, págs. 21-22. DOI: 10.1109/BRAINS52497.2021.9569821.

[104] Š. Čučko y M. Turkanović, "Decentralized and Self-Sovereign Identity: Systematic Mapping Study", *IEEE Access*, vol. 9, 2021, ISSN: 21693536. DOI: 10.1109/ACCESS.2021.3117588.

[105] S. M. M. Alam, M. A. A. Mamun, M. S. Hossain y M. Samiruzzaman, "A Novel Approach to Manage Ownership and VAT Using Blockchain-Based Digital Identity", en *UNet 2021*, Berlin, Heidelberg: Springer-Verlag, 2021, págs. 255-268, ISBN: 978-3-030-86355-5. DOI: 10.1007/978-3-030-86356-2_21.

[106] M. Xiao, Z. Ma y T. Li, "Privacy-Preserving and Scalable Data Access Control Based on Self-sovereign Identity Management in Large-Scale Cloud Storage", en *LNCS 12382*, vol. 12382 LNCS, 2021, págs. 1-18. DOI: 10.1007/978-3-030-68851-6_1.

[107] C. Dong, Z. Wang, S. Chen e Y. Xiang, "BBM: A Blockchain-Based Model for Open Banking via Self-sovereign Identity", en *LNCS 12404*, vol. 12404 LNCS, 2020, págs. 61-75. DOI: 10.1007/978-3-030-59638-5_5.

[108] M. Lockwood, "An Accessible Interface Layer for Self-Sovereign Identity", *Front. Blockchain*, vol. 3, 2021, ISSN: 2624-7852. DOI: 10.3389/fbloc.2020.609101.

[109] M. Freytsis et al., "Development of a Mobile, Self-Sovereign Identity Approach for Facility Birth Registration in Kenya", *Front. Blockchain*, vol. 4, 2021, ISSN: 2624-7852. DOI: 10.3389/fbloc.2021.631341.

[110] W. Fdhila, N. Stifter, K. Kostal, C. Saglam y M. Sabadello, "Methods for Decentralized Identities: Evaluation and Insights", en *LNBIP 428*, 2021, págs. 119-135. DOI: 10.1007/978-3-030-85867-4_9.

[111] A. J. Lotka, "The Frequency Distribution of Scientific Productivity", *J. Wash. Acad. Sci.*, vol. 16, n.º 12, págs. 317-323, jun. de 1926, ISSN: 0043-0439. dirección: http://www.jstor.org/stable/24529203.

[112] S. C. Bradford, "Sources of information on specific subjects", *J. Inf. Sci. Eng.*, vol. 10, n.º 4, págs. 173-175, 1985. DOI: 10.1177/016555158501000406.

[113] E. Bandara et al., "Promize - Blockchain and Self Sovereign Identity Empowered Mobile ATM Platform", en *LNNS, 284*, K. Arai, ed., vol. 284, Springer International Publishing, 2021, págs. 891-911, ISBN: 978-3-030-80126-7. DOI: 10.1007/978-3-030-80126-7_63.

[114] A.-E. Panait, R. Olimid y A. Stefanescu, "Identity management on blockchain – Privacy and security aspects", *Proc. Rom. Acad. Ser. A Math. Phys. Tech. Sci. Inf. Sci.*, vol. 21, n.º 1, págs. 45-52, 2020, ISSN: 14549069.

[115] A.-E. Panait y R. F. Olimid, "On Using Zk-SNARKs and Zk-STARKs in Blockchain-Based Identity Management", en *Conf. SecITC 2021*, Bucharest, Romania: Springer-Verlag, 2020, págs. 130-145, ISBN: 978-3-030-69254-4. DOI: 10.1007/978-3-030-69255-1_9.

[116] A. Abraham, C. Schinnerl y S. More, "SSI strong authentication using a mobile-phone based identity wallet reaching a high level of assurance", en *Proc. Int. Conf. Secur. Cryptography, SECRYPT*, S. P. di Vimercati S.De.C., ed., 2021, págs. 137-148, ISBN: 9789897585241. DOI: 10.5220/0010542801370148.

[117] A. C. Penedo, "Self-sovereign identity systems and European data protection regulations: An analysis of roles and responsibilities", en *Open Identity Summit 2021*, vol. P-312, 2021, págs. 95-106. dirección: https://dl.gi.de/handle/20.500.12116/36505.

[118] M. Kubach y H. Robnagel, "A lightweight trust management infrastructure for self-sovereign identity", en *Open Identity Summit 2021*, vol. P-312, 2021, págs. 155-165. dirección: https://dl.gi.de/handle/20.500.12116/36489.

[119] M. Kubach y R. Sellung, "On the market for self-sovereign identity: Structure and stakeholders", en *Open Identity Summit 2021*, vol. 312, 2021, págs. 143-154. dirección: https://dl.gi.de/handle/20.500.12116/36488.

[120] L. Alber, S. More, S. Mödersheim y A. Schlichtkrull, "Adapting the TPL Trust Policy Language for a Self-Sovereign Identity World", en *Open Identity Summit 2021*, H. Roßnagel, C. H. Schunck y S. Mödersheim, eds., Bonn: Gesellschaft für Informatik e.V., 2021, págs. 107-118, ISBN: 9783885797067. dirección: https://dl.gi.de/handle/20.500.12116/36506.

[121] M. Kubach, C. H. Schunck, R. Sellung y H. Roßnagel, "Self-sovereign and decentralized identity as the future of identity management?", en *Open Identity Summit 2021*, vol. 305, 2020, págs. 35-47. DOI: 10.18420/ois2020_03.

[122] S. Mahula, E. Tan y J. Crompvoets, "With Blockchain or Not? Opportunities and Challenges of Self-Sovereign Identity Implementation in Public Administration: Lessons from the Belgian Case", en *DG.O'21*, Omaha, NE, USA: Association for Computing Machinery, 2021, págs. 495-504, ISBN: 9781450384926. DOI: 10.1145/3463677.3463705.

[123] A. Pillai, V. Saraswat y A. V. Ramachandran, "Protection Guidelines for Blockchain Based Digital Identity", en *LNNS, 420*, vol. 420 LNNS, 2022, págs. 636-646. DOI: 10.1007/978-3-030-96305-7_59.

[124] A. Pillai, V. Saraswat y A. Vasanthakumary Ramachandran, "Attacks on Blockchain Based Digital Identity", en *LNNS, 320*, vol. 320, 2022, págs. 329-338. DOI: 10.1007/978-3-030-86162-9_33.

[125] F. Schardong, R. Custódio, L. Pioli y J. Meyer, "Matching Metadata on Blockchain for Self-Sovereign Identity", en *LNBIP, 436*, vol. 436, 2022, págs. 421-433. DOI: 10.1007/978-3-030-94343-1_32.

[126] S. Lohar, S. Babar y P. Mahalle, "A proposed approach for Digital Identity management using Self Sovereign Identity", *Int. J. Next-Gener. Comput.*, vol. 12, n.º 2, SI, págs. 158-168, abr. de 2021, ISSN: 2229-4678.

[127] T. Zhou, X. Li y H. Zhao, "EverSSDI: Blockchain-Based Framework for Verification, Authorisation and Recovery of Self-Sovereign Identity Using Smart Contracts", *Int. J. Comput. Appl. Technol.*, vol. 60, n.º 3, págs. 281-295, 2019, ISSN: 0952-8091. DOI: 10.1504/ijcat.2019.100300.

[128] R. Haque, A. Hasan, A. Daria, Q. Qu y Q. Jiang, "Towards Convergence of Blockchain and Self-sovereign Identity for Privacy-Preserving Secure Federated Learning", en *ICBDS 2021*, vol. 1563, 2022, págs. 243-255, ISBN: 978-981-19-0852-1. DOI: 10.1007/978-981-19-0852-1_19.

[129] R. Joosten, *Self-Sovereign Identity framework and Blockchain*, 2017. visitado 13 de abr. de 2021. dirección: https://ercim-news.ercim.eu/en110/special/self-sovereign-identity-framework-and-blockchain.

[130] P. Adane, A. Jadhav, S. Kodgire, A. Agrawal y S. Kumar, "Integration of Self Sovereign Identity in Security Systems", *Ijngc*, vol. 12, n.º 5, págs. 732-738, nov. de 2021, ISSN: 2229-4678. DOI: 10.47164/ijngc.v12i5.459.

[131] A.-E. Drăgnoiu, "Using Blockchain Technology for Software Identity Maintenance", en *Middleware '21*, ép. Middleware '21, Québec city, Canada: Association for Computing Machinery, 2021, págs. 25-28, ISBN: 9781450391559. DOI: 10.1145/3491087.3493682.

[132] K. Sunda, "Online privacy-self-sovereign identity", *JISSec*, vol. 16, n.º 2, págs. 121-135, 2020.

[133] A. Giannopoulou, "Data Protection Compliance Challenges for Self-sovereign Identity", en *Blockchain 2020*, Springer International Publishing, 2020, págs. 1-10, ISBN: 978-3-030-52535-4. DOI: 10.2139/ssrn.3671523.

[134] A. Bazarhanova, J. Lindman, J. Magnusson, E. Chou y A. Nilsson, "Blockchain-based electronic identification: Cross-country comparison of six design choices", en *ECIS 2019*, 2019, ISBN: 978-1-7336325-0-8. dirección: https://aisel.aisnet.org/ecis2019_rp/79/.

[135] M. A. A. Mamun, S. M. M. Alam, M. S. Hossain y M. Samiruzzaman, "A Novel Approach to Blockchain-Based Digital Identity System", en *FICC 2020*, 2020, págs. 93-112, ISBN: 978-3-030-39445-5. DOI: 10.1007/978-3-030-39445-5_9.

[136] N. V. Kulabukhova, "Zero-knowledge proof in self-sovereign identity", en *NEC'2019*, vol. 2507, 2019, págs. 381-385. dirección: https://ceur-ws.org/Vol-2507/381-385-paper-70.pdf.

[137] N. Kulabukhova, "Self-sovereign identity as trusted root in knowledge based systems", en *LNCS 12251*, 2020, págs. 14-24. DOI: 10.1007/978-3-030-58808-3_2.

[138] A. Dubovitskaya, L. Mazzola y A. Denzler, "Towards a Trusted Support Platform for the Job Placement Task", en *Euro-Par 2019*, 2020, págs. 203-215. DOI: 10.1007/978-3-030-48340-1_16.

[139] A. Grech, I. Sood y L. Ariño, "Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education", *Front. Blockchain*, vol. 4, 2021, ISSN: 2624-7852. DOI: 10.3389/fbloc.2021.616779.

[140] S. S. Darnell y J. Sevilla, "3 Stages of a Pan-African Identity Framework for Establishing Self-Sovereign Identity With Blockchain", *Front. Blockchain*, vol. 4, 2021, ISSN: 2624-7852. DOI: 10.3389/fbloc.2021.631640.

[141] J. C. Ferreira, C. F. da Silva y J. P. Martins, "Roaming service for electric vehicle charging using blockchain-based digital identity", *Energies*, vol. 14, n.º 6, 2021. DOI: 10.3390/en14061686.

[142] X. Xiang, M. Wang y W. Fan, "A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems", *IEEE Access*, vol. 8, págs. 171 771-171 783, 2020. DOI: 10.1109/ACCESS.2020.3022429.

[143] D. Pennino, M. Pizzonia, A. Vitaletti y M. Zecchini, "Efficient Certification of Endpoint Control on Blockchain", *IEEE Access*, vol. 9, págs. 133 309-133 334, 2021. DOI: 10.1109/ACCESS.2021.3115343.

[144] X. Li, J. Zhang, X. Niu y J. Guan, "Blockchain-Based Certificateless Identity Management Mechanism in Cloud-Native Environments", en *ACM ICEA '21*, Jinan, China: Association for Computing Machinery, 2022, págs. 139-145, ISBN: 9781450391603. DOI: 10.1145/3491396.3506537.

[145] G. Linklater, A. Herbert, C. Smith y B. Irwin, "Toward distributed key management for offline authentication :Self-sovereign identity using intermediate certificates", en *SAICSIT '18*, 2018, págs. 10-19. DOI: 10.1145/3278681.3278683.

[146] M. Aruna, M. Hasan, S. Islam, K. Mohan, P. Sharan y R. Hassan, "Cloud to cloud data migration using self sovereign identity for 5G and beyond", *Cluster Comput.*, vol. 25, 2022, ISSN: 13867857. DOI: 10.1007/s10586-021-03461-7.

[147] D. Pöhn, M. Grabatin y W. Hommel, "Eid and self-sovereign identity usage: An overview", *Electronics*, vol. 10, n.º 22, 2021, ISSN: 20799292. DOI: 10.3390/electronics10222811.

[148] C. Sung y J. Park, "Understanding of blockchain-based identity management system adoption in the public sector", *J. Enterp. Inf. Manage.*, vol. 34, n.º 5, págs. 1481-1505, 2021, ISSN: 17410398. DOI: 10.1108/JEIM-12-2020-0532.

[149] L. Argento et al., "ID-Service: A Blockchain-Based Platform to Support Digital-Identity-Aware Service Accountability", *Appl. Sci.*, vol. 11, n.º 1, 2021, ISSN: 2076-3417. DOI: 10.3390/app11010165.

[150] N. D. Sarier, "Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management", *Computers & Security*, vol. 105, 2021, ISSN: 0167-4048. DOI: 10.1016/j.cose.2021.102243.

[151] R. B. Gans, J. Ubacht y M. Janssen, "Self-Sovereign Identities for Fighting the Impact of COVID-19 Pandemic", *Digit. Gov.: Res. Pract.*, vol. 2, n.º 2, dic. de 2020, ISSN: 2691-199X. DOI: 10.1145/3429629.

[152] N.-C. Ursache, "Swarm Communication using Self Sovereign Identities", en *RoEduNet 2021*, 2021, págs. 1-6. DOI: 10.1109/RoEduNet54112.2021.9638293.

[153] H. Yildiz, C. Ritter, L. T. Nguyen, B. Frech, M. M. Martinez y A. Küpper, "Connecting Self-Sovereign Identity with Federated and User-centric Identities via SAML Integration", en *ISCC 2021*, 2021, págs. 1-7. DOI: 10.1109/ISCC53001.2021.9631453.

[154] H. Siddiqui, M. Idrees, I. Gudymenko, D. L. Quoc y C. Fetzer, "Credentials as a Service Providing Self Sovereign Identity as a Cloud Service Using Trusted Execution Environments", en *IC2E 2021*, 2021, págs. 210-216. DOI: 10.1109/IC2E52221.2021.00036.

[155] M. Htet, P. T. Yee y J. R. Rajasekera, "Blockchain based Digital Identity Management System: A Case Study of Myanmar", en *ICAIT 2020*, 2020, págs. 42-47. DOI: 10.1109/ICAIT51105.2020.9261785.

[156] J. Liu, A. Hodges, L. Clay y J. Monarch, "An analysis of digital identity management systems - a two-mapping view", en *BRAINS 2020*, 2020, págs. 92-96. DOI: 10.1109/BRAINS49436.2020.9223281.

[157] P. Gururaj, "Identity management using permissioned blockchain", en *ICOMBI 2020*, 2020, págs. 1-3. DOI: 10.23919/ICOMBI48604.2020.9203031.

[158] Z. Zhao e Y. Liu, "A Blockchain based Identity Management System Considering Reputation", en *ICISCAE 2019*, 2019, págs. 32-36. DOI: 10.1109/ICISCAE48440.2019.221582.

[159] M. Schanzenbach, G. Bramm y J. Schütte, "reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption", en *TrustCom/ BigDataSE 2018*, 2018, págs. 946-957. DOI: 10.1109/TrustCom/BigDataSE.2018.00134.

[160] L. Cocco, R. Tonelli y M. Marchesi, "Blockchain and self sovereign identity to support quality in the food supply chain", *Future Internet*, vol. 13, n.º 12, 2021. DOI: 10.3390/fi13120301.

[161] S. De Diego, C. Regueiro y G. Macia-Fernandez, "Enabling Identity for the IoT-as-a-Service Business Model", *IEEE Access*, vol. 9, págs. 159 965-159 975, 2021. DOI: 10.1109/ACCESS.2021.3131012.

[162] A. S. Sani, D. Yuan, K. Meng y Z. Y. Dong, "Idenx: A blockchain-based identity management system for supply chain attacks mitigation in smart grids", en *PESGN 2020*, ago. de 2020. DOI: 10.1109/PESGM41954.2020.9281929.

[163] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. L. Chen, M. Abu-Tair y Z. Cui, "Distributed, Secure, Self-Sovereign Identity for IoT Devices", en *WF-IoT 2020*, 2020, págs. 1-6. DOI: 10.1109/WF-IoT48130.2020.9221144.

[164] G. Fedrecheski, J. M. Rabaey, L. C. P. Costa, P. C. Calcina Ccori, W. T. Pereira y M. K. Zuffo, "Self-Sovereign Identity for IoT environments: A Perspective", en *GIoTS 2020*, 2020, págs. 1-6. DOI: 10.1109/GIOTS49054.2020.9119664.

[165] M. Luecking, C. Fries, R. Lamberti y W. Stork, "Decentralized Identity and Trust Management Framework for Internet of Things", en *ICBC 2020*, 2020, págs. 1-9. DOI: 10.1109/ICBC48266.2020.9169411.

[166] P. C. Bartolomeu, E. Vieira, S. M. Hosseini y J. Ferreira, "Self-Sovereign Identity: Use-cases, Technologies, and Challenges for Industrial IoT", en *ETFA 2019*, 2019, págs. 1173-1180. DOI: 10.1109/ETFA.2019.8869262.

[167] A. AlQallaf, "Blockchain-Based Digital Identity Management Scheme for Field Connected IoT Devices", en *SPEKOGS 2019*, vol. Day 3 Tue, October 15, 2019, oct. de 2019. DOI: 10.2118/198082-MS. eprint: https://onepetro.org/SPEKOGS/proceedings-pdf/19KOGS/3-19KOGS/D033S016R005/1179849/spe-198082-ms.pdf.

[168] N. Kulabukhova, A. Ivashchenko, I. Tipikin e I. Minin, "Self-Sovereign Identity for IoT Devices", en *LNCS 11620*, vol. 11620 LNCS, 2019, págs. 472-484.

[169] S. Terzi, C. Savvaidis, K. Votis, D. Tzovaras e I. Stamelos, "Securing Emission Data of Smart Vehicles with Blockchain and Self-Sovereign Identities", en *Proc. - IEEE Int. Conf. Blockchain, Blockchain*, Institute of Electrical y Electronics Engineers Inc., 2020, págs. 462-469, ISBN: 9780738104959. DOI: 10.1109/Blockchain50366.2020.00067.

[170] M. L. Alessandria y A. Vizzarri, "Self-Sovereign Identity and Blockchain applications for the automotive sector", en *AEIT Automotive 2021*, IEEE, 2021, págs. 1-6, ISBN: 978-88-87237-59-7. DOI: 10.23919/AEITAUTOMOTIVE52815.2021.9662861.

[171] A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. Lauinger y S. Steinhorst, "Towards a Blockchain-based Identity and Trust Management Framework for the IoV Ecosystem", en *GIoTS - Glob. Internet Things Summit, Proc.*, 2020, ISBN: 9781728121710. DOI: 10.1109/GIOTS49054.2020.9119623.

[172] M. Grabatin y W. Hommel, "Self-sovereign Identity Management in Wireless Ad Hoc Mesh Networks", en *Proc. IM - IFIP/IEEE Int. Symp. Integr. Netw. Manag.*, Institute of Electrical y Electronics Engineers Inc., 2021, págs. 480-486, ISBN: 9783903176324.

[173] A. Giannopoulou y F. Wang, "Self-sovereign identity", *Internet Policy Rev.*, vol. 10, n.º 2, págs. 1-10, 2021, ISSN: 21976775. DOI: 10.14763/2021.2.1550.

[174] S. Terzi, C. Savvaidis, A. Sersemis, K. Votis y D. Tzovaras, "Decentralizing Identity Management and Vehicle Rights Delegation through Self-Sovereign Identities and Blockchain", en *COMPSAC 2021*, 2021, págs. 1217-1223. DOI: 10.1109/COMPSAC51774.2021.00168.

[175] E. Samir, H. Wu, M. Azab, C. S. Xin y Q. Zhang, "DT-SSIM: A Decentralized Trustworthy Self-Sovereign Identity Management Framework", *IoT-J*, vol. 9, n.º 11, págs. 7972-7988, 2022. DOI: 10.1109/JIOT.2021.3112537.

[176] C. Zhuang, Q. Dai e Y. Zhang, "BCPPT: A blockchain-based privacy-preserving and traceability identity management scheme for intellectual property", *Peer-to-Peer Netw. Appl.*, vol. 15, n.º 1, págs. 724-738, 2022, ISSN: 19366442. DOI: 10.1007/s12083-021-01277-1.

[177] V. Lemieux, A. Voskobojnikov y M. Kang, "Addressing Audit and Accountability Issues in Self-Sovereign Identity Blockchain Systems Using Archival Science Principles", en *COMPSAC 2021*, 2021, págs. 1210-1216. DOI: 10.1109/COMPSAC51774.2021.00167.

[178] H. Nusantoro, R. Supriati, N. Azizah, N. P. Lestari Santoso y S. Maulana, "Blockchain Based Authentication for Identity Management", en *CITSM 2021*, 2021, págs. 1-8. DOI: 10.1109/CITSM52892.2021.9589001.

[179] S. S. M. Mulaji y S. S. Roodt, "The Practicality of Adopting Blockchain-Based Distributed Identity Management in Organisations: A Meta-Synthesis", *Secur. Commun. Netw.*, vol. 2021, 2021. DOI: 10.1155/2021/9910078.

[180] M. P. Bhattacharya, P. Zavarsky y S. Butakov, "Enhancing the Security and Privacy of Self-Sovereign Identities on Hyperledger Indy Blockchain", en *ISNCC 2020*, 2020, págs. 1-7. DOI: 10.1109/ISNCC49221.2020.9297357.

[181] O. Dib y K. Toumi, "Decentralized identity systems: Architecture, challenges, solutions and future directions", *AETiC*, vol. 4, n.º 5, págs. 19-40, 2020. DOI: 10.33166/AETiC.2020.05.002.

[182] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi y K. N. Qureshi, "Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare", *Healthcare*, vol. 9, n.º 6, 2021, ISSN: 2227-9032. DOI: 10.3390/healthcare9060712.

[183] N. Mohammadzadeh, S. Nogoorani y J. Muñoz-Tapia, "Decentralized factoring for self-sovereign identities", *Electronics*, vol. 10, n.º 12, 2021, ISSN: 20799292. DOI: 10.3390/electronics10121467.

[184] C. Dong, F. Jiang, X. Li, A. Yao, G. Li y X. Liu, "A Blockchain-aided Self-Sovereign Identity Framework for Edge-based UAV Delivery System", en *CCGrid 2021*, 2021, págs. 622-624. DOI: 10.1109/CCGrid51090.2021.00074.

[185] F. S. De Cristo, W. M. Shbair, L. Trestioreanu, R. State y A. Malhotra, "Self-Sovereign Identity for the Financial Sector: A Case Study of PayString Service", en *Blockchain 2021*, 2021, págs. 213-220. DOI: 10.1109/Blockchain53845.2021.00036.

[186] K. Dissanayake, P. Somarathne, U. Fernando, D. Pathmasiri, C. Liyanapathirana y D. L. Rupasinghe, "Trust Pass - Blockchain-Based Trusted Digital Identity Platform Towards Digital Transformation", en *IISEC 2021*, 2021, págs. 1-6. DOI: 10.1109/IISEC54230.2021.9672336.

[187] K. A. M. Ahmed, S. F. Saraya, J. F. Wanis y A. M. T. Ali-Eldin, "A Self-Sovereign Identity Architecture Based on Blockchain and the Utilization of Customer's Banking Cards : The Case of Bank Scam Calls Prevention", en *ICCES 2020*, 2020, págs. 1-8. DOI: 10.1109/ICCES51560.2020.9334648.

[188] V. Schlatt, J. Sedlmeir, S. Feulner y N. Urbach, "Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity", *Information and Management*, 2021, ISSN: 0378-7206. DOI: 10.1016/j.im.2021.103553.

[189] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos y S. Guerreiro, "SSIBAC: Self-Sovereign Identity Based Access Control", en *TrustCom 2020*, IEEE, 2020, págs. 1935-1943. DOI: 10.1109/TrustCom50675.2020.00264.

[190] M. A. R. Tonu, S. Hridoy, M. A. Ali y S. A. Azad, "Block - NID: A Conceptual Secure Blockchain Based National Identity Management System Model", en *CSDE 2019*, 2019, págs. 1-7. DOI: 10.1109/CSDE48274.2019.9162366.

[191] Sovrin Foundation, *Sovrin : A Protocol and Token for Self-Sovereign Identity and Decentralized Trust*, D. R. Phil Windley, ed., 2018. visitado 16 de mayo de 2022. dirección: https://sovrin.org/library/sovrin-protocol-and-token-white-paper/pdf.

[192] Hyperledger Foundation, *Hyperledger Indy*, 2022. visitado 16 de jun. de 2022. dirección: https://github.com/hyperledger/indy-sdk.

[193] Veramo, *Veramo core development: Tools for Verifiable Data and SSI*, 2016. visitado 16 de mayo de 2022. dirección: https://github.com/uport-project/.

[194] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", 2014. visitado 16 de mayo de 2022. dirección: https://github.com/ethereum/yellowpaper.

[195] Veres One Network, *Veres One: The Veres One Project*, 2022. visitado 20 de mayo de 2022. dirección: https://github.com/veres-one.

[196] Identity Foundation, *The Identity Overlay Network (ION)*, 2022. visitado 30 de sep. de 2022. dirección: https://github.com/decentralized-identity/ion.

[197] Identity Foundation, *Sidetree protocol*, 2021. visitado 20 de mayo de 2022. dirección: https://github.com/decentralized-identity/sidetree.

[198] MongoDB Inc, *MongoDB*, 2022. visitado 20 de mayo de 2022. dirección: http://www.mongodb.com/.

[199] Ping Identity, *Shocard*, 2019. visitado 20 de mayo de 2022. dirección: https://www.shocard.com/.

[200] Horizon 2020 Project, *Decode: Giving people ownership of their personal data*, 2020. visitado 17 de mayo de 2022. dirección: https://decodeproject.eu/.

[201] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn y G. Danezis, "Chainspace: A Sharded Smart Contracts Platform", en *NDSS Symposium 2018*, 2018, ISBN: 1-891562-49-5. DOI: 10.14722/ndss.2018.23241.

[202] Dyne.org foundation, *Blockchain smart-contracts in human language*, 2022. visitado 17 de mayo de 2022. dirección: https://zenroom.org/sawroom/.

[203] Stacks Open Internet Foundation, *Stacks 2.0: Apps and Smart Contracts for Bitcoin*, 2022. visitado 17 de mayo de 2022. dirección: https://docs.stacks.co/es/en/understand-stacks/technical-specs.

[204] M. Ali et al., *Stacking Consensus*, 2020. visitado 17 de mayo de 2022. dirección: https://github.com/stacksgov/sips/tree/main/sips/sip-007.

[205] clarity-lang.org, *Clarity -safer smart contracts- Write smart contracts for Bitcoin and open a world of DeFi, NFTs, and more on the world's most secure blockchain*, 2020. visitado 17 de mayo de 2022. dirección: https://github.com/clarity-lang.

[206] Jolocom.io, *Jolocom: Own your digital self*, 2020. visitado 17 de mayo de 2022. dirección: https://github.com/jolocom.

[207] Democracy Earth Foundation, *A Decentralized, Open Source Solution for Digital Identity and Access Management*, 2022. visitado 17 de mayo de 2022. dirección: https://democracy.earth/.

[208] kleros, *Kleros: The Justice Protocol*, 2022. visitado 17 de mayo de 2022. dirección: https://kleros.io/.

[209] Litentry, *Litentry*, 2022. visitado 28 de sep. de 2022. dirección: https://github.com/litentry.

[210] Litentry Technologies, *Litentry Network*, 2021. visitado 17 de mayo de 2022. dirección: https://docs.litentry.com/parachain/get-started/litentry-network.

[211] SelfKey Foundation, *SelfKey: Self-Sovereign Identity for more Freedom and Privacy*, 2022. visitado 17 de mayo de 2022. dirección: https://selfkey.org/whitepaper/.

[212] Civic Developer Hub, *Civic: We provide on-chain identity layer creating trust across web3*, 2020. visitado 29 de sep. de 2022. dirección: https://docs.civic.com/.

[213] IOVLabs, *Rootstock The foundation for a freer and fairer global financial system built on bitcoin*, 2022. visitado 23 de mayo de 2022. dirección: https://www.rsk.co/.

[214] BrightID Main LLC, *brightID: Universal Proof of Uniqueness*, 2022. visitado 23 de mayo de 2022. dirección: https://www.brightid.org/whitepaper.

[215] ArangoDB Inc, *ArangoDB: the multi-model database for graph and beyond*, 2014. visitado 23 de mayo de 2022. dirección: https://www.arangodb.com/.

[216] BOTLabs GmbH, *KILT Protocol - White Paper*, 2020. visitado 23 de mayo de 2022. dirección: https://www.kilt.io/wp-content/uploads/2020/01/KILT-White-Paper-v2020-Jan-15.pdf.

[217] Parity Technologies, *Parity substrate: Build your own Blockchain*, 2020. visitado 23 de mayo de 2022. dirección: https://www.parity.io/technologies/substrate/.

[218] SoraId Inc., *Sora: User-driven identity verification*, 2022. visitado 23 de mayo de 2022. dirección: https://soraid.com/.

[219] Everest Network Ltd, *EverID: Decentralized Identity Platform*, 2022. visitado 23 de mayo de 2022. dirección: https://everest.org/technology.

[220] R. Pava-Díaz, *Bibliometría: Self-Sovereing Identity Versión 2.0*, jul. de 2024. DOI: 10.6084/m9.figshare.25687026.v2. visitado 17 de jul. de 2024. dirección: https://figshare.com/articles/dataset/Bibliometr_a_Self-Sovereing_Identity_Versi_n_2_0/25687026.

[221] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele y C. Allen, *Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations*, 2020. visitado 7 de jun. de 2021. dirección: https://www.w3.org/TR/did-core/.

[222] M. Sporny, D. Longley y D. Chadwick, *Verifiable Credentials Data Model v1.1*, 2022. visitado 9 de jun. de 2021. dirección: https://www.w3.org/TR/vc-data-model/.

[223] C. Allen, *Self-sovereing identity principles*, 2016. visitado 6 de mayo de 2022. dirección: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md.

[224] P. J. Leach, R. Salz y M. H. Mealling, *A Universally Unique IDentifier (UUID) URN Namespace*, 2005. visitado 15 de jul. de 2021. dirección: https://www.rfc-editor.org/info/rfc4122.

[225] Namecoin, *Namecoin: Decentralized secure names*, 2021. visitado 15 de jul. de 2022. dirección: https://www.namecoin.org/.

[226] Emercoin, *Emercoin Blockchain*, 2022. visitado 15 de jul. de 2022. dirección: https://emercoin.com/en/.

[227] ens domains, *Ethereum Name Service: Decentralised naming for wallets, websites, and more*, 2022. visitado 15 de jul. de 2022. dirección: https://ens.domains/.

[228] C. Ellison, "Establishing Identity Without Certification Authorities", en *USENIX Security 96*, San Jose, CA: USENIX Association, jul. de 1996. dirección: https://www.usenix.org/conference/6th-usenix-security-symposium/establishing-identity-without-certification-authorities.

[229] Identity Foundation, *Universal Resolver*, 2022. visitado 9 de jun. de 2022. dirección: https://github.com/decentralized-identity/universal-resolver/.

[230] T. Berners-Lee, R. Fielding y L. Masinter, *Uniform Resource Identifier (URI): Generic Syntax*, 2005. visitado 10 de jun. de 2022. dirección: https://www.rfc-editor.org/rfc/rfc3986.

[231] Credentials Community Group, *JSON Web Signature 2020*, 2005. visitado 10 de jun. de 2022. dirección: https://w3c-ccg.github.io/lds-jws2020/.

[232] C. Allen et al., *Rebooting the Web of Trust*, 2022. visitado 21 de jul. de 2022. dirección: https://www.weboftrust.info/.

[233] J. Callahan et al., *Six Principles for Self-Sovereign Biometrics*, 2019. visitado 21 de jul. de 2022. dirección: https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/draft-documents/Biometrics.md.

[234] W3C Community Group, *Verifiable Credentials Examples*, 2020. visitado 11 de jun. de 2021. dirección: https://github.com/w3c-ccg/vc-examples.

[235] P. Otte, M. de Vos y J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain", *Future Gener. Comp. Sy.*, vol. 107, págs. 770-780, 2020, ISSN: 0167-739X. DOI: 10.1016/j.future.2017.08.048.

[236] Rahasak, *Rahasak Blockchain*, 2022. visitado 29 de ago. de 2022. dirección: https://rahasak.com/.

[237] N. Sakimura et al., *OpenID Connect Core 1.0*, 2014. visitado 30 de ago. de 2022. dirección: https://openid.net/specs/openid-connect-core-1_0.html.

[238] The Identity Python, *Pysam2: Security Assertion Markup Language 2.0*, 2022. visitado 30 de ago. de 2022. dirección: https://pypi.org/project/pysaml2/.

[239] ShoCard Inc., "Identity management verified using the blockchain", 2017, pág. 20. visitado 12 de ene. de 2020. dirección: https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf.

[240] Idena network, *Idena: Cryptoidentity is the building block for Web 3.0*, 2018. visitado 30 de sep. de 2022. dirección: https://docs.idena.io/.

[241] Idena network, *Idena: Proof-of-Person blockchain. It allows for proof of humanity and uniqueness for its participants by running AI-hard Turing test globally at the same time*, 2022. visitado 30 de sep. de 2022. dirección: https://github.com/idena-network.

[242] Sovrin Foundation, *Sovrin Governance Framework*, 2019. visitado 5 de mayo de 2020. dirección: https://sovrin.org/library/sovrin-governance-framework/.

[243] Sovrin Foundation, *Principios of SSI Version 2.0*, 2019. visitado 5 de mayo de 2020. dirección: https://sovrin.org/principles-of-ssi/.

[244] S. Curren, T. Looker y O. Terbu, *DIDComm Messaging*, 2020. visitado 26 de jul. de 2022. dirección: https://github.com/decentralized-identity/didcomm-messaging.

[245] Hyperledger Foundation, *Hyperledger Aries*, 2019. visitado 26 de jul. de 2022. dirección: https://github.com/hyperledger/aries.

[246] Veramo, *lambda-chasqui: Messenger service*, 2018. visitado 27 de jul. de 2022. dirección: https://github.com/uport-project/lambda-chasqui.

[247] Veramo, *lambda-sensui: uPort Funding Service*, 2017. visitado 27 de jul. de 2022. dirección: https://github.com/uport-project/lambda-sensui.

[248] Infura Inc, *The Infura Ethereum API*, 2022. visitado 27 de jul. de 2022. dirección: https://infura.io/product/ethereum.

[249] Infura Inc, *IPFS: Scalable and distributed storage infrastructure for your application*, 2022. visitado 27 de jul. de 2022. dirección: https://infura.io/product/ipfs.

[250] Y. Liu, D. He, M. Obaidat, N. Kumar, M. Khan y K.-K. Raymond Choo, "Blockchain-based identity management systems: A review", *J. Netw. Comput. Appl.*, vol. 166, 2020, ISSN: 10848045. DOI: 10.1016/j.jnca.2020.102731.

[251] Etherscan, *The Ethereum Blockchain Explorer*, 2022. visitado 28 de sep. de 2022. dirección: https://etherscan.io/.

[252] Graph Foundation, *The graph: APIs for a vibrant decentralized future*, 2022. visitado 28 de sep. de 2022. dirección: https://thegraph.com/en/.

[253] OnFinality, *Blockchain Infrastructure Made Smarter*, 2022. visitado 28 de sep. de 2022. dirección: https://www.onfinality.io/.

[254] Web3 Foundation, *Polkadot: Vision for a heterogeneous multi-chain framework*, 2017. visitado 27 de sep. de 2022. dirección: https://polkadot.network/PolkaDotPaper.pdf.

[255] Web3 Foundation, *Kusama: Polkadot's Canary Network*, 2022. visitado 27 de sep. de 2022. dirección: https://guide.kusama.network/docs/kusama-getting-started.

[256] Identity, *Identity.com: On-demand, secure, and accessible identity verification services powered by blockchain technology and governed with CVC tokens*, 2019. visitado 18 de ago. de 2022. dirección: https://github.com/identity-com.

[257] C. Brandon, *Cryptocurrency Market Capitalizations*, 2013. visitado 24 de abr. de 2020. dirección: https://coinmarketcap.com/.

[258] BOTLabs GmbH, *KILT protodol: KILT is a blockchain protocol for issuing self-sovereign verifiable, revocable, anonymous credentials in the Web 3.0*, 2022. visitado 1 de oct. de 2022. dirección: https://github.com/KILTprotocol.

[259] W3C Community Group, *WebAssembly*, 2022. visitado 23 de mayo de 2022. dirección: https://webassembly.org/.

[260] P.-L. Aublin, S. B. Mokhtar y V. Quéma, "RBFT: Redundant Byzantine Fault Tolerance", en *ICDCS 2013*, 2013, págs. 297-306. DOI: 10.1109/ICDCS.2013.53.

[261] go-ethereum team, *Rinkeby test network*, 2017. visitado 28 de jul. de 2022. dirección: https://www.rinkeby.io/.

[262] Civic Technologies Inc, *Civic Wallet - digital wallet for money and cryptocurrency*, 2020. visitado 28 de jul. de 2022. dirección: https://github.com/civicteam.

[263] Parity Technologies, *Parity Technologies: solutions for a trust-free world*, 2022. visitado 1 de oct. de 2022. dirección: https://github.com/paritytech/.

[264] Identity Foundation, *Universal Resolver Driver for Identity Overlay Network (ION) DIDs v1*, 2021. visitado 30 de sep. de 2022. dirección: https://github.com/decentralized-identity/uni-resolver-driver-did-ion.

[265] Adobe, *Crea con IA Firefly generativa*, https://www.adobe.com/es/products/firefly.html, Accessed: 30 August 2024, 2024. visitado 30 de ago. de 2024. dirección: https://www.adobe.com/es/products/firefly.html.

[266] Trust Over IP Foundation, *The trust Over IP model*, 2020. visitado 3 de ago. de 2022. dirección: https://trustoverip.org/toip-model/.

[267] C. Huitema et al., "Introduction to Trust Over IP", Trust over ip foundation, inf. téc. May 2020, 2021, pág. 35. visitado 30 de mayo de 2023. dirección: https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf.

[268] A. Kettunen et al., "Design Principles for the Trust over IP Stack", The Trust Over IP Foundation, inf. téc. November, 2021, págs. 1-63. visitado 30 de mayo de 2023. dirección: https://trustoverip.org/our-work/design-principles/.

[269] A. Mavin, P. Wilkinson, A. Harwood y M. Novak, "Easy Approach to Requirements Syntax (EARS)", en *2009 17th IEEE International Requirements Engineering Conference*, 2009, págs. 317-322. DOI: 10.1109/RE.2009.9.

[270] W3C Community Group, *Credential Handler API 1.0*, https://w3c-ccg.github.io/credential-handler-api/, Accessed: 30 August 2024, 2021. visitado 30 de ago. de 2024. dirección: https://w3c-ccg.github.io/credential-handler-api/.

[271] K. Hamilton-Duffy, R. Grant y A. Gropper, *Use Cases and Requirements for Decentralized Identifiers*, 2021. visitado 13 de mar. de 2023. dirección: https://www.w3.org/TR/did-use-cases/.

[272] ConsenSys Software Inc., *Truffle Suite*, 2024. visitado 12 de mayo de 2024. dirección: https://archive.trufflesuite.com/ganache/.

[273] Pinata, *The Internet's File API*, Pinata, 2024. visitado 20 de sep. de 2024. dirección: https://pinata.cloud/.

[274] Docker, Inc., *Docker Documentation*, https://docs.docker.com/, Accessed: 20 Septembre 2024, 2024. visitado 20 de sep. de 2024. dirección: https://docs.docker.com/.

[275] Redis Inc, *Redis: See how fast feels.* https://redis.io/, 2024. visitado 20 de sep. de 2024. dirección: https://redis.io/.

[276] Chainsafe, *Web3js - The longest-running web3 library*, https://web3js.org/, 2024. visitado 20 de sep. de 2024. dirección: https://web3js.org/.

[277] OpenJs Foundation, *Nodejs: Run JavaScript Everywhere*, https://nodejs.org/en, 2024. visitado 20 de sep. de 2024. dirección: https://nodejs.org/en.

[278] Solidity Team, *A statically-typed curly-braces programming language designed for developing smart contracts that run on Ethereum*, 2024. visitado 12 de mayo de 2024. dirección: https://soliditylang.org/.

[279] Spruce Systems, Inc., *DIDKit*, https://github.com/spruceid/didkit, Accessed: 07 September 2024, 2024. visitado 7 de sep. de 2024. dirección: https://github.com/spruceid/didkit.

[280] Svelte, *Svelte - Cybernetically enhanced web apps*, 2024. visitado 15 de mayo de 2024. dirección: https://svelte.dev/.

[281] Broadcom Inc., *Spring Boot*, 2024. visitado 15 de mayo de 2024. dirección: https://spring.io/projects/spring-boot.

[282] M. Jones, *JSON Web Key (JWK)*, https://datatracker.ietf.org/doc/html/rfc7517, Accessed: 07 September 2024, 2015. visitado 7 de sep. de 2024. dirección: https://datatracker.ietf.org/doc/html/rfc7517.

[283] National Institute of Standards and Technology, *Federal Information Processing Standards Publication 186-5. Digital Signature Standard (DSS)*, 2023. DOI: https://doi.org/10.6028/NIST.FIPS.186-5. visitado 5 de oct. de 2024. dirección: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf.

[284] D. Bernstein, N. Duif, T. Lange, P. Schwabe y B.-Y. Yang, *Ed25519: high-speed high-security signatures*, https://ed25519.cr.yp.to/, Accessed: 07 September 2024, 2017. visitado 7 de sep. de 2024. dirección: https://ed25519.cr.yp.to/.

[285] Broadcom Inc, *Spring Security*, https://docs.spring.io/spring-security/reference/, Accessed: 07 September 2024, 2024. visitado 7 de sep. de 2024. dirección: https://docs.spring.io/spring-security/reference/.

[286] R. Pava-Díaz, S. Gómez-Almeyda y L.-S. Danilo, "Modelo de almacenamiento cifrado y descentralizado basado en identidad digital auto-soberana integrando blockchain e IPFS", en *I conferencia Internacional de Innovación e Investigación*, Bogotá D.C, Colombia: Universidad Militar Nueva Granada, nov. de 2023, págs. 1-7. dirección: https://cinvedudistancia.wixsite.com/conferenciafaedis202.

[287] Oracle, *Java Security Overview*, https://docs.oracle.com/en/java/javase/11/security/java-security-overview1.html, Accessed: 07 September 2024, 2024. visitado 7 de sep. de 2024. dirección: https://docs.oracle.com/en/java/javase/11/security/java-security-overview1.html.

[288] The World Wide Web Consortium, *Contexto para credenciales verificables*, 2018. visitado 1 de oct. de 2024. dirección: https://www.w3.org/2018/credentials/v1.

[289] The World Wide Web Consortium, *Ejemplos de credenciales verificables*, 2018. visitado 1 de oct. de 2024. dirección: https://www.w3.org/2018/credentials/examples/v1.

[290] The World Wide Web Consortium, *Centro de Computación de Alto Desempeño de la Universidad Distrital Francisco José de Caldas (CECAD)*, 2024. visitado 30 de ago. de 2024. dirección: https://cecad.udistrital.edu.co/.

[291] National Institute of Standards and Technology, *Federal Information Processing Standards Publication 197. Advanced Encryption Standard - AES*, 2023. DOI: https://doi.org/10.6028/NIST.FIPS.197-upd1. visitado 4 de oct. de 2024. dirección: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf.

[292] Doctorado en Ingeniería, *Credential Mediator polyfill for the W3C CCG Credential Handler API specification*, 2024. visitado 8 de oct. de 2024. dirección: https://authn.io/.

[293] J. Castañeda y P. Santiago, "Gestión de llaves criptográfcias orientado a un respaldo seguro y su recuperación en redes distribuidas", Trabajo de grado en marco del proyecto de investigación 3370072920, denominado "Modelo para la gestión de una identidad digital descentralizada y autogobernada bajo tecnología de registro distribuido"., Trabajo de Grado, Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia, dic. de 2023.

[294] M. Leguizamo, "Diseño e Implementación de un Nuevo Método para Mitigación de Ataque Sybil con Blockchain", Trabajo de grado en marco del proyecto de investigación 3370072920. Actualmente se encuentra en desarrollo., Trabajo de Grado, Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia, dic. de 2025.

[295] D. Zapata, "Modelo de reputación basado en blockchain e identidad digital auto-soberana aplicado al proceso de evaluación docente", Trabajo de grado en marco del proyecto de investigación 3370072920. Actualmente se encuentra en desarrollo., Trabajo de Grado, Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia, jun. de 2025.

[296] D. Garzón y E. Barrios, "Diseño de un módulo para autenticación usando datos biométricos en un entorno descentralizado", Trabajo de grado en marco del proyecto de investigación 3370072920, denominado "Modelo para la gestión de una identidad digital descentralizada y autogobernada bajo tecnología de registro distribuido"., Trabajo de Grado, Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia, dic. de 2023.

[297] D. Galvan, "Prototipo de una aplicación descentralizada de apoyo a los procedimientos de gestión de inventarios de la Universidad Distrital usando Blockchain e IPFS", Trabajo de grado en marco del proyecto de investigación 3370072920, denominado "Modelo para la gestión de una identidad digital descentralizada y autogobernada bajo tecnología de registro distribuido"., Trabajo de Grado, Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia, jun. de 2021.

[298] C. Motta, "Diseño de un prototipo funcional para un gestor de calificaciones soportado en tecnología Blockchain", Trabajo de grado en marco del proyecto de investigación 3370072920, denominado "Modelo para la gestión de una identidad digital descentralizada y autogobernada bajo tecnología de registro distribuido"., Trabajo de Grado, Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia, jun. de 2020.

[299] S. Gomez, "Diseño e implementación de prototipo basado en Blockchain para verificación automática de requisitos de grado en la Universidad Distrital ¿Francisco José de Caldas", Trabajo de grado en marco del proyecto de investigación 3370072920, denominado "Modelo para la gestión de una identidad digital descentralizada y autogobernada bajo tecnología de registro distribuido"., Trabajo de Grado, Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia, dic. de 2023.

[300] Nomic Foundation, *Ethereum development environment for professionals*, https://hardhat.org/, Accessed: 09 Septembre 2024, 2024. visitado 9 de sep. de 2024. dirección: https://hardhat.org/.

[301] R. Pava-Díaz, J. Perez y L. Niño, "Perspectiva para el uso del modelo P6 de atención en salud bajo un escenario soportado en IoT y blockchain", *Tecnura*, vol. 25, págs. 112-130, 67 ene. de 2021, ISSN: 0123-921X. DOI: 10.14483/22487638.16159.

[302] R. Pava-Díaz, D. Lopez, L. Niño y R. Paez, "Tecnología de registro distribuido (DLT): Características y escenarios de aplicación", *TIA.*, vol. 9, n.º 1, 2022. dirección: https://revistas.udistrital.edu.co/index.php/tia/article/view/18989.

[303] R. Pava-Díaz, S. Gómez-Almeyda y H.-S. Cesar, "Veridoc-Chain: un modelo de identidad digital autosoberana basado en blockchain para una gestión de credenciales académicas segura y privada.", *RCCI.*, vol. 18, n.º 2, 2024. dirección: https://rcci.uci.cu/?journal=rcci&page=article&op=view&path%5B%5D=12838.

DOCTORADO EN INGENIERÍA
FACULTAD DE INGENIERÍA

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

http://doctoradoingenieria.udistrital.edu.co
doctoradoing@udistrital.edu.co

Sede Principal
Carrera 7 No. 40 B - 53 - Bogotá D.C., Colombia
PBX: 3239300 ext 1419 - 1402