Revista Cubana de Ciencias Informáticas
Vol. 18, No. 2, Abril-Julio, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-26

Tipo de artículo: Artículo original

Temática: Tecnologías de la información y las telecomunicaciones

Veridoc-Chain: un modelo de identidad digital autosoberana basado en blockchain para una gestión de credenciales académicas segura y privada

Veridoc-Chain: A Blockchain-Based Self-Sovereign Identity Model for Secure and Private Academic Credential Management

Santiago Gómez-Almeyda [1] https://orcid.org/0009-0004-8281-0978

Roberto Albeiro Pava-Díaz 1* https://orcid.org/0000-0003-0440-892X

Cesar Augusto Hernández-Suarez [1] https://orcid.org/0000-0001-9409-8341

[1] Universidad Distrital Francisco José de Caldas. 111611537. Colombia

*Autor para la correspondencia. (rapavad@udistrital.edu.co)

Editorial "Ediciones Futuro"
Universidad de las Ciencias Informáticas. La Habana, Cuba
rcci@uci.cu

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 2, Abril-Julio, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-26

RESUMEN

Las organizaciones diseñan e implementan procesos para la validación y verificación de cumplimiento de condiciones, como requisito previo para la emisión de una credencial o certificación. Estos procesos se basan usualmente en la recopilación de documentos internos o externos, los cuales deben ser verificados y almacenados preservando la privacidad de los usuarios, mitigando el riesgo de errores y posible colusión por parte de un emisor. En este contexto, la identidad digital autosoberana basada en el uso de identificadores descentralizados permite tener la privacidad por diseño, facilitando el control y la seguridad en la gestión de los atributos de identidad personal junto con las afirmaciones realizadas sobre un usuario, o titular de los derechos de identidad. Finalmente, hemos propuesto un modelo para preservar y verificar criptográficamente los documentos requeridos para la emisión de una certificación académica dentro de una institución universitaria y se implementó un prototipo funcional para su evaluación. El modelo planteado muestra una fuerte protección de la privacidad y una trazabilidad del proceso de validación de documentos.

Palabras clave: blockchain; identificadores descentralizados; credenciales verificables; IPFS; identidad digital autosoberana; veramo.

ABSTRACT

Organizations design and implement processes for the validation and verification of compliance with conditions, as a prerequisite for the issuance of a credential or certification. These processes are usually based on the collection of internal or external documents, which must be verified and stored preserving the privacy of users, mitigating the risk of errors and possible collusion by an issuer. In this context, self-sovereign digital identity based on the use of decentralized identifiers allows for privacy by design, facilitating control and security in the management of personal identity attributes along with the claims made about a user, or owner of the data. identity rights. Finally, we have proposed a model to preserve and cryptographically verify the documents required for the issuance of an academic certification within a university institution and a functional prototype was implemented for its evaluation. The proposed model shows strong privacy protection and traceability of the document validation process.

Editorial "Ediciones Futuro"
Universidad de las Ciencias Informáticas. La Habana, Cuba
rcci@uci.cu

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 2, Abril-Julio, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-26

Keywords: blockchain; decentralized Identifiers; verifiable credentials; IPFS; self-sovereign digital identity; veramo.

Recibido: 11/07/2024
Aceptado: 21/07/2024

Introducción

La sociedad actual se basa en el uso de credenciales verificables para que los individuos puedan probar afirmaciones sobre su identidad. Por ejemplo, demostrar que se posee la competencia para conducir un vehículo requiere portar una credencial denominada licencia de conducción. Cada credencial es generada por un emisor, quién es el responsable de recopilar y validar los documentos que sean necesarios, conforme al marco normativo vigente. Cuando se emita la credencial debe transmitirse al usuario o titular, y se registra en el sistema de información centralizado bajo la gestión del emisor. En este momento, se presenta un interés por la privacidad de los usuarios y la recuperación del control de la información personal, que se encuentra en custodia de cada proveedor de servicios, tendencia impulsada desde el advenimiento de la tecnología de registro distribuido, como blockchain, y su aplicación para el despliegue de un sistema de identidad auto soberana que posibilite al usuario al administración de sus información (atributos de identidad, afirmaciones y credenciales verificables) conforme a los diez principios de identidad propuestos por Christopher Allen (Soltani, 2021). Además, el desarrollo de aplicaciones descentralizadas (DApps) basadas en blockchain se acopla adecuadamente con sistemas de almacenamiento descentralizados como IPFS (Interplanetary File System) (Benet, 2014), (Chen, 2017). En este trabajo se propone un modelo denominado VeriDoc-Chain, para el aseguramiento y verificación de documentos basado en blockchain, con un almacenamiento descentralizado de documentos en IPFS y un sistema de identificación y autenticación que utiliza identificadores descentralizados implementados bajo el meta-sistema SSI de veramo (Veramo, 2016).

Finalmente, este documento está organizado de la siguiente manera: la sección Marco Teórico describe los fundamentos de blockchain, identidad auto soberana, identificadores descentralizados y credenciales verificables, la sección Modelo Propuesto describe la arquitectura propuesta, la sección Implementación y Resultados presenta los detalles de implementación del modelo VERIDOC-CHAIN junto con el resultado obtenido para el caso de estudio objeto de aplicación, y la última sección Conclusiones concluye el artículo.

Marco Teórico

Aspectos fundamentales de la tecnología blockchain

Blockchain se concibe como un registro descentralizado que preserva el total de transacciones realizadas por un grupo de participantes (Pava, 2022). El modelo inicial propuesto por Nakamoto en el 2008 integra un modelo de pseudo-privacidad que permite visualizar las transacciones de forma pseudo-anónima mediante el uso de un identificador seguro y descentralizado y un método de consenso global que garantiza la integridad de la información (Nakamoto, 2008). Las transacciones se agrupan en una estructura llamada bloque, que se verifica por nodos validadores denominados mineros. El primer en nodo en completar la verificación tendrá el derecho de agregar el nodo a la cadena y recibirá como recompensa el token nativo de la respectiva blockchain (Feng, 2019). Una blockchain es lineal, por lo cual los nodos validarán únicamente la cadena más larga. Los principales algoritmos de consenso son: Prueba de trabajo (PoW), prueba de participación (PoS, DPoS, LPoS), prueba de autoridad (PoA), prueba de existencia (PoE), Tolerancia a fallas bizantinas (BFT, dPBFT), prueba de espacio (PoSpace), prueba de importancia (PoI) y prueba de tiempo (PoET) (Pava, 2021). Las características principales de blockchain son: una arquitectura descentralizada, un registro persistente e inmutable, el cual requiere la colusión de la mayoría de sus nodos validadores para alterar un bloque, un modelo de privacidad que permite la visualización pública de cada transacción realizada, por lo cual se presenta como sistema orientado a la auditoría y trazabilidad (Zheng, 2018). Blockchain está fortaleciendo el paradigma de economía colaborativa propiciando la generación de nuevos modelos de negocio que faciliten la desintermediación de los mercados (Davidson, 2018).

Identidad autosoberana

La identidad se define como el conjunto de atributos de una persona, agrupados en perfiles para la interacción con el mundo real, acorde con un contexto de uso (Wang, 2020). La identidad digital se considera un derecho humano fundamental, indispensable para la inclusión social de un individuo, ya que le autoriza el acceso a bienes y servicios (Asamblea general de las Naciones Unidas, 2015). El enfoque de gestión de la identidad se ha dado principalmente bajo un esquema centralizado o federado, que requiere la gestión de un tercero de confianza que administra, controla, monetiza y puede censurar las identidades. Este modelo ha generado afectación en la privacidad, seguridad y libertad de los usuarios (Windley, 2021), (Soltani, 2021), (Haataja, 2017). La identidad digital descentralizada y autosoberana (SSI, por sus siglas en inglés) pretende subsanar los problemas actuales y proveer a la Internet de la capa de identidad ausente en su diseño y evolución. SSI es un nuevo paradigma para gestionar la identidad digital, centrado en el usuario y orientado a otorgar el control y administración de la información personal al titular de los derechos de identidad (Pava, 2023). El diseño de una plataforma SSI se orienta sobre los 10 principios de identidad de Allen (Allen, 2016), (Lockwood, 2021). Los principios se agrupan en tres categorías:

1. Controlabilidad: (1) Existencia de identidad independiente de la representación digital, (2) Control de la información, siendo el usuario la mayor autoridad y (3) Consentimiento para otorgar o denegar acceso a los atributos de identidad personal.
2. Seguridad: (4) Minimización de la información a revelar en una transacción, (5) Persistencia en el tiempo de la identidad, siendo el usuario el único con los privilegios para eliminarla, y (7) Protección de los derechos individuales que preserven la confidencialidad e integridad de la información.
3. Portabilidad: (8) Acceso directo y sin restricciones a la identidad digital, (9) Transparencia en el diseño y administración de las plataformas SSI, y (10) Interoperabilidad que facilite la interacción digital sin restricciones legales o tecnológicas.

Por último, se han diseñado meta-sistemas para el despliegue de aplicaciones descentralizadas con métodos de identificación y autorización autosoberanos. Los principales meta-sistemas son: Sovrin (Windley, 2021), un servicio de identidad autosoberana en un red federada desarrollada en Hyperledger Indy (Hyperledger Foundation, 2022); Veramo (Veamo, 2016), desplegado en la blockchain de Ethereum (Wood, 2014); Jolocom (Jolocom.io, 2020), diseñado sobre Ethereum con persistencia off-chain en IPFS (Benet, 2014); Shocard (Haddouti, 2019), plataforma federada dependiente de la identidad legal del individuo, que se enlaza con la blokchain de bitcoin (Nakamoto, 2008); Litentry (Litentry, 2021), permite la conexión a proveedores externos de datos, y se encuentra disponible en parachains de Polkadot (Polkadot Web3 Foundation, 2017) y Kusama (Web3 Foundation, 2022); Civic (Kuperberg, 2020) ofrece un servicio de identidad, que permite procesos de KYC (Know Your Customer), pero al igual que Shocard requiere de la existencia de una identidad previa; Kilt (BOTLabs GmbH, 2020), es un protocolo desarrollado sobre el framework Parity Substrate (Parity Technologies, 2020) y permite crear, reclamar, emitir, presentar y revocar credenciales verificables; Identity Overlay Network (ION) (Identity Foundation, 2022), implementa el protocolo sidetree (Identity Foundation, 2021) sobre bitcoin, habilitando una Infraestructura de clave pública descentralizada (DPKI); y finalmente, Idena (Iden Network, 2022) es una capa de identidad que asigna reputación a los usuarios con el objetivo de mitigar el ataque sybil.

Identificadores descentralizados

Un identificador descentralizado enlaza una entidad de manera única y global, que no requiere de un tercero de confianza para su asignación y administración. Además, permite asegurar canales de comunicación confiables y persistentes entre dos entidades. El estándar para DIDs fue propuesto por la W3C (World Wide Web Consortium, 2023) y aplica 10 principios de diseño (descentralización, control, privacidad, seguridad, basado en pruebas, visibilidad, interoperabilidad, portabilidad, simplicidad, extensibilidad) enfocados al titular, e implementados bajo un entorno descentralizado (Sporny, 2023). Un DID debe ser de administración descentralizada, con un conjunto reducido de funciones que facilite su comprensión, y que se encuentre bajo el control directo del titular para asegurar la privacidad de la información personal, soportada en pruebas

criptográficas que aseguran la interacción entre dos entidades. Por otro lado, los DIDs deben ser visibles para otras entidades, independientes tecnológicamente (ledger-agnostic), y aplicar estándares que permitan su interoperabilidad y portabilidad. Un DID es un identificador de recursos uniforme (URI) integrado por tres elementos: un esquema, un método DID y un identificador específico y tiene asociado un documento que lo describe (DID - Document DDo) (De Cristo, 2021). El DDo contiene el DID del sujeto, la llave pública, los servicios asociados y los métodos de verificación definidos (Fedrecheski, 2020).

Credenciales verificables

Una credencial verificable (VC) contiene afirmaciones sobre una entidad que se verifican criptográficamente y su utilidad se asemeja a una credencial física (Dib, 2020). El diseño de VCs se basa en la recomendación propuesta por la W3C (Sporny, 2022). La VC es una credencial que se procesa automáticamente, enlazando la identidad de su sujeto a través de su DID (Brunner, 2020), y está formada por tres elementos: un conjunto de afirmaciones o hechos sobre un sujeto, una lista de metadatos asociados a las afirmaciones y las pruebas criptográficas utilizadas en los procesos de validación (Mühle, 2018). El flujo de información en un sistema basado en credenciales verificable se realiza bajo el triángulo de la confianza (Huitema, 2021). Este triángulo se forma por la interacción entre usuario, quién es el titular de los derechos de identidad, un emisor, responsable de generar las credenciales verificables y enviarlas al usuario, y un verificador, quién recibe solicitudes de un usuario y las comprueba criptográficamente. La relación de confianza entre emisor y verificador es transitiva, y se deriva del vínculo basado en criptografía establecido entre emisor y titular.

Modelo propuesto: VeriDoc-Chain

VeriDoc-Chain integra la identidad autosoberana, la tecnología blockchain y el almacenamiento seguro y descentralizado de documentos. Es una solución integral que permite el control y autonomía de las credenciales académicas, mientras garantiza a las instituciones educativas y a terceros una verificación rápida y confiable. Este enfoque revoluciona el paradigma tradicional de certificación académica, proponiendo un

sistema descentralizado, inalterable y orientado hacia la privacidad y autonomía del usuario. A través de VeriDoc-Chain, los usuarios (estudiantes en el caso de estudio) y verificadores interesados, obtienen un entorno de confianza criptográfica que garantiza la integridad y veracidad la información, además, de proporcionar un método de verificación automática respaldado por la inmutabilidad de la tecnología blockchain. VeriDoc-Chain mejora la eficiencia de los procesos, ya que conecta directamente los titulares y emisores, minimizando errores y riesgos de colusión de los participantes, VeriDoc-Chain fue aplicado en una prueba de concepto relacionada con la validación de los requisitos necesarios para obtener un título académico, pero su diseño modular permite la aplicación para asegurar cualquier proceso que involucre la expedición y validación de afirmaciones.

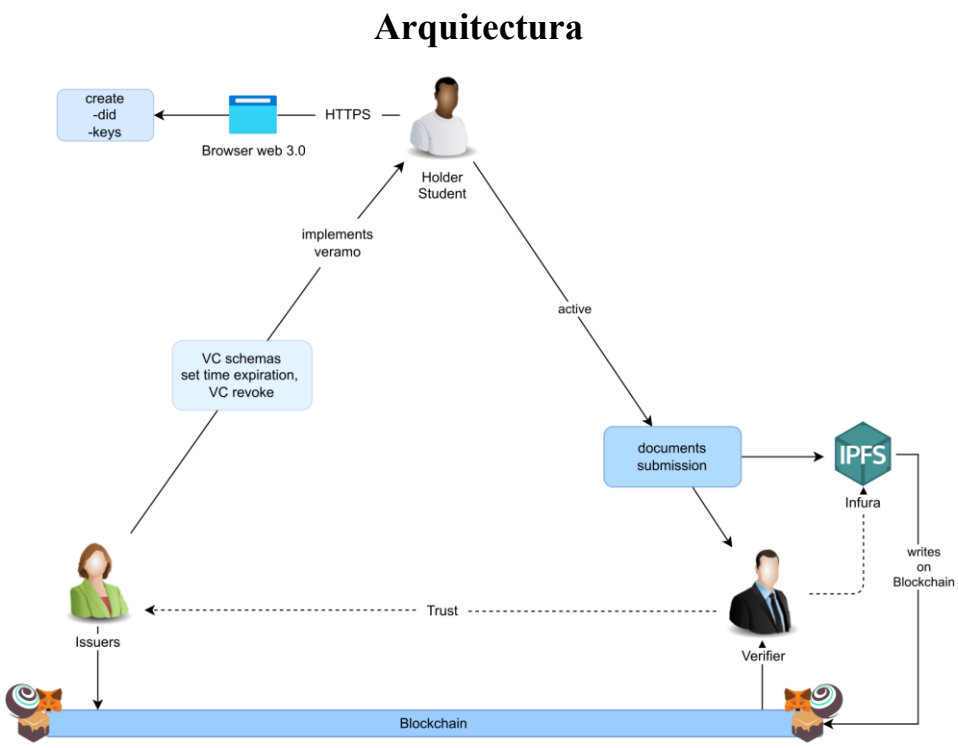

Fig. 1 – Esquema de la arquitectura basada en el paradigma de confianza triangular.

La arquitectura de VeriDoc-Chain se basa en el paradigma de confianza triangular (Davie, 2019), y su diseño se enfocó en la autenticidad, seguridad, y facilidad de uso en la verificación de afirmaciones basadas en documentos. La Figura 1 ilustra el esquema de la arquitectura planteada. La Figura 1 presenta la interacción entre el Holder, quién tendrá el rol de estudiante, conforme al caso de estudio, y es el titular de las credenciales académicas; y un Issuer, responsable de emitir las credenciales verificables solicitadas por un estudiante. En el esquema definido para VCs se cuenta con un tiempo de vigencia, con la posibilidad de revocarla, en caso de ser necesario. Además, se ilustra la interacción cuando un Holder envía el documento a un tercero (Verifier) para su corroboración. Los documentos son cifrados y almacenados en IPFS y se notarizan en la blockchain de Ethereum. Los identificadores descentralizados y la firma de las credenciales se realizaron utilizando el meta-sistema SSI Veramo (Veramo, 2016), por medio de la billetera digital Metamask (Metamask, 2023). En resumen, la arquitectura propuesta es una solución integral para la emisión y verificación de credenciales académicas. Esta solución asegura que las entidades emisoras, como las instituciones académicas, tengan las herramientas necesarias para autenticar y respaldar documentos de forma segura. Al mismo tiempo, brinda a los titulares la autonomía y la confianza para presentar sus credenciales, dado que el proceso de verificación preserva tanto su integridad como su autenticidad.

Por otro lado, dado que VeriDoc-Chain se concibe como un sistema seguro y confiable de verificación basado en blockchain, la Tabla 1 presenta los requerimientos de diseño contemplados para cumplir con estas características. La definición de requerimiento se realizó bajo el marco EARS (Easy approach to requirements syntax) (Mavin, 2009).

Tabla 1 – Requerimientos de VeriDoc-Chain.

Tipo	Descripción
Funcionales	• Generación y gestión de Identidad Digital a través de DIDs (Sporny, 2020) con Veramo (Veramo, 2016). • Carga, entrega y categorización modular de documentos. • Autenticación de documentos vía un registro descentralizado como blockchain y esquemas de credenciales adaptables. • Generación, revocación y almacenamiento descentralizado de Credenciales en un servidor de almacenamiento descentralizado. • Verificación y gestión de DIDs (Sporny, 2020) y VCs (Sporny, 2022) con Veramo en un ambiente web 3.0.
No Funcionales	• Seguridad y confidencialidad aprovechando la inmutabilidad y transparencia blockchain • Interfaz de usuario amigable e intuitiva
Tecnológicos	• Plataforma blockchain tipo Ethereum (Wood, 2014), con un entorno de rápido despliegue como Ganache (Suite, 2023). • Contratos inteligentes implementados en Solidity (Solidity Team, 2023). • Desarrollo y gestión con herramientas Truffle (Suite, 2023). • Diseño de interfaz y experiencia de usuario con React.js (Meta Open Source, 2023). • Conexión e interacción con blockchain vía Web3.js (ChainSafe Systems, 2023). • Generación y gestión de identidad utilizando Veramo (Veramo, 2016). • Almacenamiento descentralizado con Infura (Infura, 2023) y soluciones como IPFS (Benet, 2014).
Seguridad	• Mecanismos sólidos de autenticación y autorización • Cifrado end-to-end para transacciones y almacenamiento.

Entidades de VeriDoc-Chain

El ecosistema de VeriDoc-Chain presenta tres entidades esenciales: Holder, Issuer y Verifier. Estas entidades desempeñan funciones vitales para garantizar un proceso de verificación de credenciales transparente, eficiente y seguro.

Holder: Dada la prueba de concepto se representa como un estudiante dentro de VeriDoc-Chain. El Holder o titular de los derechos de identidad, es el beneficiario y usuario principal del sistema. Sus responsabilidades incluyen:

1. Creación de la Identidad Digital: Genera la identificación única en el ecosistema digital de VeriDoc-Chain mediante Veramo.
2. Introducción de Evidencia: Añadir documentos, tales como registros académicos, para su reconocimiento y validación por parte del Issuer.
3. Manejo de Credenciales Verificables: Recibir y gestionar credenciales verificables cuando se apruebe y autentique su información.

Issuer: Es la entidad responsable de generar y transferir las credenciales verificables. En el caso de estudio se relaciona con una autoridad académica o administrativa dentro de una institución universitaria. Sus funciones son:

1. Revisión de Evidencia: Garantizar que la información presentada por el Holder es auténtica y precisa.
2. Entrega de Credenciales Verificables: Emitir y registrar en la blockchain las credenciales correspondientes tras validar los documentos, y entregarlas al Holder.

Verifier: Es un tercero o entidad Verificadora, cuyo objetivo es validar las credenciales presentadas por un Holder acorde con un contexto de aplicación, como admisiones o procesos laborales. El Verifier actúa comprobando la autenticidad de las mismas mediante las pruebas criptográficas registradas. Sus tareas son:

1. Petición de Credenciales: Solicitar al Holder evidencias o logros académicos en forma de credenciales verificables.
2. Comprobación de Autenticidad: Hacer uso de las herramientas de VeriDoc-Chain y la tecnología blockchain para confirmar la integridad y veracidad de las credenciales compartidas por el Holder.

El fluido intercambio y cooperación entre estas entidades consolidan a VeriDoc-Chain como un sistema robusto y confiable para la verificación de documentos en un mundo cada vez más digital.

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 2, Abril-Julio, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-26

Fases de VeriDoc-Chain

El sistema se ha dividido en las siguientes cuatro fases.

- Fase 1: Establecimiento de la Identidad digital. La primera tarea que desarrolla una entidad es la generación de su identidad digital. Se generan los Identificadores Descentralizados (DID) junto con las claves asociadas. Esta identidad es la columna vertebral del sistema y actúa como la representación única y segura de una entidad.
- Fase 2: Entrega de Documentos. Una vez se dispone de la identidad digital, el Holder se encuentra habilitado para la entrega confiable de documentos. Este proceso es flexible y admite una variedad de documentos, desde atestaciones oficiales hasta credenciales verificables auto-emitidas.
- Fase 3: Integración y Almacenamiento Descentralizado. La arquitectura de VeriDoc-Chain utiliza esquemas de credenciales verificables adaptables. Esto permite una fácil revocación de credenciales cuando sea necesario. El almacenamiento descentralizado se realiza a través de un nodo IPFS administrado por Infura. Las credenciales, una vez emitidas y verificadas, se almacenan en el nodo de Infura, que integra soluciones como IPFS y almacenamiento basado en Ethereum (Infura, 2023).
- Fase 4: Gestión y Verificación con Veramo. La última fase es responsable de la gestión y verificación de DIDs y VCs, bajo el meta-sistema de Veramo. Esta plataforma SSI facilita la interacción del usuario y asegura una verificación rápida y confiable (Veramo, 2023). Además, los usuarios la interacción de los usuarios es mediante un navegador web 3.0, garantizando un acceso seguro a través de HTTPS.

Implementación y Resultados

Caso de estudio

Se tomó como caso de estudio la validación de los requisitos de grado, en la facultad de ingeniería de la Universidad Distrital Francisco José de Caldas, Bogotá D.C, Colombia. Actualmente el proceso se realiza de manera manual presentando limitaciones, como costos operativos elevados, posibles errores humanos y demoras en la validación (Gómez, 2023). En respuesta a estos retos, se propone VeriDoc-Chain, una solución

Editorial "Ediciones Futuro"
Universidad de las Ciencias Informáticas. La Habana, Cuba
rcci@uci.cu

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 2, Abril-Julio, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-26

automatizada basada en blockchain. El sistema planteado busca optimizar el proceso de revisión al automatizar la verificación de documentos como pruebas SABER PRO, registros en la plataforma académica, certificados de paz y salvo, entre otros. Al utilizar la tecnología blockchain, no solo se mejora la eficiencia sino también se garantiza la autenticidad y seguridad de cada documento y requisito presentado.

Componentes de VeriDoc-Chain

VeriDoc-Chain destaca por su diseño arquitectónico modular, integrado por 5 componentes. En (Gómez, 2023) se detalla la información de diseño y se encuentra disponible el código fuente.

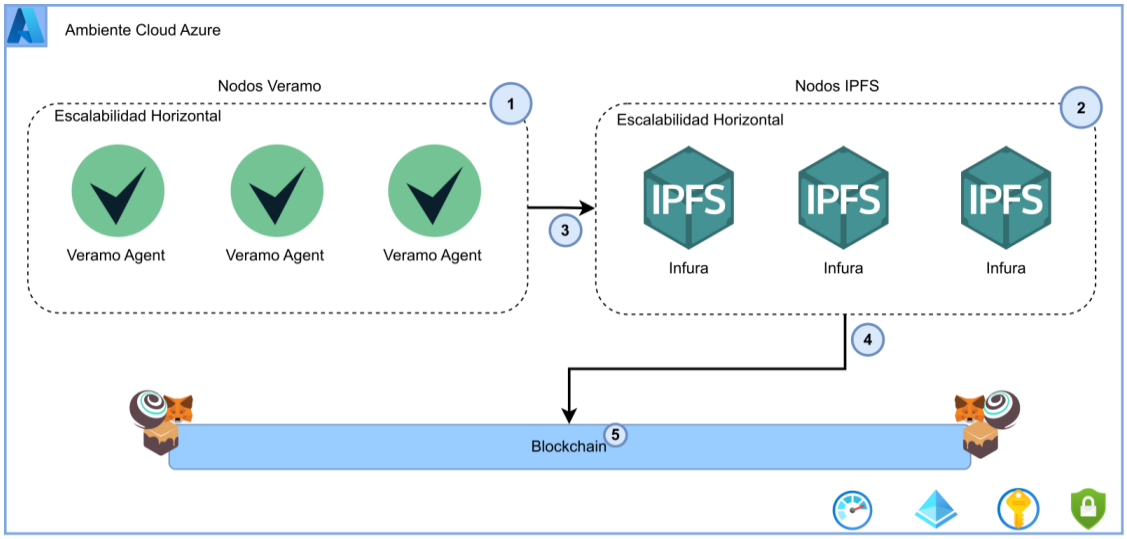

Fig. 2 – Representación gráfica de la infraestructura de nodos y componentes de VeriDoc-Chain.

Descripción de los componentes

La Figura 2 ilustra la integración de los componentes en la infraestructura general.

1. Componentes asociados a Veramo
    a. Veramo Agent Server: Es un servidor basado en Express.js, enfocado en modularidad y protección.

Editorial "Ediciones Futuro"
Universidad de las Ciencias Informáticas. La Habana, Cuba
rcci@uci.cu

Presenta un fuerte acoplamiento con SQLite, pero enfatiza en un cifrado robusto, gracias al secreto KMS X25519 raw private key y políticas CORS (World Wide Web Consortium (W3C), 2023)

b. Veramo Interface Client: Enlaza el sistema con el Veramo Agent Server, y provee desde la inicialización de DIDs hasta el control de comunicaciones encriptadas.

2. Componentes de Infura/IPFS
    a. Secure File Loader: Permite a los usuarios la carga de archivos, y se enfoca en el cifrado y tratamiento de datos antes de su transferencia a IPFS.
    b. Credential Verification Suite: Encargado de administrar y autenticar las identidades y credenciales de usuarios en el ecosistema. Utiliza IPFS para alojamiento y aplica cifrado para garantizar seguridad en sus operaciones.

3. Componentes asociados a la interacción entre Veramo e IPFS/Infura
    a. Firebase Request Handler: Se sirve de Firebase (Google developers, 2023) para el almacenamiento y gestión de peticiones vinculadas con la emisión y presentación de datos. Aunque los datos se sitúan en Firebase, se prioriza el cifrado de la información sensible.
    b. User Registration Interface: Fusiona el mecanismo de generación de DIDs con las funcionalidades de autenticación de Firebase, asegurando un sistema unificado de registro y autenticación de usuarios.

4. Componentes asociados en la relación e interacción entre IPFS/Infura y blockchain
    a. Blockchain Interaction Toolkit: Simplifica las operaciones asociadas a los datos cifrados y a la interacción con la blockchain, incorporando funciones criptográficas de Veramo con habilidades para el manejo y recuperación de datos.
    b. Document Issuance Manager: Se ocupa de coordinar y visualizar procedimientos relacionados con la emisión o denegación de documentos, ensamblando servicios externos y operaciones backend de forma cohesiva y segura.

c. Requirement Handling Interface: Centrado en el tratamiento y autenticación de documentos de identidad digital, este módulo gestiona, cifra y coordina solicitudes de confirmación tanto en la cadena de bloques como en Firebase.

5. Componentes asociados a blockchain
   a. Blockchain VC Storage Contract: Este contrato inteligente se encarga del control y registro del hash calculado para las Credenciales Verificables y sus presentaciones en blockchain, asentando su autenticidad e integridad.

Evolución de VeriDoc-Chain a través de sus Fases

VeriDoc-Chain tuvo un desarrollo iterativo e incremental, donde en cada fase se garantiza la adecuada implementación y funcionalidad de cada uno de los componentes del sistema. A continuación, se presentan ilustraciones que evidencian las operaciones más significativas de cada fase.

Fase 1: Establecimiento de la Identidad Digital

La creación de la identidad digital es el primer paso para cualquier entidad dentro del sistema. Durante esta fase, se generan los Identificadores Descentralizados (DID) y las claves asociadas, actuando como la representación única y segura de una entidad en VeriDoc-Chain. La Figura 3 presenta un subconjunto de identidades creadas, detallando el DID, método, marcas de tiempo y controlador.

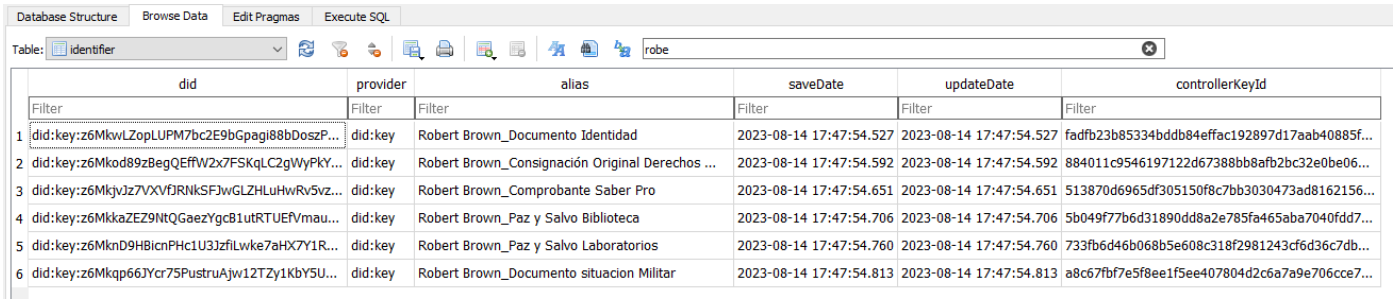
Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: identifier — robe

	did	provider	alias	saveDate	updateDate	controllerKeyId
1	did:key:z6MkwLZopLUPM7bc2E9bGpagi88bDoszP...	did:key	Robert Brown_Documento Identidad	2023-08-14 17:47:54.527	2023-08-14 17:47:54.527	fadfb23b85334bddb84effac192897d17aab40885f...
2	did:key:z6Mkod89zBegQEffW2x7FSKqLC2gWyPkY...	did:key	Robert Brown_Consignación Original Derechos ...	2023-08-14 17:47:54.592	2023-08-14 17:47:54.592	884011c9546197122d67388bb8afb2bc32e0be06...
3	did:key:z6MkjvJz7VXVfJRNkSFJwGLZHLuHwRv5vz...	did:key	Robert Brown_Comprobante Saber Pro	2023-08-14 17:47:54.651	2023-08-14 17:47:54.651	513870d6965df305150f8c7bb3030473ad8162156...
4	did:key:z6MkkaZEZ9NtQGaezYgcB1utRTUEfVmau...	did:key	Robert Brown_Paz y Salvo Biblioteca	2023-08-14 17:47:54.706	2023-08-14 17:47:54.706	5b049f77b6d31890dd8a2e785fa465aba7040fdd7...
5	did:key:z6MknD9HBicnPHc1U3JzfiLwke7aHX7Y1R...	did:key	Robert Brown_Paz y Salvo Laboratorios	2023-08-14 17:47:54.760	2023-08-14 17:47:54.760	733fb6d46b068b5e608c318f2981243cf6d36c7db...
6	did:key:z6Mkqp66JYcr75PustruAjw12TZy1KbY5U...	did:key	Robert Brown_Documento situacion Militar	2023-08-14 17:47:54.813	2023-08-14 17:47:54.813	a8c67fbf7e5f8ee1f5ee407804d2c6a7a9e706cce7...

Fig. 3 – Establecimiento de la identidad digital en VeriDoc-Chain.

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 2, Abril-Julio, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-26

Fase 2: Entrega de Documentos

Mediante su identidad digital el Holder puede comenzar con la entrega confiable de documentos, adaptando el proceso a diferentes tipos de documentos que pueden ser atestados o auto-emitidos. La Figura 4 muestra la aprobación requerida desde la billetera de Metamask para ejecutar la transacción de carga de un documento.

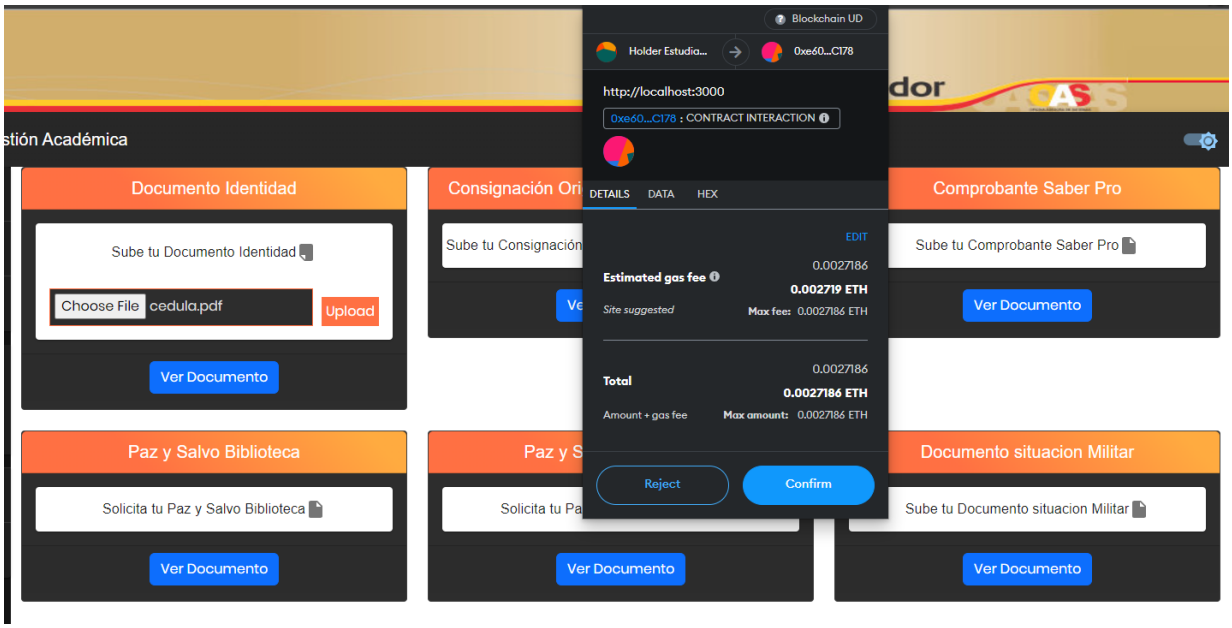

Fig. 4 – Proceso de entrega de documentos en VeriDoc-Chain.

Fase 3: Integración y Almacenamiento Descentralizado

La Figura 5 ilustra la interface de consulta de documentos almacenados, los cuales son obtenidos del nodo IPFS a través de Infura y descrifados para su visualización por parte de la entidad autorizada.

Editorial "Ediciones Futuro"
Universidad de las Ciencias Informáticas. La Habana, Cuba
rcci@uci.cu

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 2, Abril-Julio, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-26

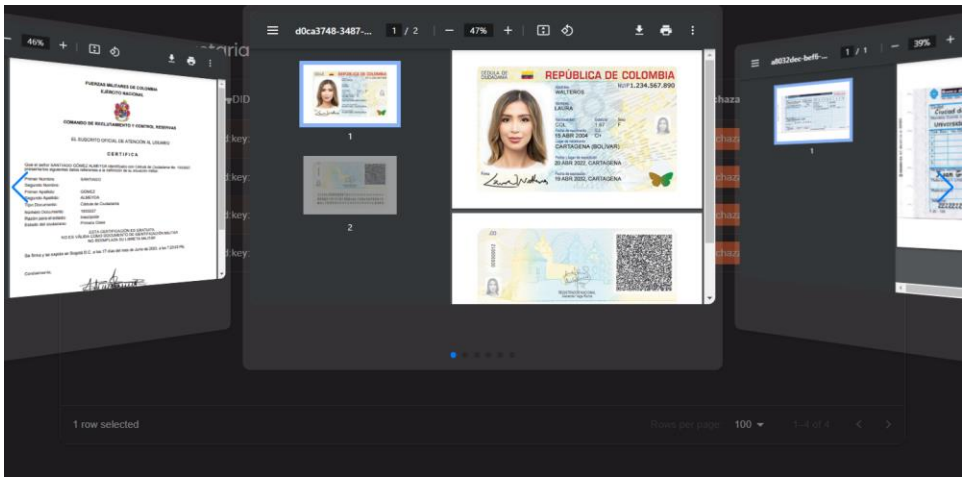

Fig. 5 – Integración y almacenamiento descentralizado en VeriDoc-Chain.

Fase 4: Gestión y Verificación con Veramo

Por último, el proceso finaliza con la verificación de los DIDs y las VCs, con el objeto de emitir la credencial final de aprobación de requisitos de grado. La Figura 6 muestra la lista de chequeo que se implementó para indicar la aprobación de cada documento.

Fig. 6 – Gestión y verificación en VeriDoc-Chain con Veramo.

Editorial "Ediciones Futuro"
Universidad de las Ciencias Informáticas. La Habana, Cuba
rcci@uci.cu

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 2, Abril-Julio, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-26

Gasto Computacional de VeriDoc-Chain

El sistema de VeriDoc-Chain conlleva costos computacionales asociados al consumo de gas en cada transacción, debido al proceso de validación por parte de los nodos de la red. Aunque esto refuerza la integridad y seguridad de la información, presenta desafíos en cuanto a eficiencia y costos operativos. La visualización del consumo de recursos se presenta en la Figura 7 que muestra el gasto computacional asociado con diferentes operaciones en VeriDoc-Chain.

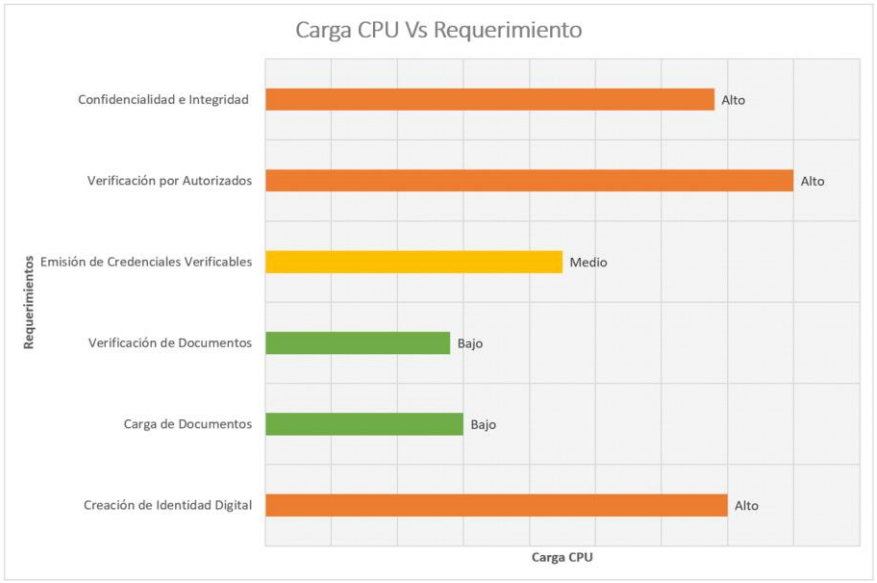

Fig. 7 – Gasto computacional asociado con diferentes operaciones en VeriDoc-Chain.

Este gráfico destaca las operaciones que requieren más recursos, siendo las de mayor costo la verificación por autoridades designadas y el proceso de cifrado de documentos antes de guardarlos. En términos de costos, la Figura 8 refleja el costo asociado al despliegue de los contratos inteligentes, tomando una cotización de ETH a 1729.07 USD. Se recomienda una optimización para disminuir el gas consumido.

Revista Cubana de Ciencias Informáticas
Vol. 18, No. 2, Abril-Julio, 2024
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 1-26

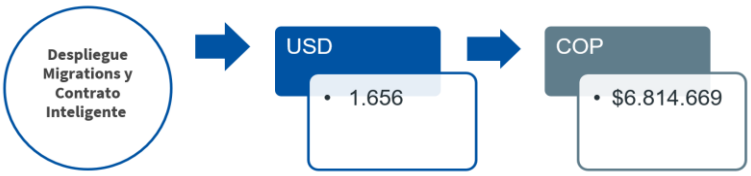

Fig. 8 – Costos asociados con el despliegue de contratos en VeriDoc-Chain.

Además, en la Figura 9 se discrimina el consumo de gas para las funciones de almacenamiento y presentación de VCs.

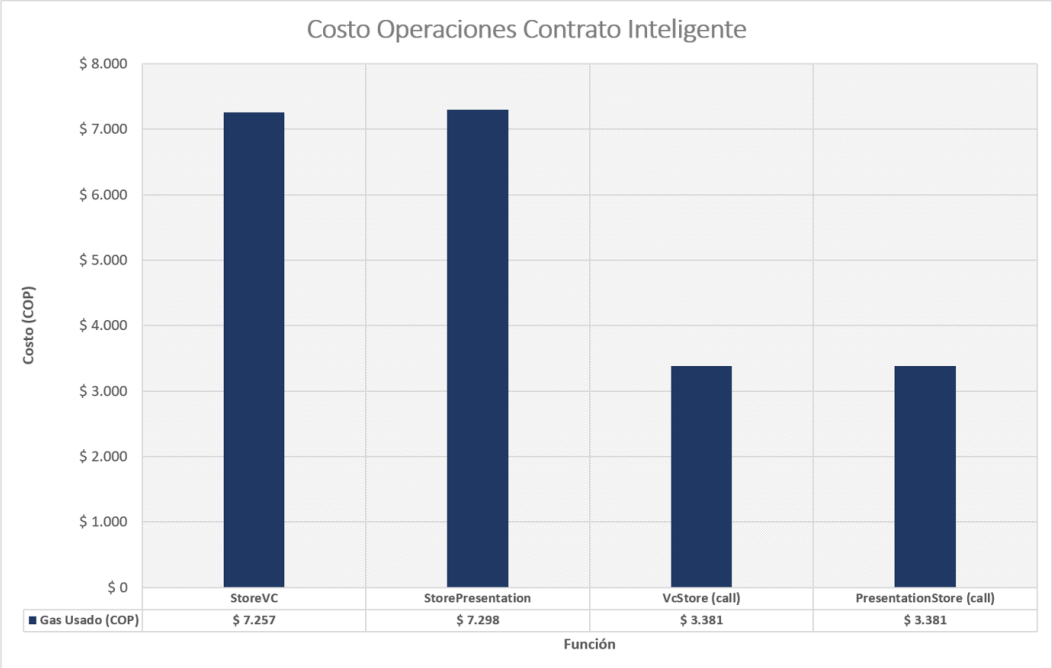

Fig. 9 – Gasto de gas por operación en VeriDoc-Chain.

En resumen, es importante tener en cuenta estos costos y analizar constantemente el código en pro de optimizar el sistema para garantizar que VeriDoc-Chain sea eficiente y económico.

Editorial "Ediciones Futuro"
Universidad de las Ciencias Informáticas. La Habana, Cuba
rcci@uci.cu

Impacto y Mejoras en la Validación de Credenciales con VeriDoc-Chain

VeriDoc-Chain se ha destacado como una herramienta vital que simplifica y acelera la verificación de credenciales académicas, demostrando su valor al abordar eficientemente los problemas asociados con los métodos manuales convencionales. Aunque se ha evaluado en un contexto hipotético en la Universidad Distrital Francisco José de Caldas, los resultados sugieren una notable reducción en los tiempos de espera y los costos operativos. Los estudiantes se beneficiarían de un proceso más fluido y preciso, libre de trámites administrativos prolongados y errores humanos comunes. Aunque el análisis del gasto computacional subraya la eficiencia de VeriDoc-Chain, su impacto real se observa en la rápida identificación y corrección de errores, como discrepancias menores en los nombres, facilitadas por la transparencia de la blockchain. Esta eficiencia no solo promete acelerar el proceso de graduación, sino que también reduce la ansiedad y las incertidumbres asociadas con los retrasos en la validación. Así, VeriDoc-Chain no solo optimiza la eficiencia computacional, sino que también eleva la experiencia de validación de credenciales, estableciendo un nuevo estándar de eficiencia, transparencia y confiabilidad en el entorno académico.

Conclusiones

VeriDoc-Chain representa una evolución significativa en la manera en que una institución educativa gestiona y verifica los requisitos de grado, ofreciendo un sistema más transparente, eficiente y seguro. Además, en el contexto de las organizaciones actuales, VeriDoc-Chain emerge como un innovador modelo centrado en la autenticación y validación de identidad digital, con blockchain como la infraestructura subyacente. Este estudio subraya la importancia de procesos robustos para la validación y verificación de documentos necesarios antes de emitir credenciales o certificaciones. Con Identificadores Descentralizados y apoyados en la emisión de credenciales comprobables, se propone una gestión de identidad altamente confiable y prioriza la privacidad por diseño. La estrategia descentralizada de manejo y protección de documentos, específicamente a través del cifrado en IPFS, refuerza la seguridad y privacidad, protegiendo la información contra posibles errores o actos malintencionados.

Por otro lado, la propuesta de VeriDoc-Chain no sólo se limita a la teoría, sino que se ha llevado a cabo una extensa caracterización y adaptación a los marcos normativos relevantes, demostrando su aplicabilidad en instituciones como la Universidad Distrital Francisco José de Caldas y más allá. Esta generalización, que contempla la recopilación y verificación de documentos tanto internos como externos, valida la importancia de la elección adecuada de blockchain y contratos inteligentes para garantizar integridad y autenticidad. Las simulaciones y pruebas evidencian la robustez y eficiencia del modelo, subrayando su adaptabilidad y pertinencia en diferentes escenarios organizacionales. Por último, la adopción de VeriDoc-Chain refuerza el potencial y la viabilidad de las directrices de identidad descentralizada del W3C en la práctica real. Al integrar el principio del "triángulo de confianza", este modelo garantiza una autenticación confiable, una privacidad mejorada y la integridad de los documentos. En una era donde la identidad digital autosoberana es cada vez más relevante, VeriDoc-Chain se erige como una solución pionera, que no sólo responde a las demandas actuales, sino que también sienta las bases para futuras adaptaciones y evoluciones en el ámbito de la identidad y verificación digital.

Referencias

Gomez, Santiago A. 2023. Prototipo De Una Dapp Para Tesis De Verificación De Requisitos De Grado En La Universidad Distrital. [Online]. Github. Disponible En: Https://Github.Com/20161020503/Dapp-Prototype-Thesis.

Allen, Christopher. 2016. Self-Sovereign Identity Principles. [Online]. Disponible En: Https://Github.Com/Weboftrustinfo/Self-Sovereign-Identity/Blob/Master/Self-Sovereign-Identity-Principles.Md. [Consultado El 6 Mayo 2022].

Asamblea General De Las Naciones Unidas. 2015. Transformar Nuestro Mundo: La Agenda 2030 Para El Desarrollo Sostenible. [Online]. Disponible En: Https://Www.Unfpa.Org/Sites/Default/Files/Resource-Pdf/Resolution_A_Res_70_1_Sp.Pdf. [Consultado El 5 Mayo 2020].

Benet, Juan. 2014. Ipfs - Content Addressed, Versioned, P2p File System. [Online]. Disponible En: Https://Arxiv.Org/Abs/1407.3561. [Consultado El 16 Mayo 2022].

Botlabs Gmbh. 2020. Kilt Protocol - White Paper. [Online]. Disponible En: Https://Www.Kilt.Io/Wp-Content/Uploads/2020/01/Kilt-White-Paper-V2020-Jan-15.Pdf. [Consultado El 23 Mayo 2022].

Brunner, Clemens; Gallersdörfer, Ulrich; Knirsch, Fabian; Engel, Dominik; Matthes, Florian. 2020. Did And Vc: Untangling Decentralized Identifiers And Verifiable Credentials For The Web Of Trust. En: 3rd International Conference On Blockchain Technology And Applications (Icbta 2020). Acm, Págs. 61-66. Isbn 9781450388962. Disponible En: Doi: 10.1145/3446983.3446992.

Chainsafe Systems. 2023. Web3.Js: A Javascript Library For Building On Ethereum. [Online]. Disponible En: Https://Web3js.Org/. [Consultado El 23 Julio 2023].

Chen, Yongle; Li, Hui; Li, Kejiao; Zhang, Jiyang. 2017. An Improved P2p File System Scheme Based On Ipfs And Blockchain. En: 2017 Ieee International Conference On Big Data (Big Data). Vol. 2018-January, Págs. 2652-2657. Disponible En: Doi: 10.1109/Bigdata.2017.8258226.

Davidson, Sinclair; Filippi, Primavera De; Potts, Jason. 2018. Blockchains And The Economic Institutions Of Capitalism. Journal Of Institutional Economics. Vol. 14, Págs. 639-658. Issn 17441382. Disponible En: Doi: 10.1017/S1744137417000200.

Davie, Matthew; Gisolfi, Dan; Hardman, Daniel; Jordan, John; O'donnell, Darrell; Reed, Drummond. 2019. The Trust Over Ip Stack. Ieee Communications Standards Magazine. Vol. 3, N.O 4, Págs. 46-51.

De Cristo, Flaviene Scheidt; Shbair, Wazen M.; Trestioreanu, Lucian; State, Radu; Malhotra, Aanchal. 2021. Self-Sovereign Identity For The Financial Sector: A Case Study Of Paystring Service. En: 2021 Ieee International Conference On Blockchain (Blockchain), Págs. 213-220. Disponible En: Doi: 10.1109/Blockchain53845.2021.00036.

Dib, O.; Toumi, K. 2020. Decentralized Identity Systems: Architecture, Challenges, Solutions And Future Directions. Annals Of Emerging Technologies In Computing. Vol. 4, N.O 5, Págs. 19-40. Disponible En: Doi: 10.33166/Aetic.2020.05.002.

Fedrecheski, Geovane; Rabaey, Jan M.; Costa, Laisa C.P.P.; Ccori, Pablo C. Calcina; Pereira, William T.; Zuffo, Marcelo K. 2020. Self-Sovereign Identity For Iot Environments: A Perspective. En: Giots 2020 -

Global Internet Of Things Summit, Proceedings. Ieee. Isbn 9781728121710. Disponible En: Doi: 10.1109/Giots49054.2020.9119664.

Feng, Qi; He, Debiao; Zeadally, Sherali; Khan, Muhammad Khurram; Kumar, Neeraj. 2019. A Survey On Privacy Protection In Blockchain System. Journal Of Network And Computer Applications. Vol. 126, Págs. 45-58. Issn 10958592. Disponible En: Doi: 10.1016/J.Jnca.2018.10.020.

Google Developers. 2023. Firebase: Make Your App The Best It Can Be. [Online]. Disponible En: Https://Firebase.Google.Com/. [Consultado El 16 Mayo 2023].

Haataja, Samuli. 2017. The 2007 Cyber Attacks Against Estonia And International Law On The Use Of Force: An Informational Approach. Law, Innovation And Technology. Vol. 9, N.O 2, Págs. 159-189. Issn 1757997x. Disponible En: Doi: 10.1080/17579961.2017.1377914.

Haddouti, Samia El; Ech-Cherif El Kettani, M. Dafir. 2019. Analysis Of Identity Management Systems Using Blockchain Technology. En: 2019 International Conference On Advanced Communication Technologies And Networking (Commnet). Vol. 10, Págs. 1-7. Disponible En: Doi: 10.1109/Commnet.2019.8742375.

Huitema, Carly; Jordan, John; Bachenheimer, Daniel; Bendixsen, Lynn; O'donnell, Darrell; Subrahmanyam, P.A.; Reed, Drummond; Mukhopadhyay, Sankarshan; Jacques, Judith Fleenor; Perry, Scott; Syntez, Victor; Young, Kaliya; Hand, Karen; Malhotra, Vikas; Chu, Wenjing; Kneiss, Karl. 2021. Introduction To Trust Over Ip. [Online]. Mayo 2020. Trust Over Ip Foundation. Disponible En: Https://Trustoverip.Org/Wp-Content/Uploads/Introduction-To-Toip-V2.0-2021-11-17.Pdf

Hyperledger Foundation. 2022. Hyperledger Indy. [Online]. Disponible En: Https://Github.Com/Hyperledger/Indy-Sdk. [Consultado El 16 Junio 2022].

Idena Network. 2022. Idena: Proof-Of-Person Blockchain. [Online]. Disponible En: Https://Github.Com/Idena-Network. [Consultado El 30 Septiembre 2022].

Identity Foundation. 2021. Sidetree Protocol. [Online]. Disponible En: Https://Github.Com/Decentralized-Identity/Sidetree. [Consultado El 20 Mayo 2022].

Identity Foundation. 2022. The Identity Overlay Network (Ion). [Online]. Disponible En: Https://Github.Com/Decentralized-Identity/Ion. [Consultado El 30 Septiembre 2022].

Infura. 2023. Infura Documentation. [Online]. Disponible En: Https://Docs.Infura.Io/. [Consultado El 16 Mayo 2023].

Jolocom.Io. 2020. Jolocom: Own Your Digital Self. [Online]. Disponible En: Https://Github.Com/Jolocom. [Consultado El 17 Mayo 2022].

Kuperberg, Michael. 2020. Blockchain-Based Identity Management: A Survey From The Enterprise And Ecosystem Perspective. Ieee Transactions On Engineering Management. Vol. 67, N.O 4, Págs. 1008-1027. Disponible En: Doi: 10.1109/Tem.2019.2926471.

Litentry Technologies. 2021. Litentry Network. [Online]. Disponible En: Https://Docs.Litentry.Com/Parachain/Get-Started/Litentry-Network. [Consultado El 17 Mayo 2022].

Lockwood, Mick. 2021. An Accessible Interface Layer For Self-Sovereign Identity. Frontiers In Blockchain. Vol. 3. Issn 2624-7852. Disponible En: Doi: 10.3389/Fbloc.2020.609101.

Mavin, Alistair; Wilkinson, Philip; Harwood, Adrian; Novak, Mark. 2009. Easy Approach To Requirements Syntax (Ears). En: 2009 17th Ieee International Requirements Engineering Conference. Ieee, Págs. 317-322.

Meta Open Source. 2023. React: The Library For Web And Native User Interface. [Online]. Disponible En: Https://React.Dev/. [Consultado El 23 Julio 2023].

Metamask. 2023. A Crypto Wallet & Gateway To Blockchain Apps. [Online]. Disponible En: Https://Metamask.Io/. [Consultado El 16 Mayo 2023].

Mühle, Alexander; Grüner, Andreas; Gayvoronskaya, Tatiana; Meinel, Christoph. 2018. A Survey On Essential Components Of A Self-Sovereign Identity. Computer Science Review. Vol. 30, Págs. 80-86. Issn 15740137. Disponible En: Doi: 10.1016/J.Cosrev.2018.10.002.

Nakamoto, Satoshi. 2008. Bitcoin: A Peer-To-Peer Electronic Cash System. [Online]. Disponible En: Http://Bitcoin.Org/Bitcoin.Pdf. [Consultado El 20 Mayo 2022].

Parity Technologies. 2020. Parity Substrate: Build Your Own Blockchain. [Online]. Disponible En: Https://Www.Parity.Io/Technologies/Substrate/. [Consultado El 23 Mayo 2022].

Pava, Roberto; Lopez, Danilo; Niño, Luis; Paez, Rafael. 2022. Tecnología De Registro Distribuido (Dlt): Características Y Escenarios De Aplicación. Tecnología Investigación Y Academia. Vol. 9, N.O 1. Disponible En: Https://Revistas.Udistrital.Edu.Co/Index.Php/Tia/Article/View/18989.

Pava, Roberto; Paez, Rafael; Niño, Luis. 2023. A Bibliometric Study Of Scientific Production On Self-Sovereign Identity. Ingeniería. Vol. 28, N.O Supl. Disponible En: Doi: 10.14483/23448393.19656.

Pava, Roberto; Perez, José; Niño, Luis Fernando. 2021. 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. Issn 0123-921x. Disponible En: Doi: 10.14483/22487638.16159.

Solidity Team. 2023. Solidity. [Online]. Disponible En: Https://Soliditylang.Org/. [Consultado El 23 Junio 2023].

Soltani, R.; Nguyen, U.T.; An, A. 2021. A Survey Of Self-Sovereign Identity Ecosystem. Security And Communication Networks. Vol. 2021. Disponible En: Doi: 10.1155/2021/8873429.

Sporny, Manu; Longley, Dave; Chadwick, David. 2022. Verifiable Credentials Data Model V1.1. [Online]. Disponible En: Https://Www.W3.Org/Tr/Vc-Data-Model/. [Consultado El 9 Junio 2021].

Sporny, Manu; Longley, Dave; Sabadello, Markus; Reed, Drummond; Steele, Orie; Allen, Christopher. 2020. Decentralized Identifiers (Dids) V1.0. Core Architecture, Data Model, And Representations. [Online]. Disponible En: Https://Www.W3.Org/Tr/Did-Core/. [Consultado El 7 Junio 2021].

Suite, Truffle. 2023. Ganache: One Click Blockchain. [Online]. Disponible En: Https://Www.Trufflesuite.Com/Ganache. [Consultado El 16 Mayo 2023].

Veramo. 2016. Veramo Core Development: Tools For Verifiable Data And Ssi. [Online]. Disponible En: Https://Github.Com/Uport-Project/. [Consultado El 16 Mayo 2022].

Veramo. 2023. Veramo Documentation. [Online]. Disponible En: Https://Veramo.Io/Docs/Basics/Introduction. [Consultado El 16 Mayo 2023].

Wang, Fennie; De Filippi, Primavera. 2020. Self-Sovereign Identity In A Globalized World: Credentials-Based Identity Systems As A Driver For Economic Inclusion. Frontiers In Blockchain. Vol. 2. Issn 2624-7852. Disponible En: Doi: 10.3389/Fbloc.2019.00028.

Web3 Foundation. 2017. Polkadot: Vision For A Heterogeneous Multi-Chain Framework. [Online]. Disponible En: Https://Polkadot.Network/Polkadotpaper.Pdf. [Consultado El 27 Septiembre 2022].

Web3 Foundation. 2022. Kusama: Polkadot's Canary Network. [Online]. Disponible En: Https://Guide.Kusama.Network/Docs/Kusama-Getting-Started. [Consultado El 27 Septiembre 2022].

Windley, Phillip J. 2021. Sovrin: An Identity Metasystem For Self-Sovereign Identity. Frontiers In Blockchain. Vol. 4. Issn 2624-7852. Disponible En: Doi: 10.3389/Fbloc.2021.626726.

Wood, Gavin. 2014. Ethereum: A Secure Decentralised Generalised Transaction Ledger. [Online]. Disponible En: Https://Github.Com/Ethereum/Yellowpaper. [Consultado El 16 Mayo 2022].

World Wide Web Consortium. 2023. Making The Web Work. [Online]. Disponible En: Https://Www.W3.Org/. [Consultado El 16 Mayo 2023].

World Wide Web Consortium (W3c). 2023. Cross-Origin Resource Sharing (Cors). [Online]. Disponible En: Https://Www.W3.Org/Tr/Cors/. [Consultado El 16 Mayo 2023].

Zheng, Zibin; Xie, Shaoan; Dai, Hong-Ning; Chen, Xiangping; Wang, Huaimin. 2018. Blockchain Challenges And Opportunities: A Survey. International Journal Of Web And Grid Services. Vol. 14, N.O 4, Págs. 352-375. Disponible En: Doi: 10.1504/Ijwgs.2018.095647.

Conflicto de interés

El autor autoriza la distribución y uso de su artículo.

Contribuciones de los autores

Conceptualización: Santiago Gómez-Almeyda, Roberto Albeiro Pava-Díaz

Análisis formal: Santiago Gómez-Almeyda, Roberto Albeiro Pava-Díaz, Cesar Augusto Hernández-Suarez

Investigación: Santiago Gómez-Almeyda, Roberto Albeiro Pava-Díaz, Cesar Augusto Hernández-Suarez

Metodología: Santiago Gómez-Almeyda, Roberto Albeiro Pava-Díaz

Administración del proyecto: Roberto Albeiro Pava-Díaz

Supervisión: Cesar Augusto Hernández-Suarez

Validación: Nombre y Apellidos del autor

Visualización: Nombre y Apellidos del autor

Redacción – borrador original: Santiago Gómez-Almeyda, Roberto Albeiro Pava-Díaz

Redacción – revisión y edición: Santiago Gómez-Almeyda, Roberto Albeiro Pava-Díaz, Cesar Augusto Hernández-Suarez.