

Explorando el potencial de las microcredenciales y la tecnología Blockchain para la Transformación Digital en la Educación Superior

Mauro Cambarieri, Alejandra Viadana, Sofía
Rached Galera, Michelle Jesús Jauge, Nicolás García Martínez

Laboratorio de Informática Aplicada, Universidad Nacional de Río Negro, Argentina

{mcambarieri,caviadana,ngarciam}@unrn.edu.ar, msofiarached@gmail.com,
michellejauge@gmail.com

Abstract. En un contexto de Gobierno Digital, las entidades públicas se encuentran activamente explorando el potencial de tecnologías innovadoras. En particular, Blockchain ofrece numerosos beneficios, así como también desafíos para el sector público. Esta tecnología proporciona un registro descentralizado e inmutable de transacciones, lo que garantiza la integridad, seguridad y autenticidad de los datos. Bajo estas condiciones se logra una mayor confianza en los servicios gubernamentales, desde la emisión de documentos oficiales hasta la gestión de la identidad digital de los ciudadanos. La transformación digital de las entidades públicas se impulsa tanto en la gestión interna como en la prestación de servicios más eficientes y transparentes a los ciudadanos. En el año 2022, el Laboratorio de Informática Aplicada (LIA) de la UNRN se unió a un proyecto liderado por BID Lab, el cual desarrolló un ecosistema Blockchain en América Latina y el Caribe - Alianza LACChain- conformada por un grupo de organizaciones. El Proyecto LACChain tiene como objetivo enfocarse en aprovechar las oportunidades que la tecnología ofrece para la región, haciéndola viable. Esta Alianza permitió el despliegue de un Nodo escritor en los servidores del LIA para realizar pruebas. En cuanto al diseño de una Identidad Digital Autogestionada, esta da la posibilidad a cada individuo la administración de sus datos y la forma en que serían presentados a terceros. Por otro lado, la emisión y verificación de documentos (credenciales digitales como títulos, licencias, etc) establece un nivel de seguridad, transparencia y confiabilidad en los procesos de emisión que evitará la manipulación por parte de terceros. Este proyecto analiza y explora la tecnología blockchain en el sector público, en particular, la emisión de microcredenciales a través de credenciales verificables, destacando su capacidad para garantizar la integridad de los elementos certificables, como puede ser, trayectos formativos, títulos académicos, y sistemas de reconocimiento.

Keywords: Blockchain, Web 3.0, Identidad Digital Autogestionada, Credenciales Verificables, Microcredenciales, Empleabilidad, Educación Superior.

1 Iniciativa del Proyecto

La responsabilidad de identificar a los ciudadanos es de los diferentes Estados Nacionales, para esto, se emite una credencial única a cada ciudadano que es válida para acreditar la identidad de los mismos frente a los servicios, tanto de los sectores

públicos como privados con los que interactúan. Entender cuáles son los beneficios y el funcionamiento de la aplicación de Blockchain y su aporte en el proceso de transformación digital, permitirá conocer su potencialidad y comprender de manera precisa cómo facilitará la recepción y entrega de información auténtica y verificable.

Blockchain, plantea una revolución tecnológica que repercute directamente en cambios organizacionales, económicos y políticos. Esta nueva era del internet del valor, la Web 3, implica un gran desafío de adaptación y oportunidad hacia la transformación digital, económica, social y política de nuestras sociedades. Podemos destacar diferencias que existen entre dos modelos para gestionar la información en la web: Web 2 y Web 3, y mencionar algunas de ellas en relación a los servicios, privacidad y seguridad. La importancia de la Web 3, ofrece una alternativa al deterioro del status quo digital. La Web 2.0 [1] [7] o "web de lectura y escritura" permitió la llegada de las interacciones del usuario y las redes sociales, como también sus debilidades. Una de ellas y considerada de mayor importancia, es la extrema centralización de la información incluida en las principales plataformas (por ej, LinkedIn, facebook, etc.). Estas controlan un porcentaje significativo del tráfico y la infraestructura web, y esto tiene importantes implicaciones sobre la privacidad, la seguridad, la identidad y los datos de los usuarios, ya que estas son "dueñas" de la información, generando un monopolio de los proveedores.

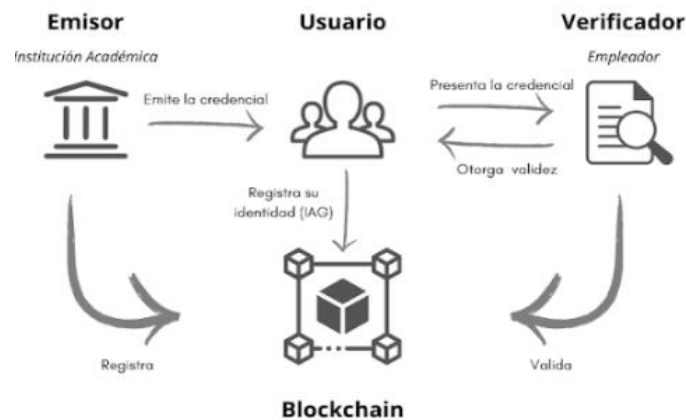
De la Web 3 se espera que sea una red completamente descentralizada, sin "censura", de forma segura sin temor de los usuarios para compartir información y que la misma no sea borrada o modificada [2]. Blockchain, mantiene una lista de registros transaccionales irrevocables, ordenado cronológicamente y firmado criptográficamente, compartido por todos los nodos de la red, "eliminando" intermediarios y garantizando integridad y consistencia de los datos al registrar el historial de todas las transacciones. Esta tecnología implicará un gran desafío de adaptación y una gran oportunidad hacia la transición digital, educativa, económica, social y política de nuestras sociedades. [5]. La adopción permitirá una internet más segura que la actual [3], pondrá el poder de la información en manos de las comunidades y no de las empresas. En resumen [4], se puede destacar las principales características de la Blockchain: Consenso, Descentralizada (P2P); Criptografía; Inmutabilidad.

Algunos conceptos claves que se incluyen en esta nueva internet: La identidad digital Autogestionada (IAG) permite a un individuo poseer y gestionar su identidad sin la intervención de las autoridades centrales. La IAG permite a las personas interactuar en el mundo digital con la misma libertad y capacidad de confianza que en el mundo físico") [9].

La Unión Europea [7] señala que los problemas de seguridad y falta de estándares en la identidad digital son preocupantes, lo que resalta la importancia de contar con sistemas escalables, interoperables, portátiles, seguros, con capacidad de recuperación, con opción de seudónimo y que generen valor para los usuarios, como propone Allende en su libro [6].

En la Web 2, los individuos carecen de control sobre sus datos y credenciales digitales, ya que estos son almacenados por terceros proveedores de servicios y de identidad. La literatura sobre Identidad Digital Autogestionada respalda los 10 principios establecidos por Christopher Allen en 2016 [9], que incluyen el acceso, consentimiento, control, independencia, interoperabilidad, minimización de reclamos,

persistencia, protección de datos, portabilidad y transparencia. Este enfoque permite a los individuos administrar sus datos, como títulos académicos y certificados oficiales, mediante billeteras digitales en aplicaciones móviles. La confianza se vuelve crucial en esta era digital, especialmente en transacciones financieras y trámites públicos, donde la transparencia, y la integridad de la información honorable son esenciales. Y contar con la identificación y autenticación electrónica, es relevante tener el control de nuestros datos pudiendo decidir en todo momento con quién, cómo y con qué fin los compartimos [6].



W3C [13]. El flujo de trabajo.

En tanto que, las Credenciales Verificables, definen un conjunto de declaraciones (atributos sobre una persona) que es realizada por un emisor, incluyendo un identificador y metadatos que describen las propiedades [4] [8], a prueba de manipulaciones que demuestran criptográficamente quién la ha emitido.

Estas credenciales verificadas [12] podrían ser un instrumento para ser usado por los estudiantes en casos de necesidad de ser presentados en otras universidades. Es esperable que dichas credenciales verificadas por Blockchain sean propiedad de los usuarios, dando integridad y confianza al emitirlas [14]. Esto mejorará el manejo de los datos y documentos relevantes para la trayectoria de los estudiantes y así generar autonomía al momento de presentarlos a terceros.



Estructura básica de afirmaciones: W3C

Declaración de afirmaciones

La W3C proporciona una especificación, una forma estándar de expresar credenciales en la Web de una manera que sea criptográficamente segura, respete la privacidad y sea verificable por “máquinas” [13].

Objetivos del Proyecto

Objetivo Principal. Diseñar una plataforma basada en la tecnología Web 3.0 para emisión de credenciales digitales (en particular, microcredenciales) utilizando tecnología Blockchain impulsando la transformación digital en la Educación Superior.

Objetivos Específicos

- Elaborar recomendaciones sobre normativas que permitan la emisión de credenciales digitales.
- Investigar la tecnología subyacente (Web 3: Blockchain, billeteras digitales, estándares, formato de datos)
- Especificar los requerimientos funcionales para el despliegue de la plataforma de servicios de certificados digitales.
- Capacitar a la institución en la tecnología Web 3 sobre emisión de credenciales digitales.
- Implementar un modelo descentralizado para la emisión y verificación de credenciales digitales para acreditar habilidades y competencias obtenidas en el ámbito no formal y formal
- Generar credenciales que sean portables y reconocidas de manera transfronteriza.
- Validar el diseño, pasible de ser implementado y transferido a otras instituciones educativas.

Caso de estudio: Microcredenciales para la Empleabilidad en la UNRN

En el año 2022, el Consejo de la Unión Europea [15] aprobó una recomendación para promover el uso de microcredenciales en toda la Unión Europea generando posibilidad de acreditar competencias, habilidades, conocimientos breves y específicos, obtenidos en períodos cortos de tiempo en ámbitos de la educación formal, no formal e informal. Estas recomendaciones apuntan a fortalecer el sistema de acreditación que permitan generar reconocimiento dentro del mercado laboral, mejorando la inclusión en el ámbito formal, dado que las mismas se generaron en diferentes instancias de su vida y dentro del mundo laboral.

El marco normativo que requiere el proyecto para su implementación, se encuentra en proceso de trabajo (Anexo) que permite determinar de qué manera se gestionan las microcredenciales en el ámbito de la Carrera de la Lic. En Sistemas. En la siguiente imagen se muestra un ejemplo de un trayecto formativo para que el estudiante pueda obtener la microcredencial, certificando actividades académicas.

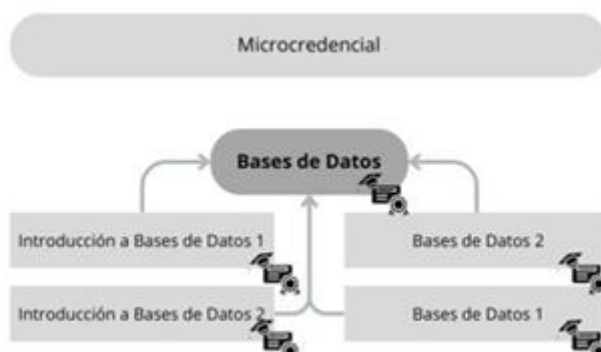


Fig. Trayectos formativos/ Microcredenciales

Software y Tecnologías Aplicadas.

Para la preparación de la prueba de concepto para el diseño de la plataforma de emisión y verificación de credenciales, se llevó a cabo una investigación exhaustiva y una implementación preliminar de diversas herramientas, como OpenCerts y Blockcerts. OpenCerts, apoyado por Skills Future Singapur 1 y el Consorcio OpenCerts, se destaca por su enfoque en la emisión y validación segura de certificados académicos a través de un esquema de código abierto y herramientas criptográficas. Esta plataforma facilita la publicación y verificación de credenciales educativas, garantizando su autenticidad e integridad mediante un portal en línea.

Por otro lado, Blockcerts2 es un estándar abierto desarrollado por el MIT Media Lab y Learning Machine. Su principal función es la creación y verificación de certificados digitales basados en blockchain. Hace uso de herramientas como cert-tools3 y cert-issuer4. Blockcerts permite personalizar certificados y asegurar que se cumplan con los estándares antes de su registro en la cadena de bloques.

Actualmente, estamos llevando a cabo una investigación e implementación de QuarkID5 y Digital Credentials Consortium (DCC)6. Estas herramientas nos están proporcionando nuevas formas en la emisión y verificación de credenciales y la gestión descentralizada de identidades, lo que abre nuevas posibilidades en el proyecto y factibles de implementar.

Digital Credentials Consortium (DCC)

El DCC busca modernizar la emisión, administración y verificación de credenciales

¹ <https://www.skillsfuture.gov.sg/resources>

² <https://www.blockcerts.org/>

³ <https://github.com/blockchain-certificates/cert-tools>

⁴ <https://github.com/blockchain-certificates/cert-issuer>

⁵ <https://quarkid.org/>

⁶ <https://digitalcredentials.mit.edu/>

académicas mediante tecnología de código abierto. A pesar de los avances tecnológicos en la educación, las credenciales educativas no han evolucionado lo suficiente. El DCC plantea preguntas sobre cómo deberían ser los títulos y certificados en la actualidad, destacando la necesidad de una autenticación confiable. Su objetivo es rediseñar el proceso de reconocimiento y transacción de credenciales en el ámbito educativo.

Características.

Implementación de protocolos estandarizados por la W3C⁷ para la creación de credenciales verificables, lo que garantiza que las mismas sean portátiles, seguras y puedan ser utilizadas en diferentes contextos.

Billetera virtual de código abierto: Una de las características clave del DCC es su billetera virtual, que permite a los usuarios el control y acceso de manera segura de las credenciales digitales, de forma sencilla, aumentando la portabilidad y confiabilidad de los documentos académicos y profesionales. La misma es interoperable, lo que significa que las credenciales emitidas por diferentes instituciones pueden ser almacenadas y verificadas dentro de un mismo ecosistema.

Desafíos

Actualmente DCC no proporciona una persistencia descentralizada de datos. Aunque las credenciales emitidas y verificadas son seguras, la falta de almacenamiento verdaderamente descentralizado podría limitar la resiliencia y confiabilidad de los datos a largo plazo. Este aspecto plantea retos en la gestión de credenciales en contextos donde la soberanía y la independencia de una autoridad centralizada son esenciales.

QuarkID

QuarkID es un protocolo de identidad digital auto soberana que utiliza tecnologías descentralizadas para mejorar la gestión, almacenamiento y verificación de identidades digitales. Ofrece una infraestructura segura que permite a los usuarios ser los propietarios de su información personal. Este protocolo se basa en blockchain, identificadores descentralizados (DIDs) y credenciales verificables (VCs), proporcionando mayor privacidad, control y confianza.

Características

- Descentralización y control del usuario: QuarkID elimina la necesidad de autoridades centralizadas, permitiendo que los usuarios gestionen sus identificadores digitales de manera directa. Esta descentralización asegura que los datos personales estén bajo el control exclusivo de los individuos, sin intervención de terceros.
- Interoperabilidad y estándares abiertos: El protocolo está diseñado para ser interoperable con diferentes sistemas y plataformas, utilizando estándares comunes para facilitar la integración y el intercambio de información. Esto permite que las identidades digitales y las credenciales sean utilizadas en diversos contextos y plataformas.
- Privacidad y seguridad: Utiliza criptografía y tecnología blockchain para garantizar

⁷ <https://www.w3.org/TR/vc-data-model-2.0/>

la seguridad y autenticidad de las credenciales digitales. Los usuarios pueden compartir solo la información mínima necesaria para cada transacción, protegiendo su privacidad y reduciendo el riesgo de exposición de datos personales.

Desafíos

- Técnica: La implementación de QuarkID puede requerir conocimientos técnicos avanzados sobre blockchain, DIDs y VCs, lo que podría ser una barrera para las organizaciones.
- Adopción: La transición a un modelo descentralizado puede enfrentar resistencia y desafíos en términos de adopción generalizada y adaptación a nuevos sistemas.

Nuestras investigaciones y pruebas con las diferentes herramientas: OpenCerts, Blockcerts, QuarkID y DCC nos han permitido explorar diferentes alternativas para el diseño e implementación de la plataforma para la emisión y verificación de credenciales verificables. Cada una de estas soluciones ofreció características únicas y comunes, y también ventajas y desventajas en el análisis de encontrar cada una de las implementaciones en la gestión de identidades y credenciales verificables.

En el caso de Blockcert y Opencert, hemos logrado avanzar en la implementación de estas plataformas, enfrentamos algunas dificultades técnicas que impidieron un progreso más significativo y la selección de las mismas. Los inconvenientes y desafíos técnicos surgidos durante el proceso limitaron nuestra capacidad para avanzar en la prueba de concepto. Por lo que, el enfoque del DCC, en particular, nos ha brindado una visión actualizada de cómo se pueden administrar las credenciales académicas contando con su propia billetera virtual y la utilización del estándar de la W3C como características fundamentales para su potencial adopción masiva, interoperabilidad, portabilidad y confiabilidad

Resultados obtenidos:

- Dictado de seminarios y/o cursos para desarrolladores de software.
- Definición de la Arquitectura para el desarrollo de las aplicaciones adoptando las tecnologías descentralizadas.
- Definición y selección de herramientas, enfoques, metodologías y soluciones innovadoras emergentes en el área.
- Preparación de la prueba de concepto (PoC, por sus ingles, Proof of Concept) para el diseño de una plataforma de emisión de credenciales.
- Selección de la herramienta para la implementación de la plataforma.

Resultados esperados:

- Sensibilización a la comunidad sobre tecnologías descentralizadas
- Elaboración de material para cursos de grado/posgrado en relación a Blockchain
- Implementación de la prueba de concepto en la Universidad Nacional de Río Negro.

- Generar trayectos formativos acreditables en la Licenciatura en Sistemas para la emisión de microcredenciales tomando como unidad de conocimientos (materia, conjunto de materias, unidad/es de la materia).

En resumen, la adopción de tecnología blockchain en entidades públicas y educativas representa un paso importante hacia la transformación digital, ofreciendo beneficios como la seguridad, transparencia, eficiencia y autonomía en la gestión de datos y credenciales, como también la soberanía de la identidad y el control de acceso a la información de cada persona. Sin embargo, se deben abordar desafíos como el marco regulatorio, la escalabilidad, la sensibilización y capacitación, los costos y la gobernanza para garantizar su implementación.

Referencias

- [1] O'Reilly, Tim, What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. Communications & Strategies, No. 1, p. 17, First Quarter 2007. Disponible en <https://ssrn.com/abstract=1008839>
- [2] Web 3.0 y blockchain, un cambio de paradigma para hacer negocios con los propios datos personales. Disponible en: <https://www.cronista.com/columnistas/web-3-0-y-blockchain-un-cambio-de-paradigma-para-hacer-negocios-con-los-propios-datos-personales/>
- [3] Liguori, Walter. Web 3 -The Decentralized Future. October 2022 Disponible en: DOI: 10.13140/RG.2.2.20599.09129 Practices and Patterns. Addison-Wesley (2001).
- [4] Building the digital credential infrastructure for the future. A White Paper by the Digital Credentials Consortium. Disponible en : <https://philippschmidt.org/articles/2020-01-White-paper-building-digital-credential-infrastructure-future.pdf>
- [5] Sovrin Foundation(2020). Disponible en: <https://sovrin.org/wp-content/uploads/Principles-of-SSI-V1.01-Spanish-v01.pdf>. Consultado el 20-02-2023.
- [6] Allende Marcos. El futuro de la identidad digital: auto-gestión, billeteras digitales y blockchain. Disponible en: <https://publications.iadb.org/publications/spanish/viewer/Identidad-digital-auto-soberana-El-futuro-de-la-identidad-digital-Auto-soberania-billeteras-digitales-y-blockchain.pdf>
- [7] The European Union Blockchain Observatory and Forum. (2019). Blockchain and digital identity. Disponible en https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf. Consultado el 27-11-2023.
- [8] Credentials. World Wide Web Consortium (W3C). Disponible en: <https://www.w3.org/TR/vc-data-model/#credentials>. Consultado 15-03-2024
- [9] Christopher Allen. The Path to Self-Sovereign Identity” Disponible en: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
- [10] Blockchain en la administración pública: Mucho ruido y pocos bloques (Pág 56) Banco Interamericano de Desarrollo. 2019. Disponible en <http://dx.doi.org/10.18235/0001951>
- [11] Grech, A. and Camilleri, A. F. 2017. Blockchain in Education. Brussels, European Commission. Disponible en: <https://doi.org/10.2760/60649>
- [12] Credentials, Reputation, and the Blockchain. J. Philipp Schmidt. Disponible en: <https://er.educase.edu/articles/2017/4/credentials-reputation-and-the-blockchain>. Consultado 20-02-2024
- [13] World Wide Web Consortium (W3C). Disponible en: <https://www.w3.org/>. Consultado 20-02-2024
- [14] Han, M., et al (2018). A novel blockchain-based education records verification solution. In Proceedings of the 19th Annual SIG Conference on Information Technology Education (pp. 178-183). <https://doi.org/10.1145/3241815.3241870>.

[15] Propuesta de Recomendación del Consejo relativa a un enfoque europeo de las microcredenciales para el aprendizaje permanente y la empleabilidad. Disponible en: <https://data.consilium.europa.eu/doc/document/ST-9237-2022-INIT/es/pdf>. Consultado 01-06-2023

ANEXO:

https://drive.google.com/file/d/1HZMSJzH_BvsafOnS0WdoWLrrg1P3mcEZ/view?usp=sharing