

Transformación Digital en Entidades Públicas: Explorando el potencial de la Tecnología Blockchain en la Gestión de Identidad y Emisión de Credenciales

Mauro Cambarieri, Claudia Alejandra Viadana, Nicolás Garcia Martinez, Luis Vivas,
Rached Sofia, Michelle Jauge

Universidad Nacional de Río Negro (UNRN), Laboratorio de Informática Aplicada LIA,
Sede Atlántica, Viedma, Río Negro

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

Resumen. 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 en la Administración Pública Nacional (APN). Esta tecnología proporciona un registro descentralizado e inmutable de transacciones, lo que garantiza la integridad, seguridad y autenticidad de los datos, bajo estas condiciones logrando 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 Global que se consolidó, permitió el despliegue de un Nodo escritor en los servidores del LIA para realizar pruebas. El diseño de una Identidad Digital Autogestionada, 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 trabajo explora la adopción de la tecnología Blockchain en el sector público para la gestión de la identidad digital y la emisión de credenciales presentando conceptos, detalles técnicos de aplicación y explicando el contexto para su utilización, así como beneficios asociados y recursos técnicos necesarios.

Palabras clave: Gobierno Digital, Transformación Digital, Blockchain LACChain, Identidad Autogestionada, Credenciales Digitales.

1 Situación, Problema u Oportunidad.

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. En relación a esto, entender cuáles son los beneficios y el funcionamiento de la aplicación de la tecnología Blockchain y su aporte en el proceso de transformación digital y desarrollo de servicios públicos digitales innovadoras, permitirá conocer su potencialidad y entender 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 una gran oportunidad hacia la transformación digital, económica, social y política de nuestras sociedades. Es por ello que, podemos obtener diferencias que existen entre dos modelos para gestionar la información: Web 2 y Web 3.

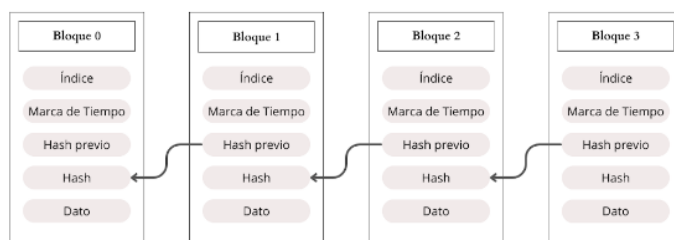
Podemos mencionar algunas de las diferencias existentes entre la Web 2 y Web 3 (“internet del valor”) en relación a los servicios, privacidad y seguridad. La importancia de la tercera era de internet (Web 3.0), ofrece una alternativa al deterioro del status quo digital. La Web 2.0 [1] [7] o “web de lectura 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 incluidas en las principales plataformas (por ej, Facebook, LinkedIn, 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 para los usuarios para compartir información y que la misma no sea borrada o modificada [2], como evolución de la Web 2.0. La tecnología blockchain, da la facilidad que una lista de registros transaccionales sea irrevocable, 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. 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. A continuación, se presentan algunos conceptos claves que se incluyen en esta nueva internet: La identidad digital autogestionada 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], por otro lado, las Credenciales Verificables, definen un conjunto de declaraciones (atributos sobre una persona) que es realizada por un emisor. [4], a prueba de manipulaciones que demuestran criptográficamente quién la ha emitido.

El proyecto analiza y explora la tecnología blockchain en el sector público, en particular, en credenciales digitales, destacando su capacidad para garantizar la integridad de los elementos certificables, por ejemplo, títulos académicos, a través de billeteras digitales en aplicaciones móviles. La próxima sección explorarán conceptos y el caso de estudio: Microcredenciales para la empleabilidad.

2 Conceptos utilizados

2.1 ¿Qué es Blockchain?



Blockchain, esta tecnología de registro distribuido (DLT- por sus siglas en inglés Distributed Ledger Technology) facilita una lista ordenada cronológicamente de registros transaccionales irrevocables y firmados criptográficamente que comparten todos los participantes de una red. Cualquier participante con los derechos de acceso adecuados puede rastrear un evento transaccional, en cualquier momento de su historia, perteneciente a cualquier actor de la red. La tecnología almacena las transacciones de forma descentralizada. Las transacciones de intercambio de valor se ejecutan directamente entre pares conectados y se verifican de forma consensuada mediante algoritmos a través de la red. La introducción de Blockchain, plantea una revolución tecnológica que repercute directamente en cambios organizacionales, económicos y políticos. Esta nueva era del internet del valor, blockchain y la Web 3, implicarán un gran desafío de adaptación y una gran oportunidad hacia la transición digital, económica, social y política de nuestras sociedades. [5].

Satisfaciendo las diferentes necesidades dependiendo del caso de uso y los requisitos, y según la normativa ISO, hay una amplia variedad de implementaciones de blockchain, mecanismos de consenso y modelos de arquitectura.

En resumen [4], las principales características de las cadenas de bloques son:

- Consenso: Todas las transacciones son validadas por los nodos participantes; un mecanismo de consenso garantiza la integridad del libro de contabilidad.
- Descentralizada: Red entre iguales (P2P), sin intermediarios.
- Criptografía: El hash y las firmas digitales garantizan la integridad y la propiedad de los datos.
- Inmutabilidad: Una vez escritos, los datos no pueden alterarse ni eliminarse de la red.

¿Cuál es el concepto de Identidad (Digital)?

La identidad, entendida como el conjunto de características distintivas que diferencian a un individuo de otro, puede comprender aspectos físicos, de género, biométricos o de pertenencia. Este conjunto de atributos, en constante cambio y evolución, puede ser definido de manera limitada y exclusiva para identificar y autenticar a un individuo frente a terceros. La identidad digital amplía esta definición al consistir en un conjunto finito de atributos que permite la identificación y validación electrónica, otorgando unicidad dentro de un contexto específico. Aunque la verificación de la identidad digital presenta desafíos al

no basarse en comparaciones visuales entre las características físicas de un individuo con las de su documento de identidad para validar quién es, sin embargo, plantea ventajas al permitir acceso a servicios digitales, de forma remota en un mundo cada vez más digitalizado. Y contar con la identificación y autenticación electrónica, es relevante para que podamos saber con quién estamos interactuando y tengamos el control de nuestros datos pudiendo decidir en todo momento con quién, cómo y con qué fin los compartimos [6].

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].

¿Qué es una credencial verificable?

“Una credencial verificable es un conjunto de declaraciones y metadatos a prueba de manipulaciones que demuestran criptográficamente quién la ha emitido”.

Es una credencial verificable a prueba de manipulaciones donde la autoría se puede verificar criptográficamente, esta puede representar todos los datos que representa una credencial física. La incorporación de tecnologías como la firma digital hace que las credenciales sean más seguras y fiables que las credenciales físicas. Una credencial es un conjunto de afirmaciones o declaraciones (atributos sobre una persona) realizadas por un emisor, pueden incluir un identificador y metadatos que describen las propiedades (fecha y hora de caducidad, una imagen, una clave pública que se utilizará con fines de verificación, el mecanismo de revocación, etcétera). [8].



Estructura básica de afirmaciones: W3C



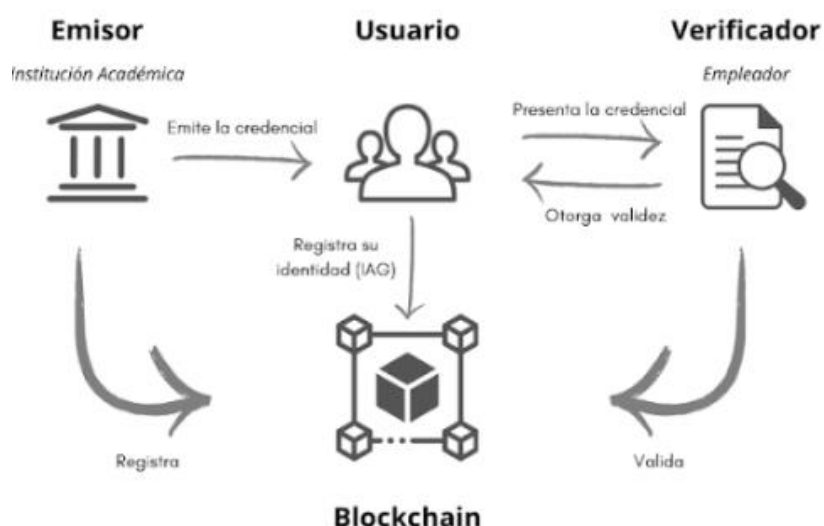
Declaración de afirmaciones

¿Cuál es el rol de la identidad Digital Autogestionada?

En la actualidad (Web2), 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.

Relacionando la Identidad digital y Credenciales verificables

El ecosistema, está dado el proceso y los actores dado el modelo de la W3C [13]. En un proceso de verificación de credenciales en una red blockchain, se realizan al instante sin compartir datos personales y garantizando una información descentralizada que no se puede manipular. El esquema seguido para la emisión y gestión de las Credenciales Verificables(VC) permite a los individuos una total independencia en la gestión de las mismas: esto posibilita la identidad autogestionada de los datos en poder de estos. Un ejemplo de flujo de trabajo que describe la emisión, intercambio y gestión de CV es el siguiente:



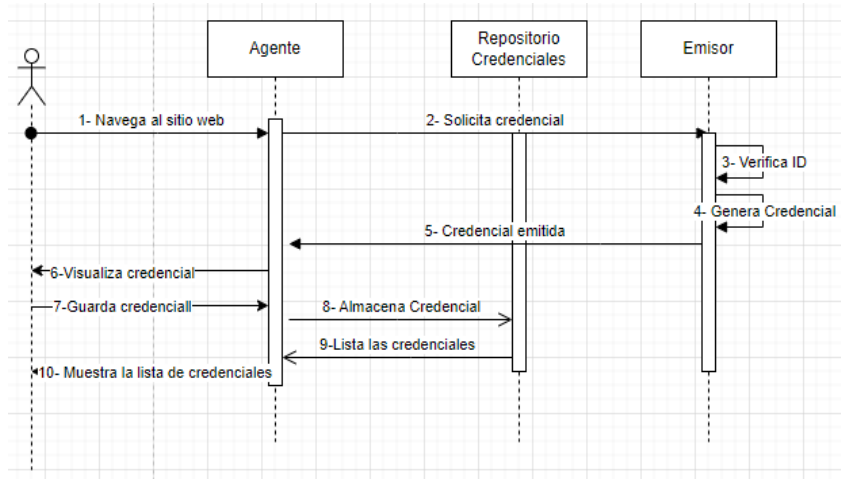
Emisor: Un emisor de credenciales puede ser cualquier entidad. Se pueden emitir de cualquier tipo, y ofrecen distintos niveles de seguridad en función de quién sea el emisor de esa credencial. El emisor envía las VC directamente al titular.

Titular: es el que recibe VC firmadas digitalmente de uno o varios emisores. Una vez enviada la credencial, éste es capaz de gestionarla de forma totalmente autónoma: de hecho, puede presentarla a quienes la soliciten, sin que el emisor intervenga en ningún momento. Las VC reproducen el mundo de las credenciales físicas en un entorno digital.

Verificador: Puede ser cualquier entidad responsable de "verificar" las VC que el titular expone. La credencial contiene todos los datos necesarios para verificarla, como quién es el Emisor, a nombre de quién está registrada y si se ha modificado o no a lo largo del tiempo.

Registro de Datos Verificables (Verifiable Data Registry- VDR) La tecnología Blockchain se utiliza para comprobar la validez de la credencial que posee el Titular.

El siguiente diagrama de secuencia muestra cómo interactúa y se relaciona una situación típica sobre una solicitud de una credencial verificable.

Diagrama de flujo de creación de credenciales verificables¹

3 La importancia de Blockchain.

3.1 En el sector público

El sector público se encuentra en un reto, donde se espera que este proporcione servicios públicos de calidad de manera eficiente y transparente, con recursos limitados. En este contexto, la tecnología Blockchain emerge como una poderosa herramienta que podría mejorar la eficiencia y la transparencia de los servicios públicos. Considerando las diversas acciones que se están evaluando en el ámbito público y tomando en cuenta las características inherentes a la tecnología, se identifican cuatro áreas claves en las cuales se podría considerar que la tecnología blockchain podría resultar beneficiosa [10]:

1- *Eliminación de intermediarios en la gestión de información*: En muchas ocasiones, la generación de información en el ámbito público implica una secuencia de procesos que involucran a diversas personas o entidades. En tanto el uso de blockchain, es factible para registrar la información de manera segura y fiable, convirtiendo la red en un tipo de notario digital para datos y transacciones. Integrar estos procesos en una cadena de bloques tiene el potencial de eliminar algunos intermediarios, mejorar la trazabilidad de cada etapa del proceso de manera confiable y reducir el tiempo y los recursos asociados.

2. *Tokenización de activos*: La tecnología ofrece la posibilidad de representar activos mediante “tokens” digitales, facilitando un registro confiable de los cambios de propiedad o ubicación en cadenas de producción. Esta característica también permite la división de la propiedad de un solo activo entre varios propietarios.

3. *Automatización de procesos*: Un aspecto clave de registrar contratos inteligentes en un sistema distribuido es la capacidad de automatizar procesos mediante la definición de reglas

¹ <https://www.w3.org/TR/vc-use-cases/#user-sequences>

que deben cumplirse para ejecutar acciones específicas de manera automática, sin necesidad de intermediarios de confianza. Ejemplos: Pagos en transferencias condicionadas, facturación de bienes y servicios tras su entrega, también cumplimiento de diversas regulaciones.

4. *Mejora de la interoperabilidad (de borde)*: El desafío principal para la prestación integrada de servicios públicos reside en la seguridad y confiabilidad de conectar sistemas de entidades públicas y privadas. La utilización de blockchain para certificar información ciudadana permite facilitar la interoperabilidad de sistemas sin necesidad de una integración directa, ya que ellos mismos pueden otorgar permisos en tiempo real de sus datos e información personal.

Estas tecnologías emergentes, especialmente aquellas que manejan información personal, demandan que el sector público tenga un conocimiento básico de su funcionamiento para resguardar los derechos de los ciudadanos. A su vez, los ciudadanos necesitan comprender estas tecnologías para confiar en su aplicación. A medida que la tecnología blockchain se consolide, los casos de uso que aporten mayor valor a las administraciones públicas se tomarán más evidentes. Es probable que aquellas administraciones con una comprensión más sólida de esta tecnología lideren su adopción. Mantener un equilibrio entre la regulación y la capacidad de innovación es crucial y requiere profesionales multidisciplinarios actualizados tanto en avances tecnológicos como en regulaciones internacionales

La implementación de Blockchain no está exenta de desafíos, algunos de ellos:

Marco Regulatorio: que sea claro y consistente, que aborde cuestiones como la protección del consumidor, la privacidad de los datos y la seguridad.

Escalabilidad: para garantizar que la infraestructura blockchain pueda manejar un volumen creciente de transacciones y usuarios sin comprometer el rendimiento.

Educación y Capacitación: Capacitar en el uso y la implementación efectiva de la tecnología blockchain,

Costos: Evaluar los costos asociados con la implementación y operación de soluciones basadas en blockchain, relacionamiento y vínculo con las plataformas.

Divulgación y adopción: Promover la aceptación y confianza del público en las soluciones blockchain implementadas por el gobierno, demostrando los beneficios en términos de transparencia, eficiencia y seguridad.

Gobernanza: Establecer mecanismos de gobernanza efectivos para la gestión de la cadena de bloques, incluida la toma de decisiones, la resolución de conflictos y la supervisión de la red.

Abordar estos desafíos requerirá una colaboración estrecha entre los sectores público y privado, es crucial entender el problema, analizar el contexto, mapear los actores y diseñar la arquitectura de la solución a través de un prototipo rápido que pueda ser escalado.

3.2 En el sector educativo

La mayoría de los proyectos de blockchain en el ámbito educativo se encuentran en las etapas de pruebas. El sistema educativo presenta oportunidades para dar un uso significativo a la tecnología, algunos ejemplos:

- *Emisión y verificación de certificados digitales*: emitir certificados legalizados,

facilitando la verificación de la autenticidad de las credenciales académicas.

- *Gestión de propiedad intelectual*: Se emplea para notarizar los derechos de propiedad intelectual generados en el sector educativo, garantizando la protección y la trazabilidad de los activos digitales.
- *Financiamiento educativo*: Se exploran aplicaciones de blockchain en la gestión de fondos educativos, incluyendo el pago de matrículas y becas, así como la implementación de microcréditos para apoyar la educación.

Estos casos de uso demuestran cómo la tecnología blockchain puede ser aplicada de manera efectiva en diversos aspectos de la educación para mejorar la transparencia, la seguridad y la eficiencia de los procesos educativos, emisión de credenciales y programas académicos digitales, gestión de la identidad y los legajos de los estudiantes, pagos basados en blockchain, gestión de datos intelectuales y contratos inteligentes. [11]

La tecnología Blockchain ha sido aplicada en otros sectores como el financiero, es probable su aplicación en el ámbito académico en tanto Devine² define esta tecnología como una transferencia universal de créditos entre diferentes instituciones. Estas credenciales verificadas podrían ser un instrumento usado por estudiantes para ser usado en casos de necesidad de ser presentados en otras universidades. Es esperable que dichas credenciales académicas verificadas por Blockchain sean propiedad de los usuarios. Esto podrá mejorar el manejo de sus datos y documentos relevantes para su vida y así generar inclusión y autonomía al momento de presentarlos a terceros.

La acreditación académica sirve para demostrar que la persona estudió un grado, un curso o un programa. Esto se demuestra a través de la credencial o certificado emitido por una institución o universidad; sin embargo, ésta puede llegar a ser falsificada. En el proceso de acreditación académica se encuentran las debilidades en relación con el tiempo de emisión, la comprobación de su autenticidad y la validez.

La importancia del uso del blockchain radica en que las instituciones educativas la pueden utilizar para poder enfrentar las problemáticas del tiempo de emisión y de la realización de la acreditación académica, para que ésta sea demostrable, registrable e inmutable. Por lo tanto, dichas acreditaciones estarían resguardadas en una blockchain, con lo cual se brindaría certeza, seguridad, integridad y confianza al emitirlas [14].

4 Caso de Estudio: “Microcredenciales para la Empleabilidad”

Existe en la actualidad y en constante crecimiento, la “credencialización del aprendizaje”, generada por pequeñas unidades formativas (microcredenciales) para lograr en las personas la actualización o profundización de determinados conocimientos, habilidades y/o capacidades. 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 periodos cortos de tiempo en ámbitos de la educación formal, no formal e informal. Estas recomendaciones tienen como objetivo la implementación y reconocimiento de credenciales en diversas instituciones.

Las recomendaciones apuntan fortalecer el sistema de acreditación de competencias que

² <https://oro.open.ac.uk/44966/2/Devine2015-altc-blockchainlearning-transcript.pdf>

permitan generar reconocimiento dentro del mercado laboral, mejorando la inclusión de todos aquellos que no tienen acceso a la acreditación de sus competencias y habilidades en el ámbito formal dado que las mismas se generaron en diferentes instancias de su vida y dentro del mundo laboral.

Si bien los esfuerzos por la realización de este tipo de estrategias ha tenido un impacto significativo en la formación específica aún no son suficientes y existe la necesidad de contar con instrumentos fiables y estandarizados con el fin de tener un registro verificable de la adquisición de los conocimientos y habilidades en ámbitos formales y no formales. Para esto, se requiere pensar en proyectos innovadores que, con apoyo de la tecnología, puedan ser más eficientes y eficaces al momento de incorporarse al mercado laboral.

Al diseñar nuevas estrategias de acreditación, las microcredenciales utilizando la tecnología Blockchain podrían facilitar su entrega compartiendo información académica digital auténtica y verificable. Blockchain, “parece perfecta” y “atractiva” para el desarrollo de aplicaciones tanto en los sectores público como privado, donde la integridad de la información debe ser segura y transparente. En este caso en particular, registrar títulos, certificados y documentos oficiales que son necesarios para garantizar la autenticidad, integridad e inalterabilidad sobre las trayectorias de las personas.

¿Cómo demostramos la validez de las habilidades dentro o fuera de nuestro país? Es necesario “apostillar” los documentos para que sean válidos tanto en el país como en el extranjero. La aplicación de la tecnología Blockchain permitiría menos trámites porque soporta la emisión de certificados digitales proporcionando seguridad al “blindar” los títulos y otras certificaciones, que, una vez que son registrados en esta, son verificables en tiempo real, abriendo las fronteras de la geografía. Sin embargo, es mucho lo que está en juego, ya que un sistema de este tipo podría llegar a representar también nuestra reputación profesional, creando o limitando oportunidades. Debemos reflexionar sobre su diseño y el tipo de instituciones en las que confiamos para regirlo. [12].

La W3C desarrolla estándares para ayudar a construir una web basada en los principios de accesibilidad, internacionalización, privacidad y seguridad. Esta 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].

4.1 Diseño de la Solución

La solución se describe en términos de dos componentes principales:

4.1.1 Componente Organizacional - Normativo:

El marco normativo que se encuentra en proceso de trabajo incluye 16 artículos (Anexo I- sección bibliografía) 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 el estudiante pueda obtener la microcredencial, certificando actividades académicas y prácticas, que están diseñadas para garantizar el desarrollo integral de las competencias pertinentes al área de base de datos, que incluye: materias completas, unidades de materias, conjunto de materias, cursos, entre otros, que sean aprobados por el Consejo Asesor de la Carrera.

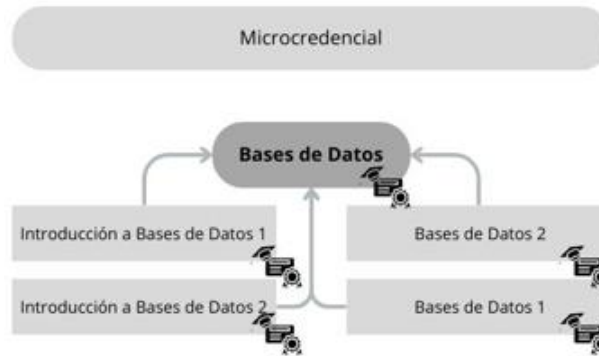
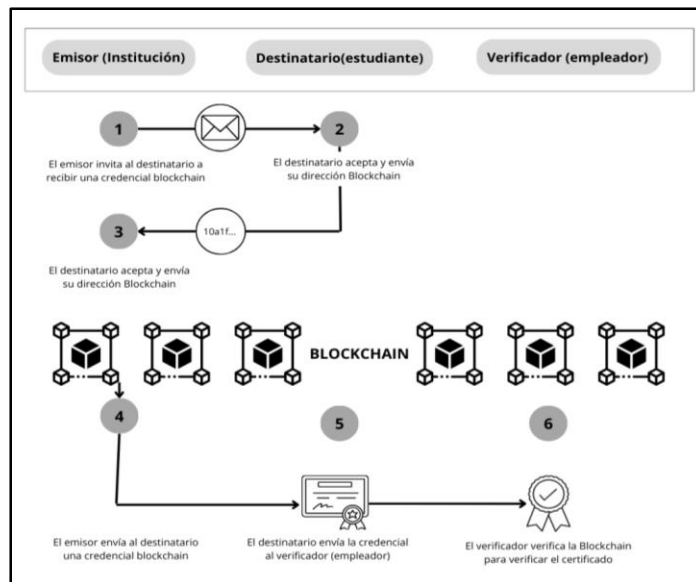


Fig. Trayectos formativos/ Microcredenciales.

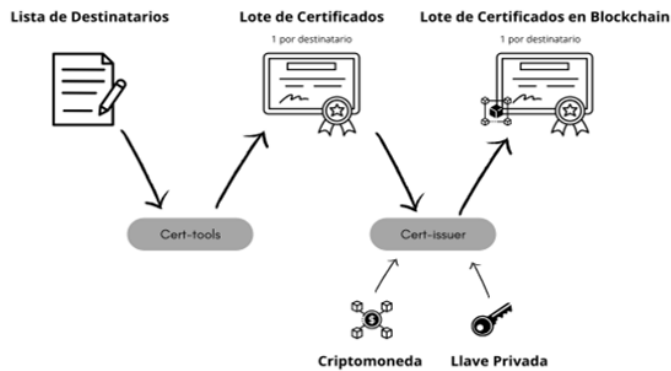
4.1.2: Software y Tecnologías Aplicadas

El estándar Blockcert. Es un estándar abierto para crear, emitir, ver y verificar certificados basados en blockchain, firmados criptográficamente, a prueba de manipulaciones y pueden compartirse. Se muestra la imagen de cómo funciona la emisión y verificación certificados digitales.



Este sistema se compone de bibliotecas, herramientas y aplicaciones móviles de código abierto que hacen posible un ecosistema descentralizado, basado en estándares abiertos. Se encuentra comprometido con la identidad auto-soberana de todos los participantes, y permite el control del receptor de sus credenciales a través de herramientas fáciles de usar, como la billetera de certificados (aplicación móvil).

Visualización y verificación de certificados. A continuación, se muestra cómo funciona la emisión de certificados de extremo a extremo utilizando los módulos de “cert-tools”, que es una biblioteca de Python para crear certificados Blockcert personalizados y “cert-issuer” que es una biblioteca de Python para emitir en la Blockchain. A modo de implementación, se encuentran los diferentes repositorios de código abierto, que el equipo de desarrollo utilizó actualmente para realizar una prueba de concepto en la emisión de certificados localmente.



Emisión de certificados de extremo a extremo. <https://www.blockcerts.org/guide/quick-start.html>

Repositorios.

A continuación, se muestra un resumen de los principales repositorios para su uso.

cert-verifier-j ³	biblioteca Javascript para la verificación en un navegador
cert-schema ⁴	los esquemas y especificaciones JSON-LD
cert-tools ⁵	biblioteca de Python para crear personalizar
cert-issuer ⁶	biblioteca de Python para emitir Blockcerts
blockcerts-verifier ⁷	un visor y verificador universal independiente
wallet-iOS ⁸ -android ⁹	billetera para agregar mantener claves y Blockcerts

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

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

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

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

7 <https://github.com/blockchain-certificates/blockcerts-verifier>

8 <https://github.com/blockchain-certificates/wallet-iOS>

9 <https://github.com/blockchain-certificates/wallet-android>

5 Conclusiones/Resultados

La transformación digital en entidades públicas mediante la implementación de tecnología blockchain para la gestión de identidad y emisión de credenciales digitales ofrece un cambio de paradigma en la manera en cómo se administran y gestionan los datos, como se presentan y se accede a diferentes servicios públicos. Este trabajo expuso definiciones, conceptos, y el diseño de una solución, como también las capacidades de la tecnología blockchain que proporciona un registro descentralizado e inmutable de transacciones, asegurando la integridad, seguridad y autenticidad de la información.

Al explorar el potencial de la tecnología blockchain, en el sector público se identifican diversas áreas en las que puede generar beneficios significativos en el sector público, como la eliminación de intermediarios en la gestión de información, la tokenización de activos, la automatización de procesos y la mejora de la interoperabilidad.

En el ámbito educativo, el uso de blockchain también presenta oportunidades importantes, especialmente en la emisión y verificación de certificados digitales (en particular, microcredenciales).

El diseño de la solución, es decir, el caso de estudio propuesto, utilizando el estándar de Blockcert, proporcionó nuestro punto de partida, contando con un producto tecnológico para la emisión, verificación y gestión de certificación digital de manera segura y confiable, acompañado con un marco normativo, que se encuentra en proceso de trabajo. En este sentido, la implementación de microcredenciales respaldadas por blockchain mejora la transparencia, seguridad y eficiencia de los procesos educativos, así como facilita la integración de personas que no tienen acceso a la acreditación formal de sus competencias y habilidades desarrolladas en ámbitos no formales.

El potencial de blockchain en la gestión de identidad y emisión de credenciales en entidades públicas revela una serie de beneficios y oportunidades significativas. A través de este trabajo, se da a conocer las tecnologías descentralizadas, que serán impulsadas por la creación de material académico y la organización de seminarios, cursos o talleres de divulgación. Esto sentará las bases para una comprensión más profunda y una adopción más amplia de estas tecnologías tanto en el ámbito público como en el educativo.

La transformación digital en entidades públicas mediante el uso de tecnologías blockchain está en sus etapas iniciales. Se necesitarán regulaciones y normativas para su adopción, lo que permitirá a las personas interactuar en el mundo digital con la misma libertad y capacidad de confianza que en el mundo físico. Existe una oportunidad para los gobiernos en los diferentes niveles de la región de aprovechar el trabajo realizado por el Comité de la Unión Europea en este tema y fortalecer así sus ecosistemas digitales.

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.educause.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: Borrador de la Normativa propuesta para la implementación de Microcredenciales en la Universidad Nacional de Río Negro. <https://drive.google.com/drive/u/0/folders/11Lsg8oiW4enHXfx1mcQrunyocKTi7zFA>