Microcredenciales y Web3: Explorando el potencial y las oportunidades para la Transformación Digital
Mauro Cambarieri, Claudia Alejandra Viadana, Nicolás Garcia Martinez, Luis Vivas, Sofia Rached, Michelle Jauge
SADIO Electronic Journal of Informatics and Operations Research (EJS) Vol. 24 No. 2 (2025) e-ISSN 1514-6774
https://doi.org/10.24215/15146774e082 | https://revistas.unlp.edu.ar/ejs
Sociedad Argentina de Informática e Investigación Operativa | Universidad Nacional de La Plata | Buenos Aires | Argentina

Microcredenciales y Web3: Explorando el potencial y las oportunidades para la Transformación Digital

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. El presente trabajo explora el potencial de la tecnología blockchain y Web3 en la transformación digital de entidades públicas, enfocándose en la gestión de identidad digital y la emisión de credenciales verificables. Se analizan conceptos clave de las tecnologías como de los estándares W3C, destacando la capacidad para garantizar integridad, seguridad, portabilidad y transparencia en procesos administrativos. En el sector público, blockchain ofrece beneficios como la eliminación de intermediarios, automatización mediante contratos inteligentes, tokenización de activos y mejora de la interoperabilidad. En educación, la acelerada evolución del mercado laboral, impulsada por avances tecnológicos y demandas de especialización dinámica, ha posicionado a las microcredenciales como componentes críticos en la reinvención profesional. Sin embargo, su implementación efectiva requiere superar desafíos de interoperabilidad, seguridad y portabilidad. Es aquí donde las tecnologías, particularmente la identidad digital y las credenciales verificables(CV), emergen como facilitador de la transformación. Las CV facilitan la emisión y verificación de certificados académicos, que promueven la empleabilidad y la portabilidad de competencias. El caso de estudio presentado utiliza el Consorcio de Credenciales Digitales (DCC, por sus siglas en inglés) para implementar CV basadas en estándares como JSON-LD e identificadores descentralizados (DID). Este trabajo presenta conceptos, detalles técnicos de aplicación y de contexto para la utilización de las tecnologías Web 3.

Palabras clave: Credenciales Verificables, Identidad Digital, Blockchain, Web 3, Gobierno Digital, Transformación Digital.

Received May 2025; Accepted June 2025; Published July 2025

Microcredentials and Web3: Exploring the Potential and Opportunities for Digital Transformation

Abstract. This paper explores the potential of blockchain and Web3 technologies in the digital transformation of public entities, focusing on digital identity management and the issuance of verifiable credentials. Key concepts of these technologies, as well as W3C standards, are analyzed, highlighting their ability to ensure integrity, security, portability, and transparency in administrative processes. In the public sector, blockchain offers benefits such as the elimination of intermediaries, automation through smart contracts, asset tokenization, and improved interoperability. In education, the accelerated evolution of the labor market—driven by technological advancements and demands for dynamic specialization—has positioned micro-credentials as critical components for professional reinvention. However, their effective implementation requires overcoming challenges related to interoperability, security, and portability. This is where digital identity and verifiable credentials (VCs) emerge as key enablers of transformation. VCs streamline the issuance and verification of academic certifications, promoting employability and the portability of skills. The case study presented leverages the Digital Credentials Consortium (DCC) to implement VCs based on standards such as JSON-LD and decentralized identifiers (DIDs). This work outlines conceptual frameworks, technical implementation details, and contextual considerations for the adoption of Web3 technologies.

Keywords: Verifiable Credentials, Digital Identity, Blockchain, Web3, Digital Government, Digital Transformation.

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 innovadores, 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, denominada - Web 3-, implica un gran desafío de adaptación y una gran oportunidad hacia la transformación digital, económica, social y política de nuestras sociedades.

Existen dos modelos para gestionar la información en internet: Web 2 (Ej. redes sociales, plataformas, etc) y Web 3 (Identidad, wallet, blockchain, NFTs, DAOs,), de ellos podemos obtener las diferencias que radican en cada uno en relación a los servicios, privacidad y seguridad.

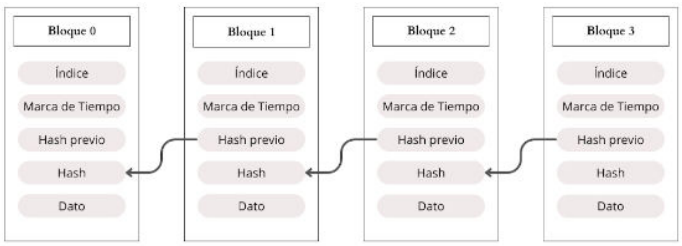
La importancia de la tercera era de internet (Web 3), ofrece una alternativa al deterioro del status quo digital. La Web 2 [1] [7] o "web de lectura y escritura" permitió la llegada de las interacciones del usuario y las redes sociales, como también sus debilidades. Una de ellas y considerada de mayor 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(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], por otro lado, las Credenciales Verificables, definen un conjunto de declaraciones (atributos sobre una persona, por ejemplo) que es realizada por un emisor. [4], a prueba de manipulaciones que demuestran criptográficamente quién la ha emitido.

El presente proyecto analiza y explora las tecnologías Web3 en el sector público, en particular, en credenciales verificables, 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 se explorará 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".

En el mundo físico, una credencial puede consistir en:

- Identificación del individuo. Información relacionada con la identificación del individuo de la credencial. (una foto, un nombre o un número de identificación)
- Emisor: Información relacionada con la autoridad emisora. (Gobierno, Institución)
- Tipo: información sobre el tipo de credencial. (Pasaporte, Licencia, certificados académicos)
- Atributos: Información relacionada con atributos o propiedades específicos que la autoridad emisora afirma sobre el individuo. (Nacionalidad, tipos de vehículos que puede conducir o fecha de nacimiento)
- Información relacionada con las restricciones de la credencial (fecha de caducidad o condiciones de uso)
- Evidencia de cómo se ha obtenido la credencial.

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 [8], que se expresan mediante relaciones sujeto-propiedad-valor.

Reclamación(Claims)

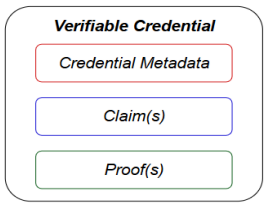
Es una declaración que se hace sobre un sujeto (individuo, por ejemplo). Un sujeto es una cosa sobre la que se pueden hacer afirmaciones, que se expresan mediante relaciones sujeto-propiedad-valor como muestra la siguiente figura.

Estructura básica de afirmaciones: https://www.w3.org/TR/vc-data-model-2.0/#basic-structure

Las declaraciones individuales pueden combinarse para expresar un gráfico de información sobre un sujeto. Los elementos del modelo de datos, ilustrado en la imagen anterior, es poderoso y puede usarse para expresar una gran variedad de declaraciones. Por ejemplo, Juan es alumno de la universidad y conoce a Pablo, y Pablo trabaja como profesor.

Ejemplos más destacados de credenciales verificables son los documentos de identidad digitales, los certificados de nacimiento y los certificados educativos. A través de las Credenciales Verificables, los ciudadanos pueden relacionarse e interactuar con el mundo digital, donde existe un sistema descentralizado de confianza en el que, hasta ahora, los datos digitales nunca han podido llegar a estar en posesión total de los individuos. Un sujeto puede realizar reclamaciones vinculados a una misma entidad y este conjunto de reclamos constituye una credencial verificable.

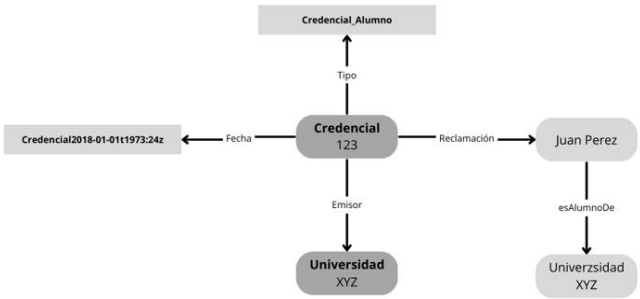
La palabra "verificable" en los términos credencial verificable se refiere a la característica de una credencial de poder ser verificada por un verificador.



Las credenciales también pueden incluir un identificador y metadatos que describan las propiedades de la credencial, como el emisor, la fecha y hora de caducidad, una imagen representativa, una clave pública que se utilizará con fines de verificación, el mecanismo de revocación, etcétera.

Estructura básica de una credencial: https://www.w3.org/TR/vc-data-model-2.0/#basic-vc

Una breve explicación, para diseñar una credencial verificable, puede expresarse de manera simple mediante el siguiente diagrama. La credencial verificable del alumno Juan Perez quien reclama ser alumno de la universidad XYZ. La universidad XYZ emitirá una credencial (123) donde indica el tipo de credencial (Credencial_Alumno) y la fecha (desde el 01 de enero del 2018) que permite demostrar a Juan Perez que es alumno de la universidad.



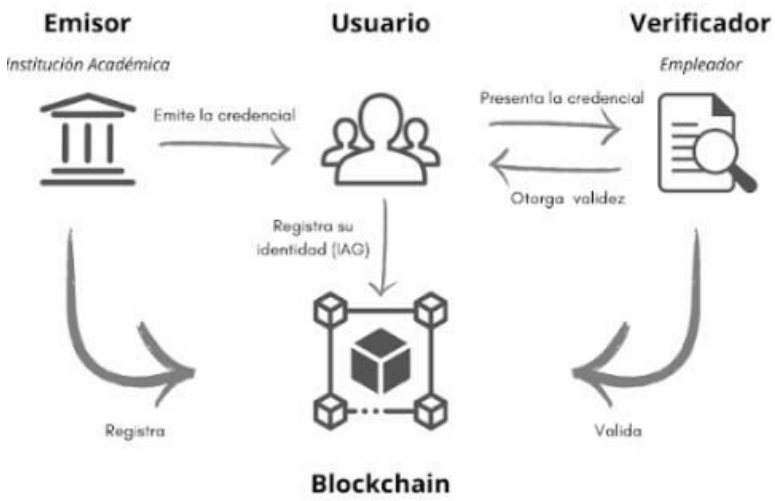
Diseño de una Credencial Verificable

¿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, por sus siglas en inglés) 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.

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.

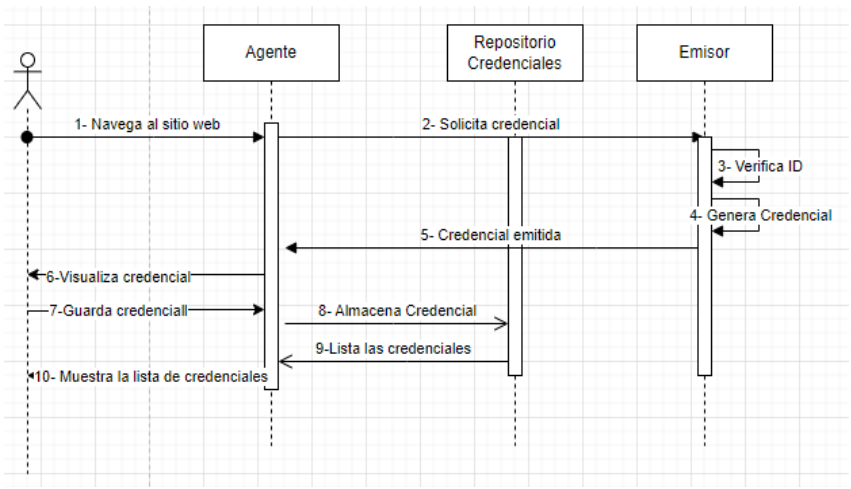


Diagrama de flujo de creación de credenciales verificables[1]

Ciclo de vida: Credenciales verificables

La Sección anterior, se describió el ecosistema de credenciales verificables. En este

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

apartado, se proporciona detalles sobre cómo se prevé que funcione ese ecosistema dado el ciclo de vida de una credencial.

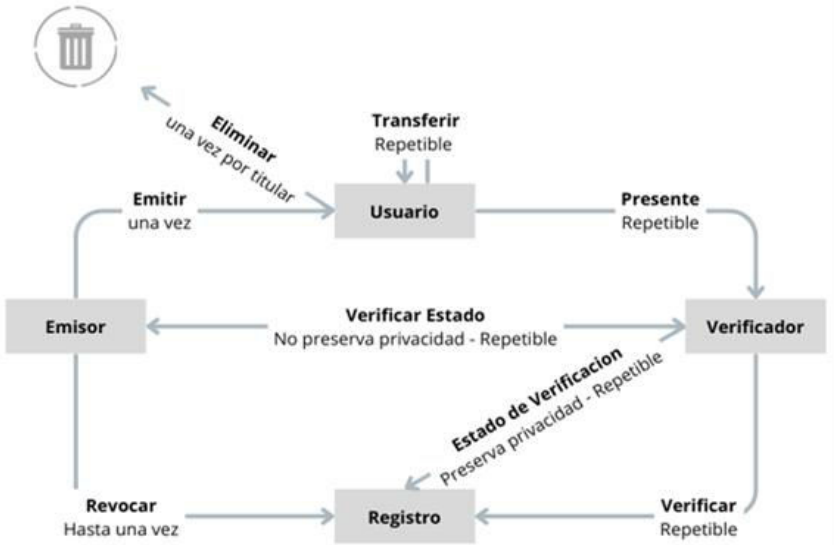


Figura representada de https://www.w3.org/TR/vc-data-model/#lifecycle-details

Las credenciales verificables son un componente crucial del ecosistema digital de confianza, que permite a las entidades emitir, poseer y verificar información de forma segura. La especificación central, el Verifiable Credentials Data Model v2.0, define los conceptos clave en términos abstractos y se serializa principalmente en JSON, aunque es posible que se desarrollen otros formatos en el futuro.

Terminología:

- Claim / Reclamo: Afirmación hecha sobre un sujeto.
- Credential / Credencial: Conjunto de uno o más reclamos hechos por un emisor sobre uno o varios sujetos.
- Decentralized Identifier (DID) / Identificador descentralizado (DID): Identificador portátil basado en URL, asociado con una entidad y utilizado en credenciales verificables.
- Default Graph / Gráfico predeterminado Gráfico que contiene todos los reclamos que no están explícitamente en un gráfico nombrado.
- Entity / Entidad: Cualquier cosa que pueda ser referenciada en declaraciones, como personas, organizaciones o conceptos abstractos.
- Graph / Gráfico: Conjunto de reclamos que forman una red de información sobre sujetos y sus relaciones.
- Holder / Titular: Entidad que posee credenciales verificables y genera presentaciones verificables.
- Issuer / Emisor: Entidad que realiza reclamos sobre uno o varios sujetos y crea credenciales verificables a partir de esos reclamos.
- Named Graph / Gráfico nombrado: Gráfico asociado con propiedades específicas, como las credenciales verificables.
- Presentation / Presentación: Datos derivados de una o más credenciales

verificables compartidos con un verificador.

- Credential Repository / Repositorio de credenciales: Software que almacena y protege el acceso a las credenciales verificables de los titulares.
- Selective Disclosure / Divulgación selectiva: Capacidad del titular para decidir qué información compartir.
- Unlinkable Disclosure / Divulgación no correlacionable: Tipo de divulgación selectiva donde las presentaciones no se pueden correlacionar entre diferentes verificadores.
- Subject / Sujeto: Cosa sobre la cual se hacen reclamos.
- Validation / Validación: Proceso para garantizar que un reclamo cumple con los requisitos de un verificador.
- Verifiable Credential / Credencial verificable: Credencial resistente a manipulaciones cuya autoría puede verificarse criptográficamente.
- Verifiable Data Registry / Registro de datos verificables: Sistema que facilita la creación y verificación de identificadores y otros datos relevantes.
- Verifiable Presentation / Presentación verificable: Presentación resistente a manipulaciones de datos cuya autoría puede ser confiada tras la verificación criptográfica.
- Verification / Verificación: Evaluación de si una credencial o presentación verificable es auténtica y cumple con las especificaciones.
- Verifier / Verificador: Entidad que recibe credenciales verificables para procesarlas.
- Verification / verificación: Información utilizada para verificar la seguridad de datos protegidos criptográficamente, como una clave pública.
- URL / URL: Localizador uniforme de recursos, una dirección que puede apuntar a un recurso, como un documento.

Modelo de datos y serialización en JSON:

El modelo de datos para las credenciales verificables define cómo representar y estructurar las credenciales, con dependencias normativas claras. La serialización en JSON asegura que todos los participantes puedan interpretar la estructura de manera coherente.

El esquema JSON es esencial para garantizar la integridad estructural de las credenciales verificables, lo que facilita la interoperabilidad entre diferentes sistemas.

Las credenciales pueden protegerse mediante pruebas envolventes o pruebas incrustadas, en ambos casos, una prueba protege criptográficamente una credencial.

- Pruebas envolventes: La protección (firmas digitales, por ejemplo) envuelve a la credencial completa.
- Pruebas incrustadas: La prueba forma parte de la propia serialización de la credencial.

Estructura y vocabularios JSON-LD:

Las credenciales se representan en JSON-LD, permitiendo un enfoque descentralizado. Los desarrolladores pueden crear vocabularios específicos para aplicaciones concretas, lo que facilita la expansión del sistema a nuevos dominios.

En el ejemplo proporcionado, una credencial que indica que una persona llamada "Sofía" es una alumna de la Universidad Nacional de Rio Negro.

```
{
  "@context": [
```

```
  "https://www.w3.org/ns/credentials/v2",
  "https://www.w3.org/ns/credentials/examples/v2"
 ],
 "id": "https://university.example/Credential123",
 "type": ["VerifiableCredential", "ExampleAlumniCredential"],
 "issuer": "did:example:2g55q912ec3476eba2l9812ecbfe",
 "validFrom": "2010-01-01T00:00:00Z",
 "credentialSubject": {
  "id": "https://www.example.org/persons/pat",
  "name": "Sofía",
  "alumniOf": {
   "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
   "name": "Universidad Nacional de Río Negro"
  }
 },
 "credentialSchema": {
  "id": "https://university.example/Credential-schema.json",
  "type": "JsonSchema"
 }
}
```


Esquema JSON para la credencial simple


```
{
 "$id": "https://university.example/schemas/credential.json",
 "$schema": "https://json-schema.org/draft/2020-12/schema",
 "title": "ExampleAlumniCredential",
 "description": "Alumni Credential using JsonSchema",
 "type": "object",
 "properties": {
  "credentialSubject": {
   "type": "object",
   "properties": {
    "alumniOf": {
     "type": "string",
     "format": "url"
    }
   },
   "required": [
    "alumniOf"
   ]
  }
 }
}
```


Identificadores Descentralizados(DID)

Los identificadores descentralizados (DID) son un nuevo tipo de identificador que permite una identidad digital descentralizada y verificable [16].

Un elemento clave de este sistema son los Identificadores descentralizados (DID): un nuevo tipo de identificador único global, diseñados para que personas y organizaciones puedan generar sus propios identificadores utilizando sistemas en los que confían. Estos nuevos identificadores permiten a las entidades demostrar el control sobre ellos mediante la autenticación con pruebas criptográficas como las firmas digitales. Sus objetivos de diseño son: descentralizados, controlados por el usuario, privados, seguros, basados en pruebas criptográficas, descubribles, interoperables, portables, simples y extensibles.

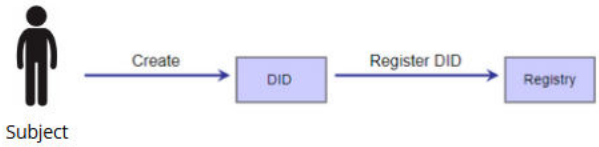


Figura tomada de: https://www.w3.org/TR/did-1.0/

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 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 tornarán 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 Devine[2] 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”

Recomendaciones del Consejo de la Unión Europea

En la actualidad, la "credencialización del aprendizaje" está en constante crecimiento.

Este proceso, basado en pequeñas unidades formativas conocidas como microcredenciales, permite la actualización y profundización de conocimientos, habilidades y capacidades de las personas.

En 2022, el Consejo de la Unión Europea [15] aprobó una recomendación para promover el uso de microcredenciales en toda la región. Esta medida busca acreditar competencias, habilidades y conocimientos específicos adquiridos en períodos cortos, tanto en educación formal como en entornos no formales e informales. Su implementación y reconocimiento en diversas instituciones tiene como objetivo fortalecer los sistemas de acreditación de competencias, facilitando la inclusión de quienes no pueden validar sus habilidades en el ámbito formal, ya que estas han sido adquiridas en distintas instancias de su vida y dentro del mundo laboral.

Microcredenciales como herramienta para la reinversión laboral

Las microcredenciales se han convertido en una herramienta clave para la reinvención profesional en un mercado laboral en rápida evolución, impulsado por avances tecnológicos y una creciente demanda de especialización. Sin embargo, su implementación efectiva enfrenta desafíos relacionados con la interoperabilidad, autenticidad y portabilidad. En este contexto, las tecnologías de la Web 3, en particular las credenciales verificables (VCs) y los sistemas descentralizados, emergen como soluciones transformadoras.

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

Las microcredenciales son certificaciones enfocadas en competencias específicas y están siendo adoptadas masivamente por instituciones educativas y empresas. Según el último informe del Foro Económico Mundial sobre el futuro del empleo, se estima que para 2027 el 61% de los trabajadores necesitará actualizar sus habilidades, mientras que se incorporarán 4 millones de nuevas funciones tecnológicas a la fuerza laboral global. En este escenario, las microcredenciales se posicionan como una estrategia fundamental para afrontar los retos del mercado laboral. No obstante, los modelos actuales presentan limitaciones críticas:

- Fragilidad en la verificación autónoma
- Riesgos de falsificación documental
- Dependencia de intermediarios centralizados

Casos de Éxito – Proyecto EBSI

Casos de estudio como el proyecto europeo EBSI demuestran cómo las VCs permiten:

- Reducción en costos de verificación de credenciales
- Validación transnacional instantánea mediante registros distribuidos
- Creación de itinerarios formativos modulares

Este modelo descentralizado impulsa la filosofía "learn-to-earn", en la cual los usuarios pueden construir identidades profesionales soberanas mediante credenciales educativas. Las plataformas Web 3 están demostrando cómo las microcredenciales permiten:

- Autenticación sin confianza: Los empleadores verifican credenciales directamente
- Composición modular: Agregación de “badges” digitales en trayectorias formativas personalizadas.

Validez de las Microcredenciales

Un desafío fundamental en la adopción de microcredenciales es su validación dentro y fuera del país de emisión. Tradicionalmente, se requiere un proceso de apostilla para que los documentos sean reconocidos a nivel internacional. Sin embargo, la oportunidad de las credenciales verificables está redefiniendo los paradigmas de acreditación profesional, transformando a los usuarios en custodios soberanos de sus trayectorias formativas dentro de ecosistemas laborales interoperables.

A pesar de sus ventajas, conlleva implicaciones importantes. La posibilidad de que estas credenciales representen la reputación profesional de una persona plantea preguntas críticas sobre su diseño y la confiabilidad de las instituciones que las administran. Es fundamental reflexionar sobre quiénes controlarán estas credenciales y cómo garantizar que su uso fomente oportunidades en lugar de limitarlas [12].

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 actualmente se encuentra en desarrollo, el mismo establecerá los procedimientos para la presentación, formulación, requisitos, aprobación y emisión de microcredenciales.

La propuesta impulsa la creación de proyectos colaborativos entre distintas carreras académicas y universidades, con el fin de diseñar microcredenciales conjuntas. Asimismo, fomenta la cooperación entre instituciones universitarias y actores del sector público-privado (empresas, entidades sociales y administraciones) para garantizar que estas credenciales respondan a las necesidades del mercado laboral y permitan a los estudiantes adquirir habilidades relevantes para su profesionalización.

Adicionalmente, se está construyendo un catálogo de microcredenciales universitarias enfocadas en competencias altamente demandadas por la sociedad. Paralelamente, se diseñarán sistemas que permitan agrupar y combinar microcredenciales en certificaciones de mayor alcance, así como estandarizar su certificación digital. Esto asegurará la autenticidad, seguridad, portabilidad internacional y protección contra fraudes, facilitando su almacenamiento en billeteras digitales y su intercambio ágil con empleadores o instituciones educativas.

Ejemplo aplicado a la Licenciatura en Sistemas: La imagen adjunta ilustra un itinerario formativo mediante el cual los estudiantes pueden obtener una microcredencial en el área de bases de datos. Esta integra actividades académicas y prácticas diseñadas para fortalecer competencias clave, incluyendo: materias completas, unidades de materias, conjunto de materias, cursos, entre otros.

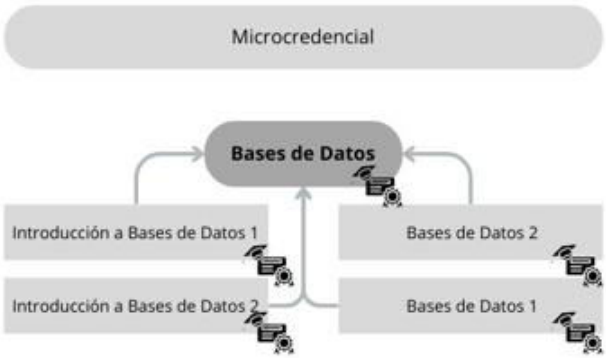


Fig. Trayectos formativos/ Microcredenciales.

4.1.2: Software y Tecnologías Aplicadas

Estándares de la W3C

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].

Esta implementación de estándares para credenciales verificables resuelve:

- Identificadores descentralizados (DIDs): Permiten a los usuarios custodiar sus credenciales en wallets digitales sin depender de entidades emisoras.
- Pruebas de validez criptográficas: Cada microcredencial incorpora firmas digitales verificables en tiempo real mediante contratos inteligentes
- Portabilidad interoperable: Las credenciales se integran en ecosistemas multiplataforma gracias a estándares abiertos como Verifiable Credentials Data Model

Plataforma de Credenciales Digitales

En cuanto a la plataforma para el despliegue del caso de uso de microcredenciales, basándonos en el trabajo anteriormente realizado en el Media Lab, el MIT se ha formado el Consorcio de Credenciales Digitales (Digital Credential Consortium, DCC). Es una red internacional de universidades para desarrollar un sistema compartido de credenciales académicas digitales. Fundado en 2018 por universidades con experiencia en el diseño de credenciales digitales verificables. Entre las universidades miembros fundadores del Consorcio se encuentran Delft University of Technology (Países Bajos), Harvard University (EEUU), Massachusetts Institute of Technology (EEUU), Tecnológico De Monterrey (Méjico), TU Munich (Alemania), UC Berkeley (EEUU), University of Milano-Bicocca (Italia) y University of Toronto (Canadá).

Con la misión de crear una infraestructura confiable, distribuida y compartida que se convierta en el estándar para emitir, almacenar, mostrar y verificar credenciales académicas digitalmente, DCC cuenta con documentos acerca de los proyectos que se desarrollan las universidades del Consorcio, el libro blanco "Building the digital credential infrastructure for the future"[3]. que expone los principios de diseño de la arquitectura del sistema y sirve como base para el desarrollo de implementaciones de referencia, software y prototipos de despliegue por parte de las universidades participantes. Por otro lado, también describe las decisiones tecnológicas que están discutiendo en el Consorcio.

DCC promueve el uso de las credenciales académicas digitales verificables y portátiles en la educación superior a través del desarrollo de tecnología de código abierto. Es por ello que cuenta con un amplio repositorio de código fuente[4] en el que proporciona herramientas para la emisión, gestión y verificación de credenciales académicas digitales basadas en estándares abiertos del W3C, como Verifiable Credentials (VCs) y Decentralized Identifiers (DIDs). La arquitectura modular y enfoque en la interoperabilidad y en la privacidad del usuario lo hacen adecuado para despliegues en entornos educativos promoviendo la portabilidad y autenticidad de credenciales digitales.

El despliegue exitoso requiere integrar componentes críticos como APIs, métodos DID y mecanismos criptográficos. A continuación, se destacan los componentes principales para la implementación del proyecto:

1. **Componentes Principales**
   a) Bibliotecas de Soporte para Credenciales Verificables (VCs)
      - [JSON-LD Processor](https://github.com/digitalcredentials/jsonld-signatures): Biblioteca para el procesamiento de datos en formato JSON-LD, esencial para la estructura de VCs.

[3] https://digitalcredentials.mit.edu/docs/white-paper-building-digital-credential-infrastructure-future.pdf

[4] https://github.com/digitalcredentials

- [Criptografía y Firmas Digitales](https://github.com/digitalcredentials/crypto-ld): Implementación de suites criptográficas (ed25519, secp256k1) para firmas digitales.
- [VC-HTTP-API](https://github.com/digitalcredentials/vc-http-api): API RESTful para operaciones de emisión, almacenamiento y verificación de credenciales.

b) Gestión de Identidades Descentralizadas (DIDs)
- [DID Methods](https://github.com/digitalcredentials/did-method-key): Soporte para métodos DID como "did:key" y "did:web" (ejemplo en `did-method-key`).
- [Registros de Claves](https://github.com/digitalcredentials/universal-registrar): Herramientas para registrar y resolver DIDs en sistemas distribuidos.

c) Almacenamiento y Portabilidad
- [Digital Wallets/Vaults](https://github.com/digitalcredentials/wallet): Repositorio base para billeteras digitales de usuarios.
- [Client Libraries](https://github.com/digitalcredentials):
- JavaScript: [vc-js](https://github.com/digitalcredentials/vc-js) y [jsonld-signatures](https://github.com/digitalcredentials/jsonld-signatures).
- Python: [python-vc](https://github.com/digitalcredentials/python-vc).

d) Interoperabilidad y Estándares
- [Conversores de Formatos](https://github.com/digitalcredentials/openbadges-converter): Herramientas para convertir OpenBadges a VCs.
- [CLI Tools](https://github.com/digitalcredentials/cli): Interfaces de línea de comandos para pruebas y despliegue local.

2. Consideraciones para el Despliegue

Dependencias:
- [Servicios de almacenamiento](https://github.com/digitalcredentials/storage-server) y [APIs auxiliares](https://github.com/digitalcredentials/issuer-registry).

Seguridad:
- Módulos de [revocación de credenciales](https://github.com/digitalcredentials/revocation-list).

3. Repositorios Clave Adicionales
- [Tutoriales y ejemplos] (https://github.com/digitalcredentials/learner-credential-wallet): Implementación de referencia para billeteras educativas.
- [Documentación técnica](https://github.com/digitalcredentials/docs): Guías detalladas para integración y configuración.

Nota:
- Algunos repositorios están en desarrollo activo, por lo que se recomienda verificar las ramas estables (ej: `main` o `latest-release`).
- Para sistemas de identidad basados en blockchain, explorar integraciones externas como [Blockcerts](https://github.com/blockchain-certificates).

5 Conclusiones/Resultados

La transformación digital en entidades públicas mediante la implementación de tecnología Web3 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, tanto normativa como también las capacidades de la tecnología Web 3.

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 Credenciales Verificables 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 DCC, proporcionará 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 tecnología Web 3 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.

El potencial en cuento a 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.

Para la transformación digital en entidades públicas mediante el uso de tecnologías “nuevas” 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 Web3 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. Las credenciales verificables representan una transformación significativa en nuestra interacción con el mundo digital. Su capacidad para garantizar seguridad, portabilidad y transparencia las posiciona como un pilar fundamental en la construcción de identidades digitales confiables y resilientes, especialmente en un entorno donde la protección de la información es crucial.

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-soverereign-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

[16] Use Cases and Requirements for Decentralized Identifiers. Disponible en https://www.w3.org/TR/2021/NOTE-did-use-cases-20210317/ Consultado 12-12-2024