Aplicación de Blockchain para proteger la autenticidad de los registros académicos

Jose Luis Del Valle M.

Máster en Ciberseguridad y Privacidad
Sistemas de Blockchain

Nombre Tutor/a de TF
Profesor Alberto Ballesteros Rodríguez
Profesor/a responsable de la asignatura
Profesor Víctor García Font

Fecha Entrega
Enero, 2024

Universitat Oberta
de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Aplicación de Blockchain para proteger la autenticidad de los registros académicos.* *Un enfoque descentralizado para proteger la autenticidad de los registros académicos*
Nombre del autor:	*José Luis Del Valle Mejías*
Nombre del consultor/a:	*Alberto Ballesteros Rodríguez*
Nombre del PRA:	*Profesor Víctor García Font*
Fecha de entrega	*01/2024*
Titulación o programa:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Sistemas de Blockchain*
Idioma del trabajo:	*Castellano*
Palabras clave:	*Hyperledger, Credenciales Verificables, Identificadores Descentralizados*

Resumen del Trabajo

El uso de tecnología blockchain ofrece un enfoque descentralizado y seguro para proteger la integridad y privacidad de los datos. En el entorno escolar, la aplicación de blockchain puede ser especialmente relevante para garantizar la autenticidad de los registros académicos, la protección de la privacidad de los estudiantes y la reducción de fraudes en la emisión de certificados y calificaciones. Este trabajo se centra en explorar cómo blockchain puede ser implementado en las escuelas para fortalecer la seguridad de los datos de estudiantes y proporcionar un sistema de almacenamiento descentralizado y de verificación confiable. Asimismo, se busca desarrollar una prueba de concepto que permita confirmar la factibilidad de una implementación con estas características. Por último, este trabajo intentará evaluar la seguridad, privacidad y habilidad para prevenir fraudes mediante la verificación manual de credenciales, la revisión de la configuración de privacidad de la plataforma seleccionada y pruebas de acceso no autorizado.

Abstract

The use of blockchain technology offers a decentralized and secure approach to protecting the integrity and privacy of data. In the educational environment, the application of blockchain can be particularly relevant to ensure the authenticity of academic records, protect the privacy of students, and reduce fraud in the issuance of certificates and grades. This work focuses on exploring how blockchain can be implemented in schools to strengthen the security of student data and provide a decentralized and reliable verification storage system. It also aims to develop a proof of concept to confirm the feasibility of an implementation with these characteristics. Finally, this work will try to assess security, privacy, and the ability to prevent fraud through manual verification of credentials, review of the privacy settings of the selected platform, and tests of unauthorized access.

Índice

Lista de figuras

1. Introducción

La falsificación de credenciales educativas es un problema creciente en los Estados Unidos y en todo el mundo. Este fenómeno se refiere al acto de crear, modificar o utilizar de manera fraudulenta documentos educativos, como diplomas, certificados y registros de calificaciones, con el propósito de obtener beneficios indebidos, como el acceso a puestos de trabajo que requieren cualificaciones específicas o la admisión en instituciones académicas que requieren de dichas credenciales como requisito de ingreso (Michael J. Stevens, 2018). Esta práctica ha venido socavando la credibilidad del sistema educativo y está planteando una serie de desafíos tanto para las instituciones educativas como para los empleadores. Según Stevens y VanDerhei (2018), la falsificación de credenciales educativas es un problema global que tiene un impacto significativo en los individuos, las instituciones educativas y la sociedad en general.

Garantizar la integridad y privacidad de estos datos se ha convertido en un desafío esencial para las instituciones educativas en un mundo cada vez más interconectado. En el pasado reciente, han estudiado diversas formas de atacar el problema. Brown, Stevens y VanDerhei (Brown, 2019) revisaron las medidas de seguridad utilizadas para prevenir la falsificación de credenciales educativas. En su estudio, se identificaron tres grupos de medidas:

- Medidas de seguridad físicas: Estas medidas incluyen el uso de materiales de alta calidad, la impresión de hologramas o marcas de agua, y la firma digital.
- Medidas de seguridad administrativas: Estas medidas incluyen el control de acceso a los archivos de credenciales, la realización de auditorías periódicas, y la educación de los empleados sobre el fraude de credenciales.
- Medidas de seguridad tecnológicas: Estas medidas incluyen el uso de software de detección de falsificación, la verificación de identidad en línea, y la integración de las credenciales educativas en un sistema de gestión de aprendizaje.

Sin embargo, otras tecnologías, como es el caso de blockchain han emergido como una solución prometedora. Originaria como el motor detrás de las criptomonedas, blockchain es un registro descentralizado e inmutable que garantiza la seguridad y la integridad de los datos almacenados en él. Singh, Singh y Sharma (Anshuman Singh, 2021) presentaron una solución basada en blockchain para detectar la falsificación de credenciales educativas. En su trabajo la solución utiliza la tecnología blockchain para almacenar y verificar de forma segura la información de las credenciales educativas y funciona de la siguiente forma:

- La institución educativa registra la información de la credencial educativa en la cadena de bloques.
- El solicitante de empleo presenta la credencial educativa a un empleador.

- El empleador verifica la autenticidad de la credencial educativa utilizando un software de verificación de blockchain.
- El software de verificación de blockchain compara la información de la credencial educativa con la información almacenada en la cadena de bloques. Si la información coincide, la credencial educativa se considera auténtica.

Haciendo pruebas prácticas para evaluar la eficacia de la solución, el estudio encontró que la solución fue capaz de detectar el 99% de las credenciales educativas falsificadas.

En línea con el trabajo de Singh, Singh y Sharma, este trabajo tiene como objetivo explorar cómo blockchain se puede implementar en el entorno educativo para garantizar la autenticidad de las credenciales mientras se protegen los datos personales de los estudiantes, mediante un sistema de validación y verificación confiable.

Iniciaremos revisando en los fundamentos de la tecnología blockchain, destacando las características que la hacen particularmente adecuada para abordar las preocupaciones de autenticidad en el ámbito educativo. Además, examinaremos casos de uso, estudios académicos y proyectos piloto que han demostrado el potencial de la aplicación de esta tecnología en escuelas, universidades y sistemas educativos en general.

A lo largo de este trabajo, se analizarán las ventajas y desafíos que surgen al implementar blockchain en el sector educativo, abordando cuestiones técnicas, legales y de adopción. Asimismo, se realizará un diseño de arquitectura para un sistema de este tipo, mostrando las partes componentes de una posible solución y las relaciones entre ellas.

Finalmente se propondrán recomendaciones prácticas basadas en la experiencia recopilada para mejorar la aplicación de blockchain en la seguridad de datos en las escuelas.

En un momento en que la privacidad y la integridad de los datos son esenciales para el funcionamiento efectivo de las instituciones educativas, esta investigación busca arrojar luz sobre cómo blockchain puede convertirse en un pilar fundamental para proteger la autenticidad de las credenciales que dichas instituciones generan.

1.1. Contexto y justificación del Trabajo

El presente trabajo pretende realizar una propuesta factible que redunde en la protección de la integridad de las credenciales generadas por el sistema educativo y en garantizar que dichas credenciales sean auténticas y legítimas. Simultáneamente, este trabajo busca proteger la privacidad de los estudiantes al evitar el acceso no autorizado a sus registros académicos.

El anterior es un problema relevante debido a su impacto negativo en la relación de confianza entre las instituciones educativas, los empleadores, el gobierno y la sociedad en general. La falsificación de credenciales socava la confianza en la educación y pone en riesgo la credibilidad de los títulos y certificados legítimos.

Aunque actualmente este problema se está abordando mediante el uso de tecnología, en general están siendo aplicadas por instituciones de educación superior o colegios profesionales, y son almacenadas de forma centralizada y por ende vulnerables ante posibles ataques cibernéticos.

En general, este trabajo busca proporcionar una comprensión práctica de cómo blockchain puede utilizarse para abordar el problema de la verificación de credenciales y que arroje luz sobre las ventajas y desafíos de la implementación de blockchain en el espacio de las escuelas públicas del condado Miami-Dade. Además, se espera que el diseño de una arquitectura de sistema basado en blockchain pueda servir como un punto de partida para futuras implementaciones prácticas.

1.2. Objetivos del Trabajo

- Investigar casos de uso existentes y estudios relacionados con la aplicación de blockchain en la seguridad de datos en escuelas y otros entornos educativos.
- Definir y diseñar una solución blockchain adecuada para garantizar la autenticidad, integridad y privacidad de registros académicos de los estudiantes, específicamente, los títulos emitidos por una institución educativa del condado Miami-Dade
- Desarrollar un prototipo de la solución blockchain diseñada.
- Evaluar la eficacia de la solución blockchain en términos de seguridad, privacidad y prevención de fraudes en los registros académicos.
- Analizar las ventajas y desafíos de la implementación de la solución desarrollada en este trabajo, dentro del entorno educativo.
- Proponer recomendaciones para la mejora de la solución blockchain y su integración efectiva en el sistema educativo, considerando aspectos prácticos y de sostenibilidad.

1.3 Impacto en sostenibilidad, ético-social y de diversidad

Al permitir la verificación digital y segura de títulos académicos, se reduce la necesidad de imprimir y distribuir documentos en papel, lo que contribuye a la reducción del consumo de recursos naturales y la emisión de gases de efecto invernadero asociados con la producción de papel. Asimismo, la implementación de sistemas blockchain en instituciones educativas puede mejorar la eficiencia administrativa al reducir la carga de trabajo asociada con la verificación manual de credenciales haciendo la actividad administrativa asociada más sostenible.

La adopción de soluciones basadas en blockchain para la emisión y verificación de credenciales promueve la transparencia y la confianza en el sistema educativo lo cual es esencial para garantizar que los logros académicos se basen en mérito y competencia. Por último, la verificación de títulos basada en

blockchain puede ser especialmente útil para estudiantes y profesionales que han obtenido títulos en instituciones extranjeras facilitando la validación de cualificaciones internacionales y promoviendo la diversidad cultural y la movilidad académica y laboral.

Respecto al tema de consumo energético y su correspondiente impacto ambiental, al usar una blockchain como plataforma es importante tomar en cuenta su huella energética. Para el desarrollo del presente trabajo se prevé usar una blockchain que, en contraste con Bitcoin, utilice un enfoque diferente para el consenso y no se base en un algoritmo de Prueba de Trabajo (*Proof of Wo*rk, PoW), que es reconocido como de muy alto consumo energético por la naturaleza de la prueba criptográfica que usa para validar transacciones y generar bloques nuevos en la blockchain (Johnston, 2017). En lugar de PoW, en este trabajo se buscará utilizar una blockchain que use el enfoque conocido como Prueba de Autoridad (*Proof of Authority*, PoA). Según Tang, (Tang, 2017) PoA es el algoritmo más eficiente en términos de energía y costo, y también es el más seguro contra ataques.

En PoA, la validación de bloques y la generación de nuevos bloques no dependen de la resolución de algoritmos matemáticos intensivos que requieran una gran cantidad de potencia de cómputo y, por lo tanto, energía. En cambio, los nodos de la red son operados por actores de confianza que se llaman "autoridades" y se les otorga el derecho a validar y crear bloques basados en su identidad y reputación en lugar de resolver desafíos criptográficos costosos en términos de energía.

1.4 Enfoque y método seguido.

En el presente trabajo se utilizará una metodología de investigación denominada Investigación Mixta (John W. Creswell, 2018), que combina métodos cuantitativos y cualitativos. Esta metodología incorpora las ventajas de ambos métodos permitiendo flexibilidad al investigador, especialmente en casos de ingeniería aplicada, sin detrimento en el rigor científico. (Abbas Tashakkori, 2010)

Los métodos a utilizar serán:

- La revisión de la literatura relevante, actualizada y confiable en el campo de blockchain y sus aplicaciones en las áreas abordadas en este trabajo, incluyendo literatura académica, artículos científicos publicados en revistas indexadas, y publicaciones en internet cuya fuente pueda considerarse confiable.
- El diseño de una solución, su implementación y la posterior recopilación de datos sobre la seguridad, privacidad y habilidad para prevenir fraudes.
- Análisis de los datos recopilados para evaluar validez de la solución implementada.

Estos métodos permitirán obtener una comprensión completa de la solución basada en blockchain debido a que son particularmente útiles para abordar preguntas complejas que no pueden ser respondidas adecuadamente por métodos cuantitativos o cualitativos por sí solos. (Alexander, 2012)

En este trabajo se seguirán las siguientes etapas:

- Revisión de la literatura (académica, científica y técnica) sobre la aplicación de blockchain en el ámbito educativo, haciendo especial énfasis en la revisión de aquellos casos de uso que ilustren las tareas que sería necesario ejecutar.
- Exploración de las diferentes tecnologías de blockchain permisionadas disponibles para la realización del presente trabajo y que cumplen con las características deseadas de privacidad y seguridad.
- Diseño y desarrollo de una solución que demuestre la viabilidad de implementar blockchain en el ámbito educativo para la validación de títulos académicos, mediante el uso de Identificadores Descentralizados (DIDs) y credenciales verificables (VCs)
- Recopilación de datos sobre la solución implementada y su seguridad, privacidad y habilidad para prevenir fraudes.
- Análisis de los datos recopilados para evaluar la validez de la solución.

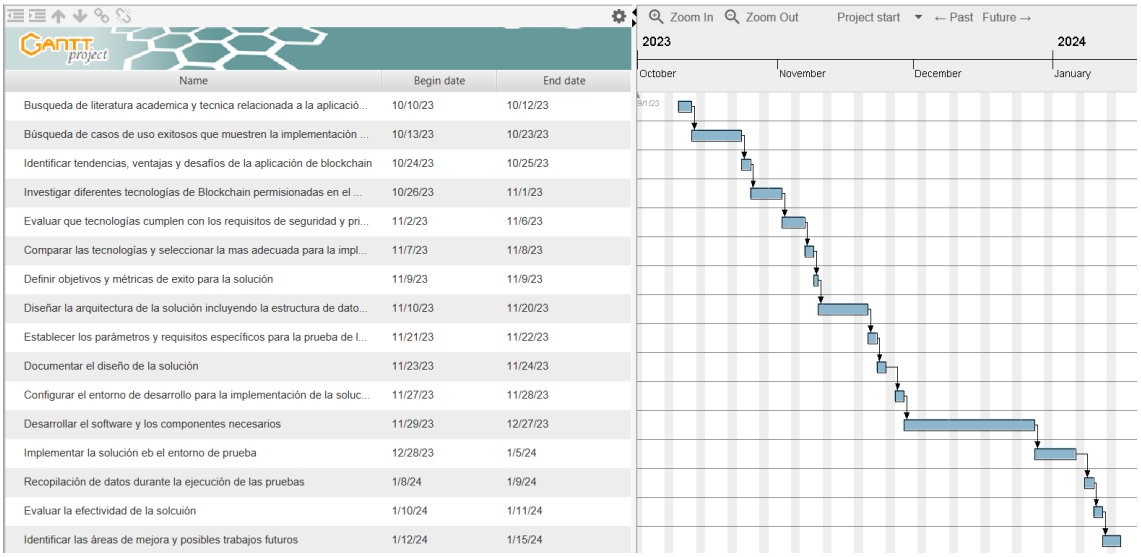
1.5 Planificación del Trabajo

La ejecución del presente trabajo se realizará en seis etapas, iniciando con una revisión de literatura científica, académica y técnica sobre la aplicación de blockchain en el ámbito educativo y se investigarán casos de uso existentes y estudios relacionados con la aplicación de blockchain en la seguridad de datos en escuelas y otros entornos educativos. Se evaluarán diferentes soluciones basadas en blockchain permisionadas que se adecúen a los objetivos del trabajo y se revisarán los pasos necesarios su utilización.

Posteriormente se definirá y diseñará una solución blockchain que cumpla con los objetivos propuestos en el trabajo, y se describirá detalladamente la solución adoptada, los elementos que la componen, así como las relaciones entre ellos. Para ello se explorarán aquellas cadenas de bloques que tengan como objeto principal la emisión y mantenimiento de Identificadores Descentralizados y Credenciales Verificables. Se explorarán, entre otras, Hyperledger Indy, Sovrin y Civic, que son plataformas de identidad descentralizada que utilizan la tecnología blockchain para crear un sistema de identificación y verificación de identidades y verificación de credenciales.

Se implementará la solución, validando su funcionamiento y se realizarán sobre ella pruebas que permitan determinar que cumple con los requisitos de seguridad e integridad requeridos. Por último, se analizarán los resultados obtenidos con el objeto de llegar a conclusiones y recomendaciones que permitan, en futuros trabajos, mejorar la solución desarrollada.

Una lista detallada de las tareas a realizar, en la forma de un diagrama de Gantt, se muestra a continuación.



Name	Begin date	End date
Busqueda de literatura academica y tecnica relacionada a la aplicació...	10/10/23	10/12/23
Búsqueda de casos de uso exitosos que muestren la implementación ...	10/13/23	10/23/23
Identificar tendencias, ventajas y desafíos de la aplicación de blockchain	10/24/23	10/25/23
Investigar diferentes tecnologías de Blockchain permisionadas en el ...	10/26/23	11/1/23
Evaluar que tecnologías cumplen con los requisitos de seguridad y pri...	11/2/23	11/6/23
Comparar las tecnologías y seleccionar la mas adecuada para la impl...	11/7/23	11/8/23
Definir objetivos y métricas de exito para la solución	11/9/23	11/9/23
Diseñar la arquitectura de la solución incluyendo la estructura de dato...	11/10/23	11/20/23
Establecer los parámetros y requisitos específicos para la prueba de l...	11/21/23	11/22/23
Documentar el diseño de la solución	11/23/23	11/24/23
Configurar el entorno de desarrollo para la implementación de la soluc...	11/27/23	11/28/23
Desarrollar el software y los componentes necesarios	11/29/23	12/27/23
Implementar la solución eb el entorno de prueba	12/28/23	1/5/24
Recopilación de datos durante la ejecución de las pruebas	1/8/24	1/9/24
Evaluar la efectividad de la solcuión	1/10/24	1/11/24
Identificar las áreas de mejora y posibles trabajos futuros	1/12/24	1/15/24

Figura 1: Diagrama de Gantt del Proyecto
Elaboración Propia

1.6 Breve sumario de productos obtenidos

Como resultado del presente trabajo, se obtendrán los siguientes productos:

1. Revisión de la Literatura (Etapa 1):
    - Informe de revisión de literatura (académica, artículos científicos publicados en revistas reconocidas y en internet) que proporcione una visión integral de la aplicación de blockchain en la educación.
    - Identificación de casos de uso específicos que ilustran cómo blockchain se ha implementado en entornos educativos.
2. Exploración de Tecnologías de Blockchain (Etapa 2):
    - Documento que evalúa diferentes tecnologías de blockchain permisionadas y su idoneidad para el proyecto.
    - Selección de una tecnología de blockchain específica de DIDs y VCs para su implementación en el ámbito educativo.
3. Diseño de la solución (Etapa 3):
    - Plan de diseño detallado de la solución, incluyendo su arquitectura.
    - Documentación de los parámetros y requisitos necesarios para llevar a cabo pruebas de seguridad y privacidad.
4. Desarrollo de la Solución (Etapa 4):
    - Implementación de la solución en un entorno de prueba.
    - Desarrollo de software y componentes necesarios, como contratos inteligentes si fuera necesario.

5. Recopilación de Datos (Etapa 5):

    - Información relacionada con la capacidad de la solución desarrollada para preservar la privacidad de los datos y la gestión de identidades de los usuarios.

6. Análisis de Resultados (Etapa 6):

    - Análisis de la efectividad de la solución blockchain en términos de seguridad, privacidad y prevención de fraudes.
    - Conclusiones basadas en los resultados de la prueba de concepto, incluyendo áreas de mejora y desafíos identificados.

1.7 Análisis de Requerimientos

La implementación de un sistema descentralizado de validación de credenciales académicas implica los siguientes requerimientos técnicos:

a. Una Infraestructura de red blockchain para identidades y credenciales.

    a. Nodos: Se deben configurar los nodos que participen en la red. Estos nodos se encargarán de la gestión de identidades y validación de credenciales.
    b. Las instituciones educativas, los estudiantes y otros participantes deben crear *Decentralized Identifiers* o DIDs. Un DID es una identidad digital única y descentralizada que permite a las partes interactuar de manera segura en la red.

b. Los emisores de credenciales:

    a. Instituciones Educativas: Las instituciones que emiten credenciales académicas deben ser identificadas y registradas en la red. Cada institución necesita su identidad en la red.
    b. Cada institución educativa, creará su propio DID y actuará como la entidad emisora de credenciales.

c. Un proceso de emisión de credenciales:

    a. Formato Estándar de Credenciales: Se definirá un formato estándar para las credenciales académicas siguiendo el estándar *W3C Verifiable Credentials (VCs)*.
    b. Emisión de Credenciales: Las instituciones deben emitir credenciales académicas firmadas digitalmente utilizando su identidad en la red y el formato estándar.

d. Un proceso de publicación de credenciales: Las credenciales emitidas deben ser publicadas en la red, permitiendo a los estudiantes acceder a ellas y presentarlas para su verificación.

e. Definición de los entes verificadores de credenciales. Será necesario definir quiénes serán los verificadores de credenciales como, por ejemplo, empleadores u otras instituciones educativas. Dado que las credenciales académicas emitidas se estructurarán como Credenciales Verificables (VCs) siguiendo el estándar W3C, cada credencial incluirá información sobre la institución que lo emite, la fecha de su emisión, logros académicos del estudiante y su firma digital.

f. Seguridad: La seguridad de la red es esencial para proteger las identidades y las credenciales. Se seleccionará una red de blockchain que, por diseño, garantice la protección de la información en ella almacenada.

1.8 Breve descripción de los otros capítulos de la memoria.

En el capítulo dos se describirán los aspectos más relevantes del diseño y desarrollo del trabajo, así como la metodología elegida para realizar este desarrollo, describiendo las alternativas posibles, las decisiones tomadas, y los criterios utilizados para tomar estas decisiones. En el tercer capítulo se detallarán los resultados obtenidos durante el desarrollo de la prueba de concepto o solución implementada. Por último, el capítulo cuatro proporciona una visión general de las conclusiones y reflexiones clave derivadas de la investigación realizada en este trabajo:

- Se resumen las conclusiones clave que se derivan de los resultados obtenidos en el estudio.
- Se discute si los resultados cumplen con las expectativas iniciales o si han revelado hallazgos importantes.
- Se proporciona una explicación de por qué los resultados son importantes en el contexto de la investigación sobre la aplicación de blockchain en la educación.
- Se analiza si se ha seguido la planificación inicial y si la metodología utilizada fue adecuada para alcanzar los objetivos, así como si fue necesario introducir cambios en la planificación o la metodología para garantizar el éxito del trabajo, y se proporciona una justificación.
- Se evalúa si los impactos ético-sociales, de sostenibilidad y de diversidad se han mitigado (en caso de ser negativos) o logrado (en caso de ser positivos) como resultado del trabajo.
- Y por último se proponen futuras líneas de investigación o posteriores trabajos que permitan ahondar en el desarrollo de aplicaciones de blockchain en la veracidad, privacidad y seguridad de credenciales académicas.

2. Revisión de la Literatura

En el presente capítulo, se realizará una exhaustiva revisión de la literatura con el propósito de establecer una base sólida para comprender los fundamentos esenciales de las tecnologías emergentes en el campo de blockchain y la descentralización. Aquí, se explorarán de manera detallada conceptos clave, en el mundo de blockchain, sistemas de identificación descentralizada, credenciales verificables y los variados protocolos de consenso que sustentan estas innovadoras soluciones. Asimismo, este capítulo aborda conceptos introductorios sobre sistemas de blockchain cuyo propósito exclusivo es el de proveer una plataforma para el desarrollo de aplicaciones de identificación descentralizada y credenciales verificables en línea, como son Hyperledger Indy y Sovrin.

2.1 Sistemas de Blockchain

Los sistemas de blockchain han surgido como una innovación revolucionaria en el ámbito de la tecnología de la información y la seguridad de datos. Estos sistemas se basan en una estructura de registro distribuido que permite la creación de bases de datos inmutables y transparentes, lo que los convierte en un elemento fundamental en una amplia gama de aplicaciones. Desde su concepción en el documento fundacional de Satoshi Nakamoto en 2008, titulado *"Bitcoin: A Peer-to-Peer Electronic Cash System,"* los sistemas de blockchain han evolucionado significativamente y se han diversificado en múltiples verticales, trascendiendo su aplicación inicial en criptomonedas.

La tecnología de blockchain es un fenómeno de relevancia histórica, comparable a la invención de Internet en términos de su potencial transformador. Este sistema de registro distribuido se ha convertido en elogiado y debatido a nivel mundial debido a su capacidad para redefinir la forma en que se gestionan los activos digitales y se garantiza la integridad de la información. A medida que la sociedad se adentra en la era digital, la necesidad de un sistema de confianza descentralizado se ha vuelto imperativa, y los sistemas de blockchain se presentan como una solución revolucionaria.

En esencia, un sistema de blockchain es una base de datos distribuida que registra transacciones de forma segura y transparente. Cada bloque de datos se vincula al anterior mediante criptografía, formando una cadena inmutable de información. La característica más distintiva de los sistemas de blockchain es su resistencia a la modificación y su descentralización, lo que los hace altamente seguros y confiables.

2.2 Evolución de Blockchain y sus aplicaciones

En el campo financiero, los sistemas de blockchain han allanado el camino para la creación de activos digitales, tokens no fungibles (NFT) y sistemas de liquidación más eficientes. Además, han impulsado la creación de soluciones de financiamiento descentralizado (DeFi) que permiten a los usuarios prestar, pedir prestado y ganar intereses sin la necesidad de intermediarios tradicionales.

Las aplicaciones de blockchain también se extienden a la gestión de la cadena de suministro, donde se utiliza para rastrear y verificar la autenticidad de los productos, garantizando la transparencia y la trazabilidad en cada etapa de la cadena. En la atención médica, los registros médicos electrónicos basados en blockchain garantizan la integridad de los datos y la privacidad del paciente.

La tecnología Blockchain, una de las mayores innovaciones del siglo 21, ha tenido un impacto significativo en varios sectores, desde el financiero hasta la manufactura y la educación. Aunque su popularidad comenzó a crecer hace unos años, la historia de Blockchain se remonta a principios de los años 90. Stuart Haber y W. Scott Stornetta tuvieron la visión de lo que muchas personas han llegado a conocer como blockchain en 1991. Su primer trabajo consistió en trabajar en una cadena de bloques protegida criptográficamente en la que nadie podía manipular las marcas de tiempo de los documentos. En 1992, actualizaron su sistema para incorporar árboles de Merkle que mejoraban la eficiencia, lo que permitía la recopilación de más documentos en un solo bloque. Es en 2008 que la historia de Blockchain comienza a ganar relevancia, gracias al trabajo de una persona o grupo con el nombre de Satoshi Nakamoto. Nakamoto conceptualizó el primer blockchain en 2008, desde donde la tecnología ha evolucionado y se ha desarrollado en muchas aplicaciones más allá de las criptomonedas. Nakamoto lanzó el primer informe sobre la tecnología en 2009. Desde entonces, la tecnología blockchain ha evolucionado más allá de las simples transacciones entre pares. Las innovaciones han llevado a que se construyan aplicaciones descentralizadas (*DApps*) sobre la cadena de bloques, y han aumentado las soluciones para velocidades y seguridad.

La primera aplicación de tecnología blockchain fue la criptomoneda bitcoin. Al proporcionar transparencia, responsabilidad, inmutabilidad y seguridad, la blockchain desencadenó la afluencia de más criptomonedas. Con el tiempo, en irrumpieron los contratos inteligentes, ampliando la funcionalidad de esta tecnología más allá de las criptomonedas, como fue el caso de los *Non Fungible Tokens* o *NFTs*, los sistemas de votación, de subasta, etc. Los contratos inteligentes ofrecen un gran atractivo porque no son alterables de forma ilegítima, reducen el coste de la verificación, la excepción, el arbitraje y la protección contra el fraude, admiten la ejecución automatizada sin necesidad de permisos y permiten el registro transparente de datos de modo fácilmente verificable.

2.3 Algoritmos de Consenso

Los sistemas de blockchain emplean varios métodos de validación de bloques, también llamados Algoritmos de Consenso, para garantizar la seguridad y la integridad de la cadena de bloques. Estos métodos varían en términos de seguridad, eficiencia y consumo de energía, y son fundamentales para entender cómo funcionan las diferentes cadenas de bloques. A continuación, analizaremos algunos de los métodos de validación más comunes, destacando sus ventajas y desventajas, con un enfoque particular en el consumo de energía.

2.3.1 Prueba de Trabajo (*Proof of Work - PoW*)

La Prueba de Trabajo es el método de validación más conocido y se utiliza en blockchains como Bitcoin y Ethereum. En PoW, los nodos de la red compiten para resolver un rompecabezas criptográfico complejo, y el primero en encontrar una solución válida tiene el derecho de agregar un bloque a la cadena y recibe una recompensa en forma de criptomonedas. Este método ha demostrado ser altamente resistente a ataques y manipulaciones debido a su costo computacional, además, permite que cualquiera pueda unirse a la red y contribuir.

Sin embargo, el proceso de minería PoW es intensivo en energía, lo que ha generado preocupaciones ambientales. La red de Bitcoin consume una cantidad significativa de energía. Según el *Bitcoin Electricity Consumption Index* de la Universidad de Cambridge, se estima que Bitcoin consume aproximadamente 70,4 Tera watts por hora (TWh) de electricidad al año en 2023. Esto es más que muchos países y alrededor del 0.54% del consumo mundial de electricidad (Centro de Finanzas Alternativas de la Universidad de Cambridge, 2023). Asimismo, este método puede enfrentar problemas de escalabilidad debido a la lenta velocidad de procesamiento de transacciones.

2.3.2 Prueba de Participación (*Proof of Stake - PoS*)

La Prueba de Participación es un método alternativo utilizado por redes blockchain como *Cardano* y *Polkadot*. En PoS, los validadores son elegidos para proponer y validar bloques basados en la cantidad de criptomonedas que poseen y están dispuestos a "apostar" como garantía. Este método consume significativamente menos energía en comparación con PoW, ya que no requiere la resolución de rompecabezas criptográficos y puede ser más escalable, ya que no hay competencia intensiva de minería. Pero, por otro lado, PoS puede llevar a una mayor centralización de la riqueza, ya que aquellos con más criptomonedas tienen más influencia en la red.

2.3.3 Prueba de Autoridad (*Proof of Authority - PoA*)

La Prueba de Autoridad se utiliza en redes blockchain privadas y consorcios, como Quorum. En PoA, un conjunto de nodos autorizados son los únicos que pueden validar bloques. La autoridad de estos nodos se basa en la confianza. PoA es extremadamente eficiente en términos de consumo de energía y al haber un control centralizado, PoA puede ser muy rápido y escalable. Sin embargo, la centralización inherente a PoA puede generar preocupaciones sobre la confiabilidad y la resistencia a ataques maliciosos, y sacrifica la descentralización en favor de la eficiencia y la confiabilidad.

2.3.4 *Byzantine Fault Tolerance* (BFT)

El algoritmo de consenso de blockchain conocido como BFT, o Byzantine Fault Tolerance, es un algoritmo que permite que una red de nodos llegue a un acuerdo sobre el estado de una blockchain, incluso si algunos de los nodos son maliciosos o están fallando.

BFT funciona mediante la selección de un líder entre los nodos de la red. El líder es responsable de proponer nuevos bloques para la blockchain. Los demás nodos de la red verifican la validez del bloque propuesto por el líder. Si el bloque es válido, los demás nodos lo agregan a la blockchain. En el caso de que un nodo sea malicioso o esté fallando, los demás nodos pueden detectarlo y excluirlo de la red. Esto ayuda a garantizar que la blockchain sea segura y confiable (Michael K. Reiter, 2015).

BFT es un algoritmo tolerante a fallas bizantinas, lo que significa que puede resistir ataques de nodos maliciosos o que estén fallando; es un algoritmo seguro, ya que los bloques solo se agregan a la blockchain si son válidos y es un algoritmo eficiente, ya que los bloques se agregan a la blockchain de manera rápida y sencilla. Sin embargo, requiere un número relativamente grande de nodos para funcionar correctamente y puede ser costoso implementar y mantener.

2.3.5 Robust Byzantine Fault Tolerance (RBFT)

En el contexto de blockchain, una falla bizantina es una situación en la que un nodo de la red se comporta de manera maliciosa o incorrecta. Esto puede incluir enviar información falsa o incorrecta, o negarse a participar en el consenso. El término "falla bizantina" se deriva de un problema matemático propuesto por Leslie Lamport en 1982. En este problema, un grupo de generales bizantinos deben decidir si atacar o retirarse. Sin embargo, algunos de los generales pueden ser traidores y enviar información falsa. El algoritmo de consenso debe garantizar que la decisión tomada sea correcta, incluso si algunos de los generales son traidores (Lamport, 1982).

El algoritmo RBFT, o *Robust Byzantine Fault Tolerance*, es un algoritmo de consenso de blockchain que es tolerante a fallas bizantinas. RBFT es una variante de BFT. RBFT es un algoritmo más robusto que BFT porque puede soportar un mayor número de fallas. En particular, RBFT puede soportar hasta una tercera parte de los nodos de la red que sean maliciosos o estén fallando (Hui Zhang, 2022). En un sistema basado en RBFT, se mantiene un registro ordenado de transacciones replicado en el ledger (libro), los participantes del sistema que mantienen este registro se denominan nodos, y los nodos ejecutan el protocolo de consenso RBFT para acordar el orden de las transacciones. De forma simplifica, se puede suponer que uno de los nodos es el líder (primario) que determina el orden de las transacciones y lo comunica al resto de los nodos (seguidores).

Cada ejecución (*commit* de 3 fases) del protocolo de consenso ordena un lote (colección) de transacciones. Los nodos mantienen varios ledger, cada uno con un propósito distinto. Tiene un *pool* ledger para transacciones de membresía de nodos, como la adición de un nuevo nodo, la suspensión de un nodo, el cambio de IP/puerto o claves de un nodo, un ledger para transacciones de identidad, etc.

Además del ledger, los nodos mantienen un estado (para cada ledger) del tipo Merkle Patricia Trie. Sólo los clientes con los permisos adecuados pueden enviar solicitudes de escritura (transacciones) a los nodos, pero cualquier cliente puede

enviar solicitudes de lectura a los nodos. La comunicación de cliente a nodo y de nodo a nodo se realiza en CurveZMQ que es un protocolo de comunicación segura para uso en internet que tiene como objetivo proporcionar el mismo nivel de seguridad que CurveCP, a pesar de las diferencias entre UDP y TCP. Es decir, tiene como objetivo prevenir la escucha, datos fraudulentos, datos alterados, ataques de repetición, ataques de amplificación, ataques de intermediario, ataques de robo de claves, ataques de identidad y ciertos ataques de denegación de servicio (ZeroMQ, 2023).

Al recibir transacciones, los nodos realizan una validación básica y difunden la solicitud a otros nodos y se denomina “propagación de solicitudes”. Cada vez que los nodos se dan cuenta de que suficientes nodos han recibido la solicitud, consideran que la solicitud está lista para ser procesada. El nodo primario inicia una nueva ronda de consenso a través de un proceso de confirmación de 3 fases al final del cual todos los nodos agregan la transacción a su ledger.

Cuando el nodo primario falla (o se vuelve no funcional de alguna manera), o se comporta mal enviando mensajes incorrectos o se ralentiza, los nodos seguidores inician un protocolo para cambiar el líder. (Hyperledger Indy, 2018)

2.4 Redes de Blockchain Permisionadas

Las redes de blockchain permisionadas, también conocidas como consorcios o redes privadas, representan una variante de la tecnología blockchain que difiere significativamente de las blockchain públicas, como Bitcoin y Ethereum. A medida que la tecnología de blockchain ha madurado, se ha vuelto evidente que su aplicación no se limita únicamente a las criptomonedas y al sector financiero. De hecho, las redes de blockchain permisionadas se han convertido en una solución atractiva para empresas, instituciones financieras y organizaciones que buscan aprovechar las ventajas de la tecnología blockchain dentro de un contexto más controlado y regulado.

A diferencia de las blockchain públicas, en las cuales cualquiera puede unirse y participar en el proceso de validación y creación de bloques, las redes de blockchain permisionadas imponen restricciones en quién puede unirse y qué participantes tienen el derecho de validación. Algunas de las características clave de estas redes incluyen:

- Acceso Controlado: En una red de blockchain permisionada, la participación está limitada a un grupo de actores autorizados. Estos actores son generalmente organizaciones, empresas o instituciones que han sido invitadas a unirse a la red.

- Validadores Autorizados: A diferencia de las redes blockchain públicas, donde cualquiera puede ser un validador, en una red permisionada, los nodos validadores son conocidos y autorizados. Esto aumenta la confianza y permite una gobernanza más estructurada.

- Privacidad y Confidencialidad: Las redes de blockchain permisionadas a menudo brindan soluciones para garantizar la privacidad de los datos,

permitiendo transacciones y contratos inteligentes confidenciales, lo que es fundamental para aplicaciones empresariales.

- Rendimiento y Eficiencia: Estas redes a menudo ofrecen un mayor rendimiento y eficiencia en comparación con las blockchain públicas, ya que no están sujetas a la competencia de minería y a la sobrecarga de validación.

Las redes de blockchain permisionadas han encontrado aplicaciones en una variedad de sectores y escenarios, destacando su versatilidad y capacidad para abordar desafíos específicos de la empresa. Algunas aplicaciones destacadas incluyen:

- Gestión de la Cadena de Suministro: Las redes de blockchain permisionadas permiten un seguimiento y trazabilidad precisos de los productos a lo largo de la cadena de suministro, lo que es esencial para garantizar la autenticidad y la calidad de los productos.

- Gestión de Identidad: Estas redes son ideales para soluciones de identidad digital seguras y verificables, lo que puede ser fundamental en sectores como la atención médica y las finanzas.

- Contratos Inteligentes en Empresas: Las redes de blockchain permisionadas son utilizadas para implementar contratos inteligentes en empresas, automatizando procesos y garantizando el cumplimiento contractual.

2.5 Identificaciones Descentralizadas (DIDs)

Las Identificaciones Descentralizadas representan una innovación fundamental en el ámbito de la identidad digital. Son una forma de gestionar y controlar la propia identidad en línea sin depender de intermediarios centralizados, como redes sociales o instituciones gubernamentales (World Wide Web Consortium, 2023). Las redes de blockchain permisionadas son un sistema ideal para implementar soluciones de DIDs, aprovechando las ventajas de control, privacidad y seguridad que ofrecen.

En redes de blockchain permisionadas, las DIDs pueden ser gestionadas por organizaciones, lo que garantiza un nivel de control sobre la identidad digital. Esto es particularmente valioso en casos donde se deben cumplir regulaciones y políticas específicas. Las blockchain permisionadas ofrecen un alto nivel de seguridad, lo que es esencial para la gestión de DIDs. En ellas, los datos de identidad pueden almacenarse y protegerse de manera confiable en estas redes, reduciendo los riesgos de hackeos y fraudes.

Algunos ejemplos de implementación de DIDs en redes de blockchain permisionadas son:

- Hyperledger Indy: Indy se utiliza para crear aplicaciones de identidad digital para una variedad de sectores, incluyendo finanzas, salud y

gobierno. Por ejemplo, Indy se utiliza para crear una aplicación de identidad digital para pacientes que permite a los pacientes compartir sus datos médicos de forma segura con sus proveedores de atención médica.

- W3C Verifiable Credentials: Las credenciales verificables W3C se utilizan para crear credenciales digitales para una variedad de propósitos, incluyendo educación, empleo y salud. Por ejemplo, para crear certificados académicos que acreditan competencias o habilidades y que que pueden ser verificadas por universidades y empleadores para determinar su autenticidad.

- Sovrin: Sovrin se utiliza para crear un sistema de identidad digital para ciudadanos del mundo. Sovrin se utiliza para crear credenciales digitales que pueden ser utilizadas por ciudadanos para acceder a servicios gubernamentales y privados.

2.6 Credenciales Verificables (VCs)

Estas credenciales son emitidas por una entidad confiable y verificables por terceros para confirmar la autenticidad de los logros o atributos de un individuo (World Wide Web Consortium, 2023). Las redes de blockchain permisionadas se han destacado como un entorno adecuado para la gestión y verificación de VCs debido a sus ventajas particulares. Por otro lado, para lograr su uso masivo y homogéneo, las VCs se basan en un estándar abierto desarrollado por el *World Wide Web Consortium* (W3C) que define un formato de datos para VCs y un proceso para verificarlas.

Una VC consta de los siguientes elementos:

- Un identificador: Un identificador único para la VC.
- Un emisor: La entidad que emitió la VC.
- Un titular: La persona o entidad a la que pertenece la VC.
- Una declaración: La información contenida en la VC.
- Una firma: Una firma digital que verifica la autenticidad de la VC.

Las VCs se pueden almacenar en una blockchain. Almacenar VCs en una blockchain proporciona una serie de beneficios, incluyendo:

- Seguridad: Las VCs almacenadas en una blockchain son seguras y casi imposible de falsificar.
- Transparencia: Las VCs almacenadas en una blockchain son transparentes, lo que significa que cualquier persona puede verificar su autenticidad.
- Interoperabilidad: Las VCs almacenadas en una blockchain son interoperables, lo que significa que pueden ser verificadas por cualquier entidad que cumpla con el estándar VC.

2.7 Hyperledger Indy

Hyperledger Indy ha sido diseñado específicamente para abordar los desafíos de las Identidades Descentralizadas (DIDs). A diferencia de otras plataformas de blockchain que abordan una variedad de casos de uso, Hyperledger Indy se enfoca exclusivamente en la gestión de identidades. Este enfoque especializado permite que la plataforma sea altamente optimizada para la emisión y verificación de DIDs.

Uno de los aspectos más críticos en la gestión de DIDs es la privacidad y el control del titular de la identidad. Hyperledger Indy aborda este desafío al permitir a los individuos tener un control total sobre sus DIDs y los datos asociados. Esto significa que el propietario de la identidad decide qué información compartir y con quién. La privacidad en Hyperledger Indy se logra mediante el uso de técnicas de criptografía avanzadas. La plataforma permite a los usuarios presentar pruebas criptográficas sin revelar la información subyacente. Esto garantiza que las transacciones y la verificación de DIDs sean altamente seguras y que la información personal del usuario esté protegida.

La interoperabilidad es esencial en el ámbito de las DIDs, ya que se espera que las identidades digitales sean utilizadas en una variedad de aplicaciones y sistemas. Hyperledger Indy se destaca en este aspecto al integrarse bien con otros estándares de DIDs y tecnologías relacionadas, esto debido a que sigue los estándares W3C para DIDs y *Verifiable Credentials Data Model* (VCDM). Esto significa que las credenciales verificables emitidas en Hyperledger Indy son compatibles con otros sistemas que siguen estos estándares lo cual facilita la adopción y la integración de DIDs en una amplia gama de aplicaciones, desde la atención médica hasta la educación.

Por otra parte, Hyperledger Indy utiliza el algoritmo de consenso tolerante a fallas bizantinas (BFT), específicamente el algoritmo de consenso Plenum. Los algoritmos BFT están diseñados para garantizar el consenso en una red incluso en presencia de nodos no confiables o defectuosos.El algoritmo de consenso Plenum utilizado por Indy es una versión modificada del algoritmo de consenso PBFT, optimizado para redes descentralizadas a gran escala (Hyperledger Indy, 2023).

Hyperledger Indy no solo es una plataforma robusta y especializada, sino que también está respaldada por una comunidad activa de desarrolladores y organizaciones, cuya participación apoyo continuo son aspectos cruciales para garantizar que una plataforma de este tipo siga siendo relevante y eficaz en el largo plazo.

2.8 Sovrin: Red pública para la Identidad Autosoberana en Internet

Sovrin es el primer servicio público global exclusivamente dedicado a la identificación autosoberana y a las credenciales verificables (Reed, 2016). Su historia comienza en 2015 cuando la empresa emergente Evernym percibió el potencial de la tecnología blockchain para abordar el problema fundamental de

la confianza en la identidad soberana y se embarcó en el diseño de una nueva blockchain denominada Sovrin para abordarlo.

Uno de los retos principales consistía en que la solución debía operar tan universalmente como el Sistema de Nombres de Dominio (DNS) por lo que Sovrin debía ser un esfuerzo comunitario, similar a la construcción de otros componentes fundamentales de la infraestructura de Internet. Con la colaboración de expertos en identidad digital, seguridad y privacidad de todo el mundo para abordar aspectos clave del diseño y la gobernanza, se decidió que Sovrin usara exclusivamente estándares abiertos y código fuente de libre acceso, a través del proyecto Hyperledger Indy.

El 29 de septiembre de 2016, se anunció la creación de la Fundación Sovrin en Londres. Esta fundación internacional sin ánimo de lucro cuenta con una junta directiva de doce fideicomisarios, además de un Consejo de Gobernanza Técnica. A principios de 2017, la Fundación Sovrin transfirió el código fuente de libre acceso, originalmente desarrollado por Evernym, a la Fundación Linux.

Tras un año de pruebas en entornos controlados y versiones iniciales, la Red Sovrin se lanzó oficialmente el 31 de julio de 2017, con una transacción inicial entre las primeras diez organizaciones participantes conocidas como "mayordomos".

De acuerdo con el artículo "*Sovrin: digital identities in the blockchain era*" (Khovratovich, 2017) cada componente de la arquitectura Sovrin se ha diseñado meticulosamente para cumplir con los cuatro requisitos fundamentales de la Identidad Soberana y Autogestionada (SSI): gobernanza, escalabilidad, accesibilidad y privacidad.

- Gobernanza: Garantizar que la red sea confiable para todas las partes interesadas.
- Rendimiento: Lograr que la red ofrezca identidad soberana a escala global.
- Accesibilidad: Asegurar que la identidad esté disponible para todos.
- Privacidad: Cumplir con los estándares más rigurosos de privacidad en todo el mundo.

2.8.1 Funcionamiento de la red Sovrin

Sovrin es una red de identidad descentralizada basada en Hyperledger Indy. Usa una base de datos descentralizada, para registrar transacciones de datos relacionados con la identidad, como claves públicas, esquemas, definiciones de credenciales y otros registros. El ledger es mantenido por un conjunto de nodos operados por organizaciones independientes. Estos nodos utilizan un protocolo de consenso para garantizar la integridad y seguridad de los datos del ledger.

El ledger se divide en cuatro dominios: principal, piscina (pool), configuración y auditoría.

- El dominio principal almacena los datos relacionados con la identidad.

- El dominio de la piscina almacena la información sobre los nodos y su estado.
- El dominio de configuración almacena los parámetros de configuración de la red.
- El dominio de auditoría almacena los hashes de las transacciones de los otros dominios para proporcionar un historial verificable del ledger.

La red Sovrin también utiliza un token digital llamado Token Sovrin para habilitar un mercado global de credenciales verificables. El token se utiliza para pagar las transacciones en el ledger, como la emisión, verificación o revocación de credenciales. El token también se utiliza para incentivar a los nodos a proporcionar servicios confiables y seguros para la red. El token se basa en el estándar ERC-20 y se ejecuta en un ledger separado llamado Ledger de Pagos Sovrin, que está conectado al Ledger de Identidad Sovrin a través de un sub-protocolo de pago.

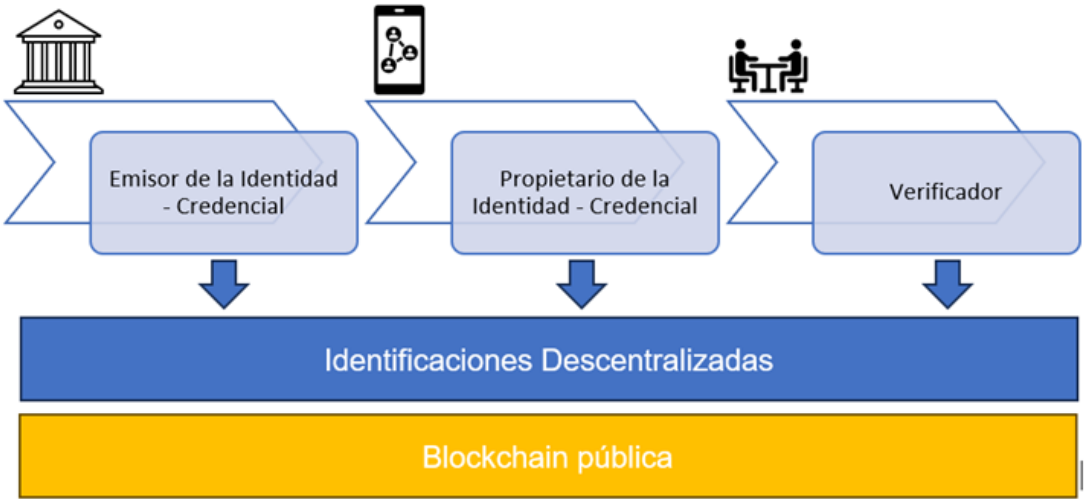


Figura 2: Arquitectura Funcional de Sovrin
Elaboración propia

La red Sovrin admite una variedad de transacciones de identidad, como la creación de Identificaciones Descentralizadas (DID), la emisión de credenciales verificables, la demostración de atributos o reclamaciones y la revocación de credenciales. Estas transacciones son realizadas por diferentes roles en la red, como propietarios de identidad, emisores de credenciales, titulares de credenciales y verificadores de credenciales (Sankarshan Mukhopadhyay, 2023).

Estos roles utilizan técnicas criptográficas, como firmas digitales, pruebas de conocimiento cero y credenciales anónimas, para garantizar la privacidad, seguridad y verificabilidad de los datos de identidad. La Red Sovrin también proporciona un conjunto de protocolos y API, como DIDComm, Aries e Indy, para habilitar la interoperabilidad y estandarización entre diferentes sistemas de identidad y aplicaciones.

3. Arquitectura de una solución basada en una blockchain permisionada

Este capítulo desglosa la estructura y el funcionamiento de una solución para la gestión descentralizada de credenciales verificables con un enfoque especial en el proyecto pionero en Identificaciones Autosoberanas y Credenciales Verificables de la provincia de Columbia Británica, Canadá. Se exploran los componentes críticos y la infraestructura necesaria para la implementación de una red VON, incluyendo la identificación digital, la gestión de credenciales verificables y la interacción segura entre los participantes de la red.

Este diseño se estructura en tres capas funcionales principales: la primera dedicada a la gestión de Identificaciones Descentralizadas (DIDs) y Credenciales Verificables (VCs) a través de la tecnología *Distributed Ledger Technology* (DLT); la segunda centrada en la interoperabilidad y la comunicación segura entre entidades; y la tercera, que se ocupa del intercambio efectivo y seguro de credenciales.

3.1 *Verifiable Organization Networks* (VON)

Las *Verifiable Organization Networks* (VON) son redes de organizaciones que utilizan tecnología blockchain para crear y compartir reclamos verificables y criptográficamente seguros sobre las empresas. VON se basa en el ledger distribuido Hyperledger Indy, que proporciona una base para la identidad digital soberana y las credenciales verificables.

Uno de los casos de aplicación más importantes es un proyecto liderado por el gobierno de la provincia de Columbia Británica, en Canadá que busca implementar una red VON para mejorar la economía digital y la experiencia de los usuarios de servicios gubernamentales (Province of British Columbia, 2023).

Algunas de las características de dicho modelo son:

- Usa una red permisionada como infraestructura para emitir y verificar credenciales digitales DIDs sobre organizaciones.
- Crea un directorio público y verificable de organizaciones registradas en Columbia Británica.
- Permite a las organizaciones y a los usuarios tener un control soberano sobre sus datos y compartirlos con otras entidades de forma segura y confiable.
- Facilita la interoperabilidad y la innovación entre diferentes sectores y jurisdicciones.

3.2 Plataforma para la Interoperabilidad e Intercambio de Credenciales Verificables

La implementación de una red de organizaciones verificables involucra muchos componentes. En un ecosistema de este tipo, los componentes que lo conforman trabajan en conjunto para emitir, verificar y validar credenciales de

manera segura y eficiente. Siguen protocolos de transmisión segura de información para comunicar las credenciales entre ellos, tienen programas de que sirven de interfaz para que los diferentes actores interactúen con el sistema y poseen un conjunto de reglas y de roles que las partes deben seguir.

En particular, una red de este tipo usa un sistema de identificación digital común basada en estándares aceptados universalmente, para todos los entes dentro de la organización, así como también un criterio común para definir credenciales digitales. Luego un sistema que permita mantener un registro distribuido y seguro de dichas identificaciones y credenciales. Posteriormente requiere de un sistema compatible con el primero que permita la distribución segura de dicha información entre los miembros de la red. Y por último se requiere de un conjunto común de algoritmos criptográficos que garanticen la seguridad y privacidad de todo el sistema.

Podemos agrupar estos elementos de manera funcional, en forma de capas que interactúan entre sí. La característica modular de este tipo de redes permite que desarrolladores puedan concentrarse en capas en particular en lugar de todo el sistema en su conjunto.

3.3 Capa 1: DLT para gestión de DIDs y VCs

La primera capa es el centro del sistema. Aporta un conjunto de herramientas, bibliotecas y componentes reutilizables que permitan proporcionar identidades digitales basadas en registros distribuidos. Esto permitirá que las Identificaciones Descentralizadas y las Credenciales Verificables asociadas a éstas sean intercambiables a través de dominios administrativos, aplicaciones y otros tipos de componentes del sistema. Entre los servicios y componentes involucrados en una capa como esta están:

3.3.1 Las Identificaciones Descentralizadas DIDs.

Estas identificaciones deberán estar en formato *Verifiable Credentials* (VC), conforme a las directrices del W3C, con el objeto de garantizar su interoperabilidad y seguridad en la red. Durante el proceso de verificación de estas credenciales, un participante (o *holder*) presentará sus credenciales digitales a un verificador, quien luego consulta la red para confirmar la autenticidad y validez de dichas credenciales. Esto se logra mediante la verificación de la firma digital y el control de la revocación de las credenciales. Estas identificaciones se almacenarán, transmitirán y procesarán como archivos formato JSON y basados en el *Verifiable Credentials Data Model* de W3C (World Wide Web Consortium, 2022)

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "https://example.org/credentials/1872",
  "type": ["VerifiableCredential", "PersonalIdentityCredential"],
  "issuer": "https://example.org/issuer/1234",
  "issuanceDate": "2023-11-20T12:00:00Z",
  "credentialSubject": {
    "id": "did:example:abcdef1234567890",
    "name": "Juan Pérez",
    "dateOfBirth": "1990-01-01",
    "nationality": "Española",
    "documentType": "DNI",
    "documentNumber": "12345678A"
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2023-11-20T12:00:00Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.org/credentials/1872#keys-1",
    "jws": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjI3Nzk0MjE5MjA5In0.eyJpYXQiO..."
  }
}
```


Figura 3: JSON de una DID
Elaboración Propia

3.3.2 Un algoritmo de creación y gestión de DIDs que opere sobre el DLT permisionado, que permita a los usuarios gestionar sus identificaciones sin depender de una autoridad central y que garantice que dichos registros no puedan ser alterados.

3.3.3 Credenciales Verificables.
Estas credenciales deberán estar basadas en el estándar W3C (World Wide Web Consortium, 2023), se deberán almacenar y distribuir en un formato JSON y se vincularán al DID del usuario, permitiendo la verificación de atributos sin revelar información innecesaria. Un ejemplo de una credencial verificable puede verse en la figura 5.


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.gov/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.university.edu",
  "issuanceDate": "2020-01-01T19:73:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2020-01-01T19:73:24Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.university.edu/keys/1",
    "jws": "eyJhbGciOiJSUzI1NiIsImtpZCI6Ij... (recortado por brevedad)"
  }
}
```


Figura 4: JSON de una VC
Elaboración Propia

3.4 Capa 2: Plataforma de Interoperabilidad

En segundo lugar, se requiere de una capa de agentes, protocolos y herramientas que permitan a las entidades que participen en el sistema

interactuar de forma segura utilizando identidades digitales basadas en estándares. Deberá tratarse de un conjunto de herramientas no atado a un blockchain específico y debe poder interactuar con diferentes sistemas DLT tal que facilite la creación y el intercambio de credenciales verificables y la realización de pruebas de conocimiento nulo (*Zero Knowledge Proofs*). Entre los componentes de esta plataforma se encuentran:

1. Un protocolo de comunicación entre organizaciones o entidades que permita intercambiar información destinada a la validación de las credenciales.
2. Los emisores de credenciales, por ejemplo, una institución educativa, como una universidad o una escuela, que emite credenciales digitales a sus graduados. El emisor de credenciales utilizaría la plataforma DLT anterior para emitir credenciales digitales, asignando un identificador único a cada credencial y firmándola digitalmente.
3. Los titulares de credenciales, que son los individuos que recibe una credencial digital y la almacenan de manera segura en sus billeteras.
4. La Billetera que es una aplicación utilizada por el titular de la credencial para almacenar y gestionar sus credenciales digitales y que permite al titular tener un control completo sobre sus credenciales y decidir qué y cuándo compartir. El titular importa sus credenciales digitales a la billetera desde la plataforma anterior. De igual forma, el titular usa su billetera para presentar credenciales para su verificación.
5. Los entes verificadores de credenciales, como por ejemplo un empleador o una institución, que necesitan verificar la autenticidad de una credencial. Estas entidades utilizan la información proporcionada por el titular de la credencial para verificar su autenticidad. Un verificador solicitaría al titular que presente su credencial digital desde su billetera para luego verificar la información y la firma digital en la capa DLT anterior con el objeto de validar que la credencial sea auténtica.

3.5 Capa 3: Intercambio de Credenciales

Esta capa se encarga de servir como interfaz entre la tecnología subyacente de los diferentes frameworks DLT y los usuarios del sistema. Esta capa, que actuará como un *front-end* se ejecutan procesos del flujo de trabajo de acuerdo con los siguientes roles:

a. Titulares de Credenciales
   Son usuarios individuales u organizaciones que poseen y controlan sus identidades digitales y credenciales en la red. Gestionan su propia identidad digital, incluyendo la creación, control y compartición de sus credenciales. Utilizan agentes para interactuar con la red, almacenar credenciales y comunicarse con emisores y verificadores.
b. Verificadores de Credenciales
   Son entidades (pueden ser organizaciones o sistemas) que necesitan verificar la autenticidad y validez de las credenciales presentadas por los titulares. Verifican la autenticidad y validez de las credenciales digitales sin necesidad de interactuar directamente con el emisor. Utilizan la red para verificar que una credencial existe, es legítima y no ha sido revocada o alterada.

c. Emisores de Credenciales
   Son entidades autorizadas (como instituciones educativas, gobiernos, empresas) que emiten credenciales digitales a los titulares. Crean y emiten credenciales digitales, como licencias, certificados educativos, identificaciones, etc. Registran la emisión de estas credenciales en la red, lo que garantiza su autenticidad y permite su verificación posterior.

Estos procesos se ejecutan mediante el uso de “Agentes”, que son software que actúa en nombre de los usuarios para interactuar con la red; y “Carteras”, que son software que permite a los usuarios almacenar y gestionar sus credenciales digitales y DIDs de forma segura. Una representación gráfica de este modelo general de capas puede verse en la figura 5.

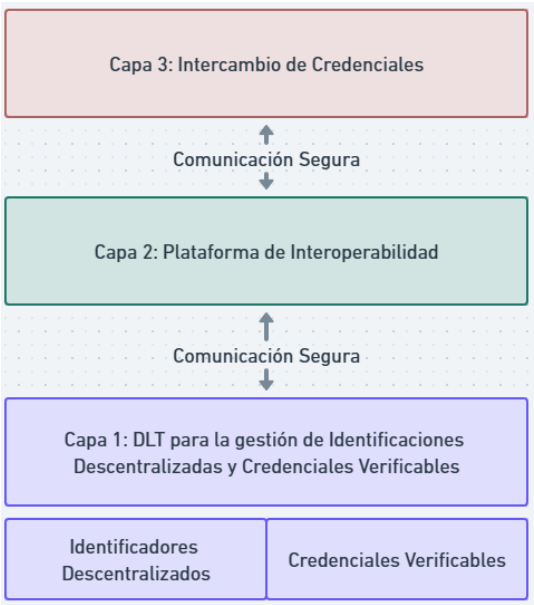


Figura 5: Arquitectura Funcional Genérica
Elaboración Propia

4. Propuesta de Arquitectura

En este capítulo se describe la propuesta específica de arquitectura para la una red descentralizada basada en el modelo descrito en el capítulo anterior, esto es, una red semejante a una VON Network. Con el objeto de obtener un diseño abierto, escalable y fácil de mantener, una VON Network, utiliza elementos componentes del ecosistema Hyperledger. A su vez, Hyperledger consiste en un ecosistema global abierto para tecnologías de blockchain empresarial que forma parte de la *Linux Foundation*. Hyperledger aloja varios proyectos de software de código abierto que sirven como pilares para despliegues de blockchain y son liderados y mantenidos por una comunidad y desarrollados de manera colaborativa y abierta.

4.1 Capa 1. VON Network: Hyperledger Indy

En este diseño, la plataforma de Hyperledger Indy actúa como el núcleo de la red de validación de credenciales educativas. Indy proporciona herramientas y servicios para emitir, presentar y verificar credenciales digitales (Hyperledger Indy, 2023). Hyperledger Indy utiliza un ledger descentralizado para garantizar la integridad y la autenticidad de las credenciales y permite a organizaciones emitirlas y a los titulares de estas presentarlas de manera segura. Además, permite a verificadores (un tercero interesado, como por ejemplo un empleador) validar las credenciales previa aprobación del titular.

4.2 Capa 2. Plataforma de Interoperabilidad: Protocolo Agent-to-Agent (A2A)

Esta es una capa lógica donde se define el flujo de información del intercambio de credenciales. En esta solución, dicho flujo se realizará de acuerdo con el de Hyperledger Indy (Hyperledger Indy, 2023) y se ejecuta mediante el uso de agentes. Los agentes de identidad actúan como intermediarios entre los usuarios y la red y permiten a los usuarios crear y gestionar sus DIDs y credenciales, proporcionando una interfaz para recibir, almacenar y presentarlas. Los agentes se comunican entre sí usando el protocolo de mensajería segura A2A denominado DIDComm.

4.3 Capa 3. Intercambio de Credenciales: Hyperledger Aries

Hyperledger Aries es un proyecto de código abierto bajo el paraguas de Hyperledger, diseñado para facilitar la interoperabilidad de sistemas de identidad descentralizados a través de la creación, transmisión y almacenamiento de datos de identidad digital (Hyperledger Foundation, 2023). Hyperledger Aries proporciona las herramientas necesarias para el manejo de interacciones relacionadas con las identidades soberanas (*Self-Sovereign Identity, SSI*), tales como la creación y gestión de credenciales verificables y la comunicación segura entre las partes.

La arquitectura funcional del sistema propuesto se muestra en la figura 6.

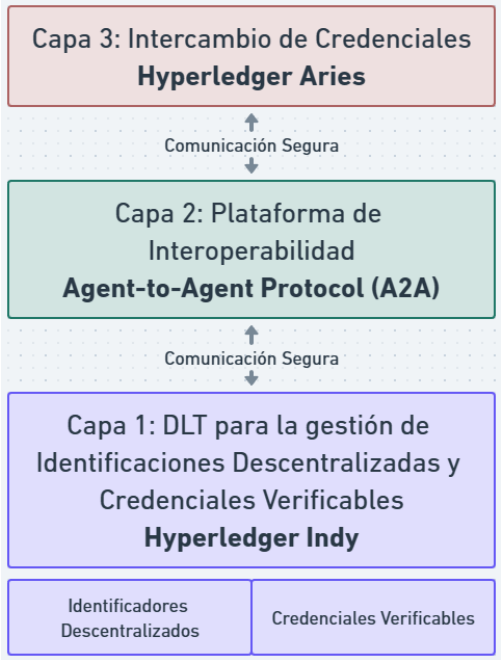


Figura 6: Arquitectura Funcional del Sistema Propuesto
Elaboración Propia

4.4 Flujo de información en el intercambio de credenciales

En general, el flujo de información de credenciales entre los elementos definidos en el capítulo anterior (Titulares, Validadores y Emisores) mediante el uso de agentes sigue los siguientes pasos:

a. El emisor de la credencial (por ejemplo, una universidad) se registra en la red como una entidad de confianza, creando un par de claves pública y privada, y publicando la clave pública en el ledger.
b. El emisor crea un esquema de credencial, que define los atributos que contendrá la credencial (por ejemplo, nombre, fecha de nacimiento, título, etc.), y lo publica también en el ledger.
c. El titular de la credencial (por ejemplo, un estudiante) crea una cartera digital, que es una aplicación que le permite almacenar y gestionar sus credenciales verificables.
d. El titular también genera un par de claves pública y privada, y crea un identificador descentralizado (DID), que es una cadena alfanumérica que lo identifica de forma única en la red.
e. El titular solicita al emisor una credencial verificable (VC), proporcionando su DID y los datos necesarios para la credencial.
f. El emisor verifica los datos del titular, y crea una credencial verificable, que contiene los atributos del esquema, los valores de los datos, una firma digital del emisor, y un identificador de la credencial.
g. El emisor envía la credencial verificable al titular, que la almacena en su cartera digital.
h. El verificador de la credencial (por ejemplo, un empleador) solicita al titular una prueba de ciertos atributos de la credencial (por ejemplo, el título y la fecha de expedición).

i. El titular crea una prueba de los atributos solicitados, usando el protocolo criptográfico ZKP, que le permite demostrar que posee una credencial verificable sin revelar toda la información que contiene.
j. El titular envía la prueba al verificador.
k. El verificador verifica la prueba, consultando el ledger para obtener el esquema de la credencial, la clave pública del emisor, y el estado de revocación de la credencial.
l. Si la prueba es válida, el verificador confía en los atributos del titular.

El proceso anterior puede verse gráficamente en la figura 7.

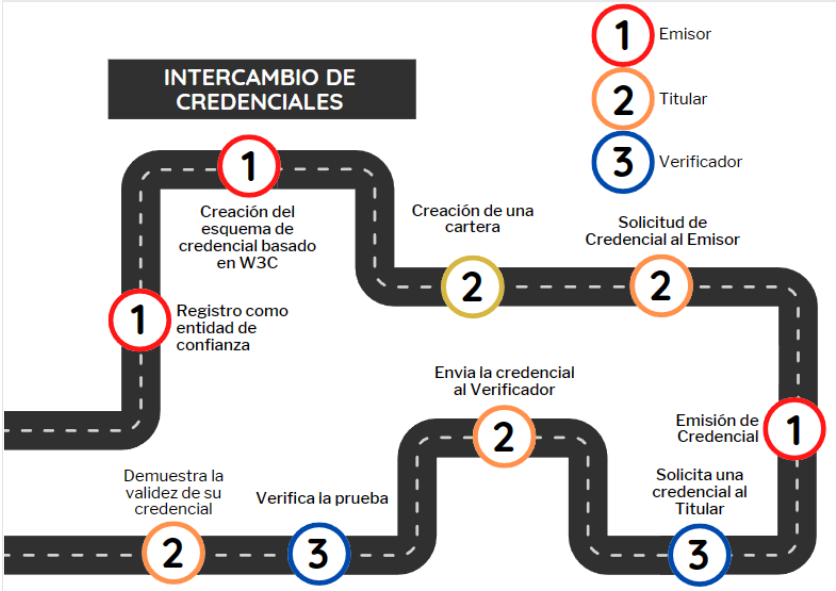


Figura 7: Flujo del Intercambio de Credenciales
Elaboración propia

Adicionalmente, todo el sistema utilizará un conjunto de recursos criptográficos compartidos que forman parte de otro proyecto Hyperledger denominado Hyperledger Ursa que es una biblioteca de criptografía compartida que puede ser utilizada por proyectos de blockchain para proporcionar implementaciones de seguridad avanzadas (Hyperledger Foundation, 2018). Mediante la biblioteca Hyperledger Ursa los verificadores puedes confirmar criptográficamente la autenticidad de una credencial presentada por un titular.

5. Desarrollo de la solución

En el presente capítulo se muestra el desarrollo de una demostración de una red de verificación de credenciales educativas basada en el diseño propuesto en el capítulo anterior. Se usó Hyperledger Indy para la creación de una VON Network, usando como base el repositorio GitHub VON-Network (BCGOV, 2023) que servirá de soporte para el intercambio y validación de las credenciales. Asimismo, se desarrollaron los tres agentes, y se demostrarán en el mismo orden del flujo de trabajo de la solución. Los agentes realizarán el intercambio de credenciales usando a Hyperledger como soporte para las funciones de bajo nivel. Toda la solución, incluyendo un modelo portable de la VON Network se subirá a un repositorio GitHub para su debida documentación.

El despliegue de toda la solución puede realizarse de tres formas:

- En un navegador: Se utiliza "*Play with Docker*" (PwD) para ejecutar los contenedores Docker de los agentes y una instancia para levantar la VON Network, todo ejecutándose en máquinas virtuales. PwD permite levantar los entornos Docker en línea sin necesidad de configurar copias locales sin limitaciones en la realización de pruebas, modificaciones y configuraciones a la solución, sin embargo, las carteras con las DID y las VCs no son persistentes.

- En Docker: Se requiere una instancia de VON Network ejecutándose localmente en un contenedor Docker donde se abren cuatro terminales: uno para iniciar la VON-network, y luego uno para cada agente. Las carteras son persistentes.

- Localmente: Se requiere desplegar un entorno Python3 en y las dependencias necesarias. Se inicia una red local VON Network en Docker y se generan los archivos de génesis. También se requiere ejecutar una instancia local de la base de datos *Postgres* para la persistencia de las carteras.

El método utilizado en esta demostración de la solución desarrollada es el primero, debido a su portabilidad, practicidad y el hecho de que la persistencia de las carteras es irrelevante a los efectos de este trabajo. El contenido desarrollado en este trabajo puede encontrarse en su repositorio GitHub (Del Valle, 2023)

5.1 Agentes

Se han desarrollado tres agentes encargados de realizar las transacciones antes mencionadas y se han denominado **Titular, Emisor y Verificador.**

Agente Titular

El agente Titular, es una instancia de uno de los tres tipos de agentes necesarios en el contexto Hyperledger Aries. Este agente, desempeña un papel importante

en el ecosistema de identidad digital basado en blockchain y representa a un participante (en este caso, el titular de una credencial) en una red de identidad descentralizada VON Network. Este agente implementa una instancia de la clase `AriesAgent` definida en Hyperledger y por consecuencia éste hereda de aquella los métodos y atributos necesarios para la implementación de sus funciones y responsabilidades clave: Manejo de conexiones e invitaciones, administración de credenciales, presentación de pruebas y una simple interfaz de usuario que permite a su portador interactuar con el sistema de acuerdo con su rol.

Este agente implementa varios aspectos esenciales del manejo de la identidad en la VON Network, pues puede establecer y mantener conexiones con otros agentes, puede intercambiar información, credenciales y solicitudes de manera segura, recibir y almacenar credenciales digitales. Estas credenciales pueden ser emitidas por diferentes entidades educativas y representan afirmaciones verificables sobre atributos o calificaciones de su portador. Asimismo, tiene la capacidad de generar y presentar pruebas de sus credenciales sin revelar toda la información contenida en ellas.

Además, el agente puede responder a eventos específicos, como la recepción de una nueva credencial o una solicitud de prueba, controlando qué información comparte y con quién.

Agente Emisor

Tal como el agente Titular, el agente Emisor es un miembro del ecosistema de credenciales verificables. Este agente implementa una instancia de la clase *AriesAgent*. Representa una entidad (como una organización, institución o individuo) que interactúa con otros agentes) en un ecosistema de identidad digital y credenciales verificables VON Network. Este agente se encarga del establecimiento de conexiones con otros agentes en la red, emisión de credenciales, generación de invitaciones, solicitudes de pruebas y revocación de identidades.

Desde el punto de vista del proceso de verificación de credenciales, este agente tiene una función muy importante pues es en él donde se llenan los campos que definen la credencial con los datos específicos del titular.

Los campos contenidos en una credencial verificable se definen mediante su incorporación en un archivo JSON denominado *context* que el agente que las genera, es decir el emisor**,** llama. Cabe destacar que por diseño, Hyperledger Aries es *credential format agnostic* esto es, que puede usar cualquier formato de credencial siempre que haya un RFC que lo defina (Hyperledger, 2023). Los contextos disponibles y compatibles con W3C incluyen una variedad de vocabularios que incluyen una gran variedad de posibles casos de uso y aplicaciones y de los cuales se han tomado los necesarios de acuerdo con los requerimientos de éste trabajo. Una lista completa de los posibles vocabularios y sus declaraciones se puede obtener en internet. (Schema.org, 2023) y se ha incluido en el repositorio.

Propiedad	Tipo de dato	Descripción
`name`	Texto	Nombre de la persona.
`birthdate_dateint`	Fecha	Fecha de Nacimiento
`date`	Fecha	Fecha de culminación de los estudios
`degree`	Text	Descripción de la credencial educativa obtenida. En este caso: "*High School Diploma"*
`prefix`	Text	Emisor de la credencial

Figura 8: Campos de la Credencial
Elaboración Propia

Mediante el uso del agente, la organización emisor puede actualizar los campos de la credencial con los datos del titular de la misma.

Agente Verificador

En el agente Verificador, se implementa otro agente Hyperledger Aries, una instancia de la misma clase *AriesAgent* a la que perteneces los agentes Titular y Emisor. Este nuevo agente, muy similar al agente Emisor, puede interactuar dentro de un sistema de identidad digital, manejando conexiones, emitiendo credenciales, solicitando y verificando pruebas de identidad, y por su puesto comunicándose con otros agentes.

En el esquema de esta solución, el agente Verificador es un miembro del ecosistema que tiene por objeto verificar la validez de una credencial, sin necesidad de comunicarse directamente con el Emisor y sin requerir de información personal del Titular, sino sólo recurriendo a la información registrada en la blockchain. La credencial permite validar que el titular de la credencial es quien dice ser, y posee un título de High School válido emitido por una institución educativa miembro del mismo ecosistema.

5.2 Demostración de la solución

A continuación, se presenta una demostración de la solución siguiendo la secuencia de pasos correspondiente al intercambio de credenciales educativas entre tres partes: primero, una institución educativa que acredita a los egresados de un programa de *High School*. Segundo, un egresado que, habiendo completado el programa, recibe una credencial por parte del primero. Y tercero, una empresa que, para otorgar un puesto de trabajo requiere al segundo presentar una prueba que demuestre que ha culminado los estudios de *High School*. Adicionalmente, la demostración incluye un paso adicional en el que la empresa otorga una credencial de empleo. El flujo de trabajo se muestra en la siguiente figura:

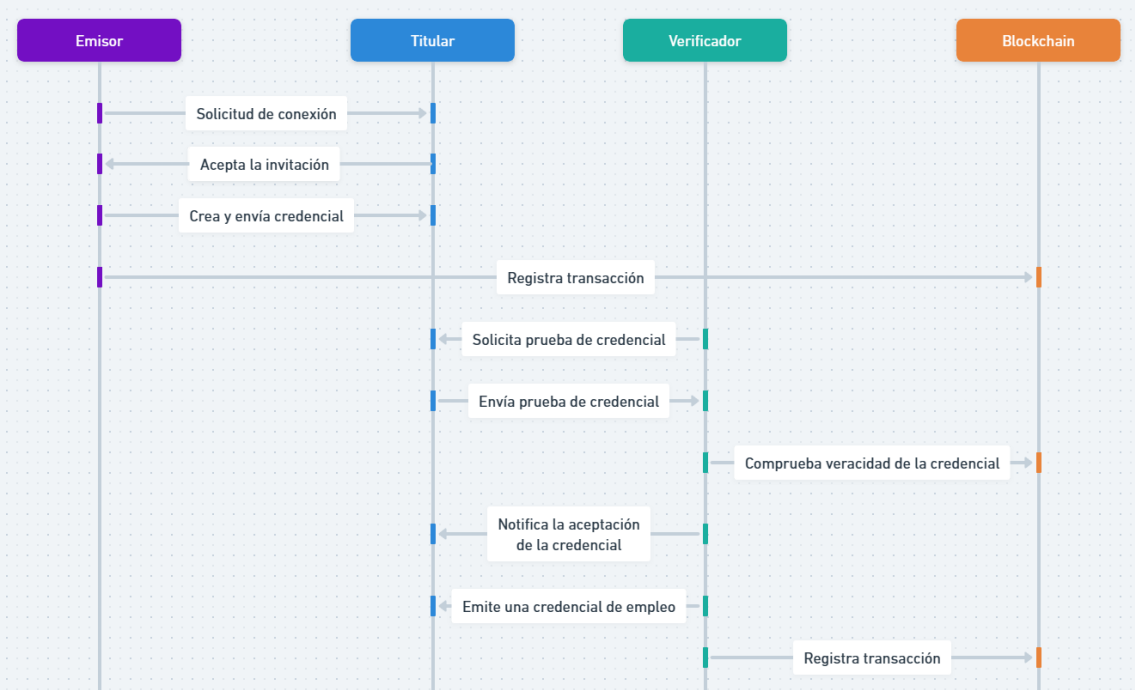


Figura 9: Intercambio de Credenciales
Elaboración Propia

Etapa 1. Creación de una credencial

Paso 1. Se levantan dos instancias en PWD y se cargan en ambas el contenido del repositorio que contiene la solución. La primera ejecutará el agente Emisor, la segunda, instancia ejecutará el agente Titular. Una vez que ambos agentes están en línea y conectados a la VON network, se procede a conectarlos e iniciar el proceso.

Paso 2. El emisor genera una invitación a conectar. Esta conexión incluye la identificación digital del emisor, así como información sobre la dirección IP, puerto y protocolos. La invitación luce de la siguiente forma:

```
#9 Input issuer invitation details
Invite details:

{
  "@type": "https://didcomm.org/out-of-band/1.1/invitation",
  "@id": "b15b638c-e608-4c2b-a680-280f79cbb1d7",
  "label": "faber.agent",
  "handshake_protocols": [
    "https://didcomm.org/didexchange/1.0"
  ],
  "services": [
    {
      "id": "#inline",
      "type": "did-communication",
      "recipientKeys": [
        "did:key:z6Mkgt5VGi77pQfMuiTSNYBpDCSazmb637LH7RqxgYCemZwX#z6Mkgt5VGi77pQfMuiTSNYBpDCSazmb637LH7RqxgYCemZwX"
      ],
      "serviceEndpoint": "http://ip172-18-0-42-cmbiif2o7r5g00bg4hk0-8020.direct.labs.play-with-docker.com"
    }
  ]
}
```

Figura 10: Invitación
Elaboración Propia

Una vez que ambas partes están conectadas, dicha conexión puede probarse mediante el envío de mensajes a través de la red:

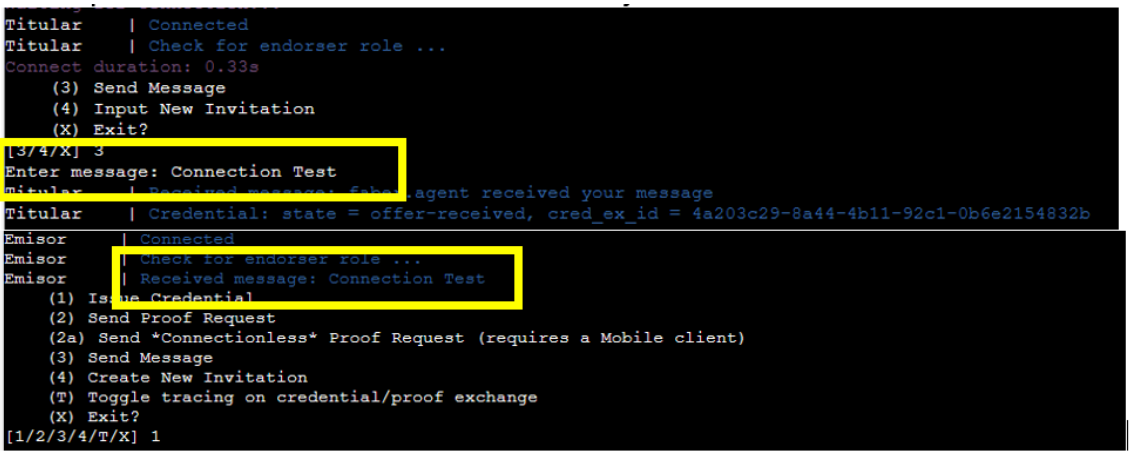


Figura 11: Envío de mensajes
Elaboración Propia

En este momento, ambas partes, emisor y titular, han intercambiado sus correspondientes identificaciones, por lo que ya es posible emitir una credencial que contendrá los datos correspondientes a “Jose Del Valle” quien ha obtenido un diploma de “High School”.

Paso 3. Generación de una credencial

Usando la opción 1, se crea la credencial y se envía al titular quien recibe una notificación. El agente Titular ha sido programado para aceptar esta credencial automáticamente.

Figura 12: Credencial
Elaboración Propia

La emisión de la credencial se registra en el ledger de la VON Network y puede verificarse en http://dev.greenlight.bcovrin.vonx.io.

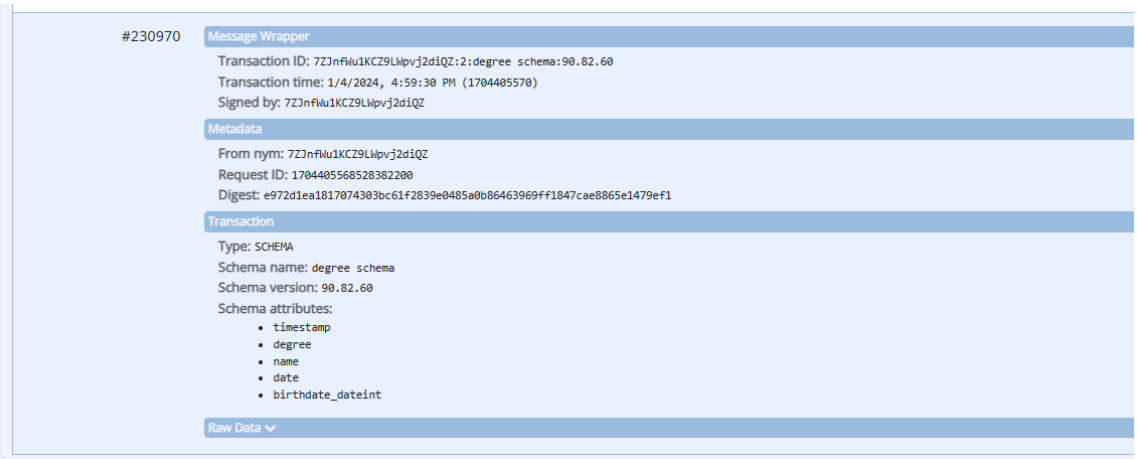


Figura 13: Verificación de la transacción
Elaboración Propia

Paso 4. Solicitud de una prueba por parte del emisor

Con el fin de verificar la transacción hecha, el agente Emisor puede usar solicitar una prueba al Titular. El agente Titular responde automáticamente a la prueba de la credencial y el agente Emisor recibe la validación satisfactoria de la prueba.

Etapa 2: Verificación de una credencial

En esta etapa, un tercer elemento del ecosistema desea validar si el titular de una credencial posee una credencial educativa válida emitida por otro miembro del ecosistema de identidad digital y credenciales verificables. Para ello, se levanta una nueva instancia Docker y en ella levantamos el agente denominado “Verificador”.

Paso 1. Generación de una nueva conexión.

El agente Verificador debe conectarse con el agente Titular con el fin de intercambiar la credencial. Para ello emite una invitación -similar a la figura 10- que el agente Titular debe aceptar, similar al proceso previo de conexión entre el Emisor y el Titular. Una vez aceptada la invitación puede comprobarse la comunicación entre ambos agentes mediante el envío de mensajes.

Figura 14: Prueba de conexión
Elaboración Propia

Paso 2. Solicitud de prueba de educación.

Ahora el agente Verificador puede enviar una solicitud de prueba de educación (*proof of education*) al titular de la credencial mediante un *Proof Request*. El agente Titular ha sido programado para aceptar esta solicitud automáticamente y validar su autenticidad. La credencial la validación exitosa en el agente Verificador se muestra en la figura siguiente.

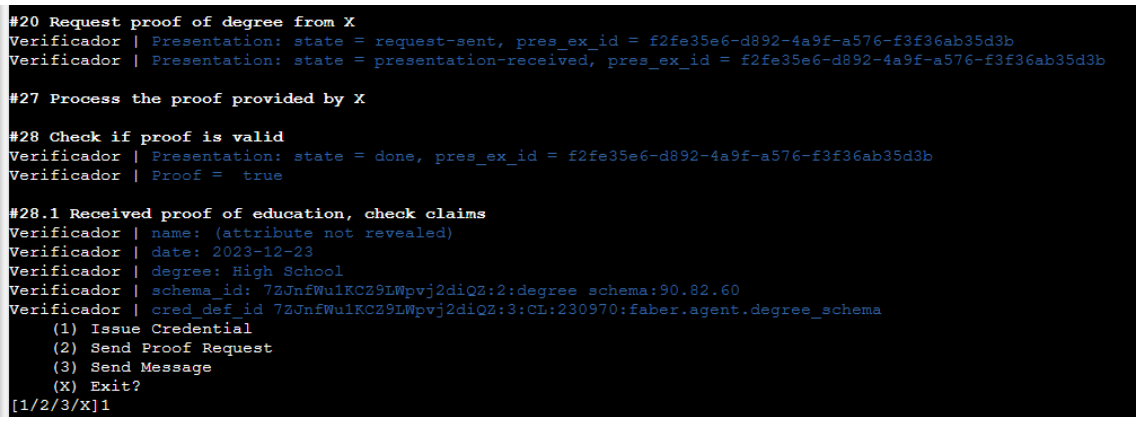


Figura 15: Verificación de la Credencial
Elaboración Propia

Puede observarse que la prueba se valida sin revelar el atributo *name* manteniendo así la privacidad del Titular.

Paso 3. Emisión de una credencial de empleo.

De igual forma que en el caso de agente Emisor, el agente Verificador puede también emitir una credencial. Esto es particularmente útil si el organismo o institución que realiza la verificación de la credencial académica también asigna una credencial, por ejemplo, de empleo, al titular. En este caso, se ha programado al agente Verificador para que emita una credencial que indica que ha contratado al titular y le ha asignado una posición y un número de identificación. Tal como en el caso anterior, el agente Titular ha sido programado para aceptar estas credenciales de forma automática.

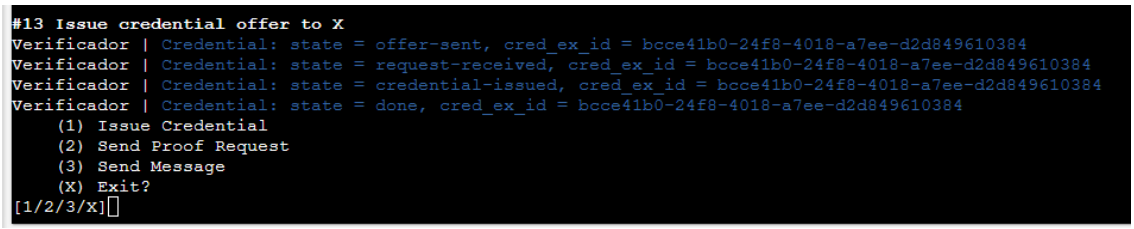


Figura 16: Emisión de credencial de empleo
Elaboración Propia

El contenido de dicha credencial puede verse en la figura 17.

Figura 17: Credencial de Empleo
Elaboración Propia

Asimismo, esta segunda credencial también queda registrada en el *ledger* http://dev.greenlight.bcovrin.vonx.io.

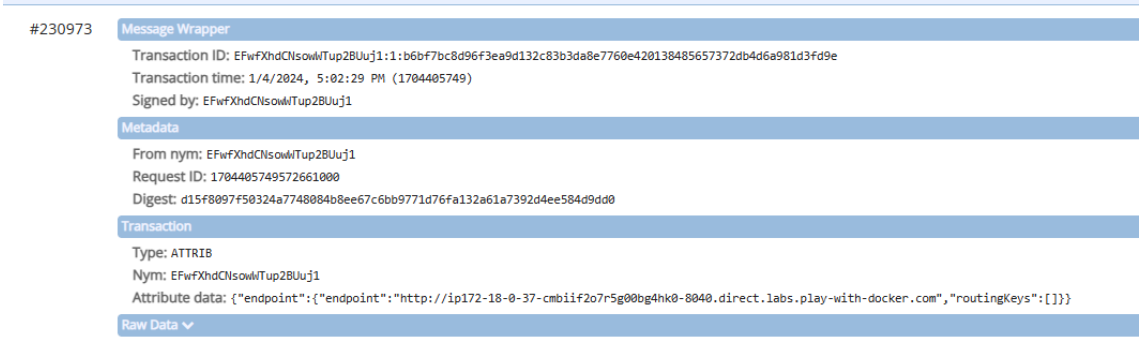


Figura 18: Registro de la credencial de empleo
Elaboración Propia

De esta forma el proceso de la verificación de la credencial educativa del titular queda validada ante el posible empleador dado que éste ha confirmado -por medio de su agente- la integridad criptográfica de dicha credencial en el *ledger*. Además de no necesitar contactar al emisor de la credencial, lo cual simplifica el proceso y lo descentraliza, la confianza en la credencial no depende en la confianza en el emisor sino en la verificación matemática de la credencial.

Por otro lado, el proceso otorga control (soberanía) del titular sobre la información que se hace pública en la transacción, de modo que éste puede determinar que parte de su información personal revela a un tercero.

Por último, este sistema también aporta bidireccionalidad en la relación entre emisores de credenciales y verificadores pues, los agentes de ambos tienen la capacidad de emitir credenciales y verificar credenciales de otros, siempre y cuando -como en este caso- ambos utilicen los mismos esquemas.

6. Conclusiones y trabajos futuros

El presente Trabajo Final detalla el desarrollo e implementación de una red descentralizada para la verificación de credenciales educativas, utilizando tecnología *blockchain* y a partir del cual se pueden extraer las siguientes conclusiones:

1. **Implementación exitosa de una solución de red descentralizada basada en *blockchain***: El trabajo realizado demuestra con éxito el diseño y construcción de una red descentralizada para la gestión y verificación de credenciales educativas, para ser utilizada en el contexto de escuelas secundarias del condado Miami-Dade, en el Estado de Florida, Estados Unidos.

2. **Uso eficaz de la tecnología una red permisionada para el manejo de identidades digitales**: Este trabajo ilustra el potencial de la tecnología *blockchain*, específicamente una red permisionada, en la creación de identidades digitales autónomas y verificables, y se demostró que las herramientas y servicios proporcionados por *Hyperledger Indy* y *Hyperledger Aries,* actuando coordinadamente, permiten la emisión, presentación y verificación seguras de credenciales digitales.

3. **Arquitectura modular y escalable**: La estructura de la solución implementada, dividida en capas funcionales, demuestra la eficiencia de una arquitectura modular y escalable. El diseño basado en capas del ecosistema *Hyperlegder* facilita la implementación de soluciones similares en diferentes contextos a la vez que permite futuras expansiones o modificaciones.

4. **Privacidad y seguridad en la gestión de credenciales**: En este trabajo se enfatiza la importancia de la privacidad y seguridad en la gestión de credenciales digitales mediante la utilización de pruebas de conocimiento cero, el almacenamiento seguro de credenciales digitales en billeteras criptográficas y la inmutabilidad de *blockchain*, los cuales constituyen aspectos clave de cualquier sistema de identidades auto-soberanas.

5. **Interoperabilidad y estandarización**: El sistema promueve la interoperabilidad y estandarización en la gestión de identidades digitales. Al seguir estándares como los del W3C para las credenciales verificables y los identificadores descentralizados (DIDs), el proyecto asegura la compatibilidad con otros sistemas y aplicaciones.

6. **Demostración práctica y funcionalidad del sistema**: A través de una demostración práctica, el presente trabajo muestra programas denominados agentes (Titular, Emisor y Verificador) los cuales interactúan dentro del sistema para emitir, almacenar y verificar credenciales, ilustrando la funcionalidad y aplicabilidad del sistema en escenarios reales.

7. **Contribución en la lucha contra el fraude de credenciales**: La solución aquí desarrollada representa un paso significativo en la lucha contra el fraude de credenciales educativas, ofreciendo una alternativa a los sistemas centralizados de credenciales digitales, y propone un método más seguro que simplifica la carga de trabajo administrativo asociado.

8. **Responsabilidad ambiental**: La solución desarrollada en el trabajo demuestra también que, al usar algoritmos de consenso energéticamente eficientes como la Prueba de Autoridad (PoA), es posible desarrollar sistemas de este tipo con bajo impacto ambiental.

En general, puede afirmarse que los objetivos planteados inicialmente fueron plenamente cumplidos, tanto a nivel de los productos esperados (intermedios y finales), como a nivel del marco temporal inicialmente planeado. El trabajo desarrolló y demostró con éxito la aplicación de la tecnología *blockchain* para crear un sistema de identidad digital y de verificación de credenciales seguro, confiable y escalable, con potencial para ser aplicado en una variedad de contextos inclusive más allá del ámbito educativo.

Por otra parte, se identificaron algunas líneas de trabajo que pueden derivarse de éste como, por ejemplo:

- Explorar la aplicación de esta solución en la verificación de otros tipos de credenciales académicas o relacionadas con el mundo académico, como licencias profesionales, títulos universitarios, o certificaciones industriales.
- Investigar la integración de esta tecnología con los sistemas de información académicos actuales (CMS) para facilitar la emisión y verificación de credenciales.
- Trabajar en la creación y adopción de esquemas JSON-LD estándares para garantizar la interoperabilidad de las credenciales educativas digitales con requisitos específicos.
- Investigar la integración de la inteligencia artificial en este tipo de sistemas para mejorar la eficiencia de los procesos de verificación y gestión de credenciales.

Glosario

Acuerdo de Autor de Transacción	Un documento controlado que funciona como un acuerdo legal entre la Fundación Sovrin y cualquier autor de transacción, que debe ser firmado digitalmente o acordado explícitamente por el autor de la transacción para poder escribir una transacción.
Agente	Un programa de software o proceso utilizado por o en nombre de una entidad para interactuar con otros agentes o con el Ledger Sovrin u otros ledgers distribuidos. Dentro de un agente se encuentra un Servicio de Gestión de Claves (KMS) que realiza operaciones criptográficas en nombre de la entidad que el agente representa.
Comunicación DID (DIDComm)	Un mecanismo de comunicación de mensajes asegurado utilizando las claves y puntos finales de servicio almacenados en los DIDs propiedad de las partes que se comunican.
Controlador	Un controlador proporciona las reglas que definen qué acciones iniciará un agente y cómo responderá el agente a los eventos. Hay un controlador para cada instancia de agente.
Credencial	Una afirmación digital que contiene un conjunto de reclamaciones hechas por una entidad sobre sí misma o sobre otra entidad. Una credencial se basa en una definición de credencial. Ejemplos de credenciales incluyen transcripciones universitarias, licencias de conducir, tarjetas de seguro de salud y permisos de construcción.
Credencial Verificable	Una credencial que incluye una prueba del emisor. Típicamente, esta prueba está en forma de una firma digital.
Definición de Credencial (CredDef)	Una definición legible por máquina de la estructura semántica de una credencial basada en uno o más esquemas. Las definiciones de credenciales se almacenan en el ledger. Las definiciones de credenciales deben incluir una clave pública del emisor. Las definiciones de credenciales facilitan la interoperabilidad de credenciales y pruebas entre múltiples emisores, titulares y verificadores.
Documento DID	El documento legible por máquina al que apunta un DID según lo definido por la especificación DID de W3C. Un documento DID describe las claves públicas, puntos finales de servicio y otros metadatos asociados con un DID. Un documento DID está asociado con exactamente un DID.
Emisor	La entidad que emite una credencial a un titular.
Esquema	Una definición legible por máquina de la semántica de una estructura de datos. Los esquemas se utilizan para definir los atributos utilizados en una o más definiciones de credenciales.
Fundación Sovrin	La organización de confianza pública sin fines de lucro encargada de administrar la Infraestructura Sovrin en nombre de la Comunidad Sovrin. La Fundación Sovrin es la Autoridad de Gobernanza para el Marco de Gobernanza Sovrin y el Marco de Confianza Web de Sovrin.
Hyperledger	Una iniciativa de la Fundación Linux para desarrollar tecnología de ledger distribuido y blockchain de código abierto.

Hyperledger Aries	Hyperledger Aries es infraestructura para interacciones entre pares basadas en blockchain. Incluye almacenamiento criptográfico compartido para clientes de blockchain, así como un protocolo de comunicaciones para permitir la interacción fuera del ledger entre esos clientes. Este proyecto consume el soporte criptográfico proporcionado por Hyperledger Ursa, para proporcionar una gestión segura de secretos y funcionalidad de gestión de claves descentralizada.
Hyperledger Indy	Un proyecto de código abierto bajo el paraguas de Hyperledger para identidad autónoma descentralizada. El código fuente de Hyperledger Indy fue originalmente contribuido a la Fundación Linux por la Fundación Sovrin. Los administradores de Sovrin ejecutan el software de nodo de Hyperledger Indy para operar sus nodos.
Hyperledger Ursa	Hyperledger Ursa es una biblioteca criptográfica compartida que permite a las personas (y proyectos) evitar duplicar otro trabajo criptográfico y, con suerte, aumentar la seguridad en el proceso. La biblioteca es un repositorio opcional para proyectos (y potencialmente otros) para colocar y usar cripto.
Identidad Autónoma	Identidad portátil de por vida para cualquier persona, organización o cosa que no depende de ninguna autoridad centralizada y que nunca puede ser quitada.
Identificador Descentralizado (DID)	Un tipo especial de identificador que es creado por su propietario, independientemente de cualquier autoridad central. Es un identificador globalmente único desarrollado específicamente para sistemas descentralizados según la especificación DID de W3C. Los DIDs permiten la gestión de identidad autónoma descentralizada interoperable. Un DID está asociado con exactamente un Documento DID.
Interfaz de Agente	La interfaz de agente es un componente de un agente que permite al agente establecer y gestionar conexiones con otros agentes e intercambiar mensajes con esos agentes.
Interfaz de Ledger	La interfaz de ledger permite leer y escribir DIDs y otras transacciones hacia/desde el ledger.
Marco de Gobernanza	El conjunto de definiciones, políticas, especificaciones y contratos comerciales, legales y técnicos por los cuales los miembros de una comunidad de confianza acuerdan ser gobernados para lograr sus niveles deseados de aseguramiento. Un marco de gobernanza también se conoce como marco de confianza.
Peer to Peer (P2P)	Una relación directa entre exactamente dos entidades. Las relaciones entre empresas son *peer-to-peer* por defecto. Un DID, una clave pública o un punto final de servicio es par a par si se usa exclusivamente en una relación par a par.
Proof of Authority (PoA)	Algoritmo de consenso que funciona otorgando el derecho de validar transacciones a un conjunto preseleccionado de nodos, conocidos como validadores.

Proof of Stake (PoS)	Algoritmo de consenso utilizado que funciona requiriendo que los validadores bloqueen sus propias criptomonedas como garantía para participar en el proceso de consenso.
Proof of Work (PoW)	Algoritmo de consenso que funciona requiriendo que los mineros realicen cálculos complejos para resolver un problema matemático.
Protocolo de Intercambio DID	El método por el cual se establecen conexiones entre agentes con diferentes roles (invitador, invitado), utilizando una secuencia de tipos de mensajes (invitación, solicitud, respuesta) para intercambiar elementos de datos (IDs, DIDs, DIDdocs). Vea la especificación de la Solicitud de Cambio de Aries (RFC) del protocolo de Intercambio DID.
Protocolo de Sobre DIDComm	El método por el cual se entregan los mensajes del Protocolo de Contenido DIDComm, independientemente del contenido del mensaje. El mensaje de contenido se cifra y almacena dentro del sobre.
Protocolo Tolerante a Fallas Bizantino de Plenum	Plenum es el corazón de la tecnología de ledger distribuido dentro de Hyperledger Indy. Como tal, proporciona características algo similares en alcance a las que se encuentran en Hyperledger Fabric.
Protocolos de Contenido DIDComm	Protocolos que definen secuencias de ida y vuelta de mensajes específicos enviados entre agentes colaboradores para lograr algún objetivo compartido. Los mensajes del Protocolo de Contenido DIDComm se entregan en mensajes del Protocolo de Sobre DIDComm.
Prueba	Verificación criptográfica de una reclamación o una credencial. Una firma digital es una forma simple de prueba. Un hash criptográfico también es una forma de prueba. Las pruebas de conocimiento cero permiten la divulgación selectiva de la información en una credencial.
Prueba de Conocimiento Cero	Una prueba que utiliza criptografía especial y un secreto de enlace para respaldar la divulgación selectiva de información sobre un conjunto de reclamaciones de un conjunto de credenciales. Una prueba de conocimiento cero proporciona prueba criptográfica sobre algunos o todos los datos en un conjunto de credenciales sin revelar los datos reales o cualquier información adicional, incluida la identidad del probador.
Revocación	El acto de un Emisor revocando la validez de una Reclamación o una Credencial. Con el Protocolo Sovrin y el Ledger Sovrin, la Revocación se logra utilizando un Registro de Revocación.
Solicitud de Prueba	La estructura de datos enviada por un verificador a un titular que describe la prueba requerida por el verificador.
SSI	Acrónimo de Identidad Autónoma.
Steward	Una organización aprobada por la Fundación Sovrin para operar un nodo. Un Steward debe cumplir con las calificaciones definidas en las Políticas Comerciales de Steward y los requisitos técnicos definidos en las Políticas Técnicas de Steward.

Tecnología de Ledger Distribuido	Un ledger distribuido (también llamado ledger compartido o tecnología de ledger distribuido o DLT) es un consenso de datos digitales replicados, compartidos y sincronizados distribuidos geográficamente en múltiples sitios, países o instituciones. No hay un administrador central ni almacenamiento de datos centralizado.
Titular	Un rol desempeñado por una entidad cuando se le emite una credencial por un emisor. El titular puede o no ser el sujeto de la credencial. Si la credencial admite pruebas de conocimiento cero, el titular también es el demostrador.
Transacción	Un registro de cualquier tipo escrito en un Ledger.

Bibliografía

Abbas Tashakkori, C. T. (2010). *Designing and Conducting Mixed Methods Research.*

Alexander, P. A. (2012). The promise of mixed methods research in education. . *Educational Researcher*, 41(1), 14-26.

Anshuman Singh, A. S. (2021). A Blockchain-based Solution for Detecting Diploma Fraud. *IEEE Access*.

BCGOV. (2023). *VON Network.* Obtenido de GitHub: https://github.com/bcgov/von-network/tree/main

Centro de Finanzas Alternativas de la Universidad de Cambridge. (2023). *Índice de Consumo de Bitcoin.* Cambridge, UK: Centro de Finanzas Alternativas de la Universidad de Cambridge.

Christopher C. Brown, M. J. (2019). A Review of Countermeasures to Diploma Fraud. *Journal of Education for Business*, 27-33.

Del Valle, J. (2023, December). *TFM_Jose_Delvalle.* Obtenido de GitHub: https://github.com/jdelvalle10/TFM_Jose_Delvalle

Hui Zhang, N. L. (2022). RBFT: A Robust Byzantine Fault Tolerance Protocol for Blockchains. *IEEE Transactions on Parallel and Distributed Systems, Volume 33*, 256-270.

Hyperledger. (2023). *Github.* Obtenido de aries-cloudagent-python: https://github.com/hyperledger/aries-cloudagent-python

Hyperledger. (2023). *GitHub.com.* Obtenido de Aries RFC 0593: JSON-LD Credential Attachment format for requesting and issuing credentials.

Hyperledger Foundation. (2018, December 4). *Hyperledger Ursa*. Obtenido de Hyperledger Foundation: https://www.hyperledger.org/blog/2018/12/04/welcome-hyperledger-ursa

Hyperledger Foundation. (2023). *Hyperledger Foundation*. Obtenido de Hyperledger Aries.

Hyperledger Indy. (2018). *Overview of the system*. Obtenido de Indy Plenum: https://hyperledger-indy.readthedocs.io/projects/plenum/en/latest/main.html

Hyperledger Indy. (2023). *Hyperledger Indy.* Obtenido de ReadtheDocs: https://hyperledger-indy.readthedocs.io/en/latest/index.html

Hyperledger Indy. (2023, November). *Indy Walkthrough.* Obtenido de Github Hyperledger: https://github.com/hyperledger/indy-sdk/blob/main/docs/getting-started/indy-walkthrough.md

John W. Creswell, V. L. (2018). *Mixed Methods Research: A Synthesis of Methods and Approaches.*

Johnston, D. (2017). Proof of Authority: A Consensus Mechanism for Blockchains. *IEEE Security & Privacy*, 15, 3 40-52.

Khovratovich, D. &. (2017). Sovrin: digital identities in the blockchain era. *Real World Crypto Symposium*, 1-9.

Lamport, L. S. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems. *TOPLAS*, 382-401.

Michael J. Stevens, S. E. (2018). The Global Problem of Fake Diplomas. *Journal of Higher Education*, 961-983.

Michael K. Reiter, A. A. (2015). Byzantine Fault Tolerance: A Survey. *IEEE Transactions on Dependable and Secure Computing, Volume 12*, 410-446.

Province of British Columbia. (2023). *Digital Trust*. Obtenido de Digital Government: https://digital.gov.bc.ca/digital-trust/

Reed, D. H. (2016). Sovrin: An identity metasystem for self-sovereign identity. *Self-Sovereign Identity Workshop.*

Rossetti, M. G. (2019). Mixed methods research in educational research: A review of the literature. *Educational Research Review*, 26, 1-14.

Sankarshan Mukhopadhyay, L. K. (2023). *Sovrin Ecosystem Governance Framework V3.1.* The Sovrin Foundation.

Schema.org. (2023). *Educational Occupational Program.* Obtenido de Schema.org: https://schema.org/EducationalOccupationalProgram

Tang, W. (2017). A Comparison of Proof of Work, Proof of Stake, and Proof of Authority Consensus Algorithms. *arXiv*.

World Wide Web Consortium. (2022, March). *Verifiable Credentials Data Model v1.1*. Obtenido de W3C Recommendation: https://www.w3.org/TR/vc-data-model/#abstract

World Wide Web Consortium. (2023). *Decentralized Identifiers (DIDs) v1.0.* Wakefield: W3C.

World Wide Web Consortium. (2023). *Verifiable Credentials Data Model v2.0.* Wakefield: W3C.

ZeroMQ. (2023). *ZeroMQ Request for Comments*. Obtenido de Project ZeroMQ: https://rfc.zeromq.org/spec/26/