



D2.1

Informe del Estado del Arte de las Credenciales Digitales

Entregable generado cómo parte de la siguiente tarea:

T2.1 Estado del Arte de las Credenciales Digitales

Título del Documento	Estado del Arte de las Credenciales Digitales	
Paquete de Trabajo	WP2	
Fecha de inicio/Fecha de término	02/02/2024 / 24/08/2024	
Socio Responsable	TU Graz	
Entregable (título y número)	D2.1 Reporte de Esstado del Arte de Credenciales Digitales (Versión Español)	
Fecha límite	31/08/2024	
Autores	Chiara Ruß-Baumann, Carina Kern	
Colaboradores	Alexander Nussbaumer, Christian Gütl, Carlos Alario Hoyos, Carlos Delgado Kloos, Héctor R. Amado-Salvatierra	
Socios participantes	TU Graz, UC3M, UG, KINAL	
Versión	1.0	
	Borrador ☐	Final ☒

Tabla de contenido

1. Introducción	5
2. Definiciones	5
○ 2.1. Credenciales	6
○ 2.2. Credenciales Digitales	7
2.2.1. Clasificación de Credenciales Digitales	7
○ 2.3. Certificados Digitales	9
○ 2.4. Credenciales Alternativas	9
○ 2.5. Credenciales Verificables	10
○ 2.6. Macro-Credenciales	11
○ 2.7. Insignias Digitales (Badges)	11
○ 2.8. Micro-Credenciales	13
○ 2.9. Nano-Credenciales	15
○ 2.10. Conclusión	15
● 3. Aspectos Tecnológicos	15
○ 3.1. Ecosistema de Credenciales Digitales	15
3.1.1. Emisión	16
3.1.2. Almacenamiento	16
3.1.3. Intercambio	17
3.1.4. Verificación	18
3.1.5. Revocado	19
○ 3.2. Fundamentos Tecnológicos	19
3.2.1 Firmas Digitales	20
3.2.2. Técnica Zero-Knowledge (ZKPs)	20
3.2.3. Infraestructura de Clave Pública (PKI)	20
3.2.4. Identidades Auto-soberanas (SSIs)	21
3.2.5. Blockchain y Tecnologías de Libro Contable Distribuida (DLTs)	22
○ 3.3. Requerimientos Generales No-Funcionales	23
● 4. Desarrollo Global de Credenciales Digitales	25
○ 4.1. Europa	26
4.1.1. Legislación	26
4.1.2. Iniciativas e infraestructuras ejemplares	27
○ 4.2. Latinoamérica	30
4.2.1. Legislación	30
4.2.2. Iniciativas e Infraestructuras ejemplares	31
○ 4.3. Desarrollos Internacionales	33
4.3.1. Digital Credential Consortium (DCC)	33
4.3.2. Groningen Declaration Network	33
4.3.3. Credential Engine	34
4.3.4. Monitor de Credenciales Digitales	34
4.3.5. Consorcio World Wide Web (W3C) y Credenciales Verificables (VC)	35

4.3.6. 1EdTech, Open Badges and Comprehensive Learner Record (CLR)	36
4.3.7. Estándar Blockcerts	37
○ 4.4. Proveedores	38
4.4.1. Proveedores Públicos	38
4.4.2. Proveedores Privados.....	38
○ 4.5. Ventajas y Posibilidades de las Credenciales Digitales	40
○ 4.6. Retos e Implicaciones	41
● 5. Conclusiones	42
● Referencias	43

1. Introducción

En un entorno de trabajo flexible y mejorado tecnológicamente, la educación y la formación cambian y enfrentan nuevos desafíos en lo que respecta al aprendizaje, los resultados del aprendizaje y el reconocimiento de estos resultados. Varias posibilidades para reconocer los resultados del aprendizaje han ganado popularidad en los últimos años, por ejemplo, las credenciales digitales.

Este informe ofrece una visión general del estado actual de las credenciales digitales. Sirve como un recurso fundamental para comprender y participar en el campo dinámico de las credenciales digitales. Al cubrir diferentes perspectivas de las credenciales digitales, tiene como objetivo proporcionar una visión holística del panorama actual de las credenciales digitales y reconocer la vasta y rápidamente cambiante naturaleza de este campo. Sin embargo, es importante señalar que este informe no pretende ser exhaustivo y no se creó para proporcionar una representación completa.

El informe está subdividido en cuatro partes principales. La sección 2 aclara diferentes términos y significados en el contexto de las credenciales digitales. En la sección 3, se explican el proceso de operación de las credenciales digitales, así como los fundamentos tecnológicos relevantes y los requisitos no funcionales. La sección 4 destaca importantes desarrollos en el campo de las credenciales digitales en todo el mundo, incluidos los proveedores y las infraestructuras relevantes utilizadas para el otorgamiento de credenciales digitales.

Este informe es un entregable (D2.1) que forma parte del Proyecto Erasmus+ ECOCredGT (<http://www.ecocredgt.org/?lang=en>) y sirve como base para una comprensión general de los aspectos relevantes en el ámbito de las credenciales digitales. Está disponible en inglés y español.

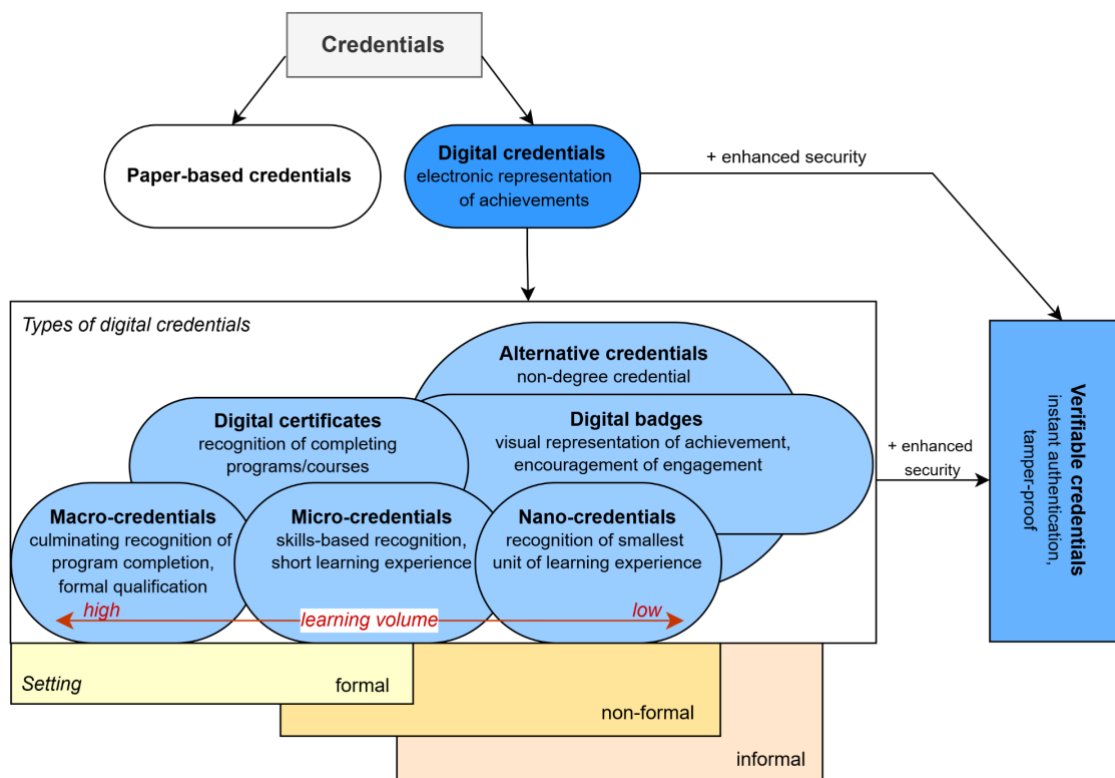
2. Definiciones

Dado que ha habido confusiones con los términos y significados en el contexto de las credenciales, es importante definir "credenciales" y conceptos relacionados. A continuación, se especifican algunas confusiones comunes, comenzando con el término "credencial" en sí, que puede utilizarse para describir un documento de certificación, pero también se usa para describir métodos de transporte de credenciales como billeteras y plataformas. En su informe de 2022, la "Asociación Americana de Registradores y Oficiales de Admisiones Universitarias" (AACRAO) utiliza el término "micro-credencial" de manera intercambiable con "programa de micro-credenciales" para referirse a un cierto diseño o programa en el que los estudiantes deben adquirir competencias. Además, también es común utilizar los términos "insignia" y "credencial digital" o "micro-credencial" de manera intercambiable. Se observa una falta de definiciones específicas de los términos utilizados en la literatura

científica, así como en los proveedores, lo que puede resultar en una falta de comprensión común.

Por lo tanto, esta sección está dedicada a las definiciones de términos relevantes y a menudo utilizados de manera similar en el contexto de las credenciales digitales. Aunque intentamos incluir definiciones y comprensiones comúnmente utilizadas en la investigación y la práctica profesional en esta sección, el uso en tendencia de las credenciales digitales resulta en diferentes comprensiones y significados circulantes, lo que hace imposible aclarar todos en este informe. Por lo tanto, no pretendemos ser completos y abarcativos en las definiciones incluidas. Más bien, el objetivo principal de este capítulo es señalar las diferencias, así como las similitudes entre varios términos y formar una terminología aceptada dentro del proyecto. Por lo tanto, esta sección de definiciones se inicia con una figura (Figura 1) que destaca las superposiciones y peculiaridades entre términos en el contexto de las credenciales digitales. En los siguientes capítulos, cada uno de estos términos mencionados se describen en detalle.

Figura 1: Espectro de credenciales digitales



○ 2.1. Credenciales

Antes de involucrarnos específicamente con las credenciales digitales, donde se centra el proyecto ECOCredGT (ECOCredGT, n.d.), la definición de una credencial en sí debe ser aclarada. El Oxford English Dictionary define las

credenciales como "las cualidades, formación o experiencia que te hacen adecuado para hacer algo" o como "documentos como cartas que prueban que eres quien dices ser, y por lo tanto se puede confiar en ti" (Oxford University Press, 2024). En la educación superior, la definición de credenciales se centra en documentos que certifican el logro de un cierto nivel de conocimiento y están documentados por una tercera parte autorizada (AACRAO, 2023). Las credenciales representan diferentes resultados de aprendizaje adquiridos por un individuo y verifican, validan, confirman o corroboran los logros de aprendizaje, el conocimiento y la preparación para realizar tareas (Keevy & Chakroun, 2015).

En general, las credenciales son electrónicas o en papel, y a menudo se las denomina transcripciones (UNESCO, 2018). Dado que existen muchos tipos diferentes de credenciales, dependiendo del formato, propósito, estado, proveedor, extensión de las actividades de aprendizaje y formación, y el contexto, el término "credencial" se utiliza a menudo como un término general. En los siguientes capítulos se describen diferentes formas de credenciales y términos relacionados, que son relevantes en el contexto de la educación y la formación profesional.

○ 2.2. Credenciales Digitales

Las credenciales digitales se refieren a representaciones electrónicas de logros, habilidades y competencias, y generalmente se almacenan y transmiten en formatos digitales. Las credenciales digitales son equivalentes a documentos en papel, tokens tangibles u otros objetos hápticos emitidos por una entidad de confianza (Brands, 2002). Por lo tanto, el formato electrónico es una característica importante de las credenciales digitales, que permite el almacenamiento, la transmisión y el uso en plataformas. El término "credencial digital" es un término amplio que abarca diferentes tipos de credenciales, como insignias digitales, certificados digitales y microcredenciales. Representan una evolución de las credenciales tradicionales en papel, como certificados, resultados y premios. Las credenciales digitales se utilizan en varios dominios, incluidos la educación y la formación (Quigley, 2023). Especialmente en este contexto, la seguridad es un factor importante en lo que respecta a la fiabilidad y autenticidad. Por lo tanto, el uso de la tecnología blockchain, la criptografía o las firmas digitales se está estableciendo rápidamente en este contexto. Para garantizar la autenticidad, la inviolabilidad, la compatibilidad y la interoperabilidad entre diversos ecosistemas de credenciales, las credenciales también deben ser verificadas. Con las tecnologías emergentes, los formatos y especificaciones estandarizados, la verificación de las credenciales digitales a menudo se da por sentada o se presupone para las credenciales digitales. No obstante, en la aparición original del término, el enfoque estaba en el formato, que no es en papel, sino una representación electrónica de varios logros.

2.2.1. Clasificación de Credenciales Digitales

Como se mencionó anteriormente, el espectro de las credenciales digitales es extremadamente amplio. Por lo tanto, a menudo puede ser necesario categorizarlas. En general, existen varias características que permiten la

descripción y categorización de las credenciales digitales en la educación y la formación.

- **Formalidad:** Las credenciales digitales pueden ser formales, no formales o informales. Cada tipo sirve para diferentes propósitos y se reconoce de diversas maneras dentro de contextos educativos, profesionales y personales. Las credenciales formales son calificaciones oficialmente reconocidas que generalmente otorgan instituciones acreditadas después de un currículo estructurado. A menudo se requieren para la práctica profesional o para ingresar a la educación superior. Las credenciales no formales suelen otorgarse por aprendizajes que ocurren fuera del entorno académico tradicional. Son más flexibles y están orientadas a habilidades o áreas de conocimiento específicas. Las credenciales informales son menos estructuradas y a menudo implican experiencias de aprendizaje que ocurren de manera natural en la vida cotidiana. Por lo general, son autodirigidas y no siguen un currículo formal.
- **Proveedor:** Varias organizaciones y plataformas proporcionan credenciales digitales, cada una con diferentes propósitos y audiencias. Los proveedores pueden ser públicos o privados y ofrecen software propietario o de acceso abierto que se utiliza para emitir, gestionar o verificar credenciales digitales. Algunos de los principales proveedores de credenciales digitales son instituciones educativas, organizaciones profesionales, plataformas de aprendizaje en línea (por ejemplo, Udacity, edX, Coursera), organismos de certificación (por ejemplo, Microsoft, CompTIA) o redes profesionales (por ejemplo, LinkedIn, Credly).
- **Volumen de aprendizaje:** Algunos términos específicos en el contexto de las credenciales digitales se centran en el volumen de aprendizaje de una credencial (por ejemplo, microcredenciales con un pequeño volumen de aprendizaje). Para cada credencial, el volumen de aprendizaje se puede describir en calidad y cantidad, que van desde muy pequeño hasta muy grande. Para asegurar la comparabilidad, el volumen de aprendizaje debe describirse dentro de un marco de calidad o calificación (por ejemplo, Marco Europeo de Cualificaciones para el Aprendizaje Permanente - EQF; CEDEFOP, 2024) u otro sistema estandarizado, como un sistema de puntos de crédito (por ejemplo, Sistema Europeo de Transferencia y Acumulación de Créditos - ECTS; European Commission, n.d.-a).
- **Verificabilidad/autorización:** Las credenciales digitales pueden ser autorizadas y verificadas para garantizar la autenticidad, validez y confiabilidad de las credenciales emitidas y recibidas. Estos procesos involucran varias tecnologías, incluidas firmas digitales, blockchain y plataformas de verificación seguras que se pueden describir.
- **Propósito:** Dentro de estas diferentes categorías, a menudo hay un propósito específico para recibir una credencial digital, que puede ser la

obtención de una calificación, una habilidad específica o podría servir como un factor motivador.

○ **2.3. Certificados Digitales**

Como se mencionó anteriormente, un certificado digital es un tipo específico de credencial digital que certifica la competencia de un individuo en una habilidad o campo específico y tiene el propósito de reconocer y validar logros en el contexto de un aprendizaje estructurado, como la finalización de cursos formales, programas de formación o certificaciones profesionales. Los certificados digitales se utilizan comúnmente para validar habilidades y competencias profesionales, y a menudo se requieren para ciertos roles laborales o avances profesionales. Son comunes en instituciones académicas, formación corporativa y programas de certificación (Sertifier, 2023). Un certificado digital incluye algún tipo de prueba que confirma que una entidad es lo que dice ser, como una firma electrónica de una o más partes de confianza que garantiza la autenticidad y validez (Agencia de la Unión Europea para la Ciberseguridad, n.d.).

El propósito principal de los certificados digitales, en el contexto de reconocer logros, es reconocer la finalización de un curso formal, programa de formación o certificación profesional. Por el contrario, otras formas de credenciales digitales, como las insignias digitales, son más versátiles y pueden representar una gama más amplia de logros, ya que se utilizan para reconocer logros también de experiencias de aprendizaje informales, talleres, conferencias, voluntariado y otras demostraciones de habilidades.

Los certificados digitales y las credenciales digitales tienen mucho en común. No obstante, mientras que un certificado es un tipo específico de credencial, enfocado en reconocer la finalización de un programa o logro formal, una credencial es un término más abarcador que incluye varias formas de validación (por ejemplo, logros informales) y todos los términos descritos a continuación.

○ **2.4. Credenciales Alternativas**

El término "alternativo" dentro del contexto de las credenciales digitales significa una alternativa a las credenciales tradicionalmente utilizadas en la educación superior (títulos de licenciatura, maestría y doctorado) (AACRAO, 2022). En consonancia con esto, Kato y sus colegas (2020) definen "credenciales alternativas" como "credenciales que no son reconocidas como calificaciones educativas formales independientes por las autoridades educativas nacionales relevantes". Además, no es necesario un nivel específico de educación para que se otorguen las credenciales alternativas. Según su comprensión, los certificados, las insignias digitales y las microcredenciales son tres formas de credenciales alternativas que son conceptualmente distintas.

Asimismo, la AACRAO (2022) define las credenciales alternativas como "credenciales no tradicionales (sin títulos)". Cuando son ofrecidas por instituciones de educación superior, pueden incluir diversas otras alternativas de

crédito, incluidos Cursos Masivos Abiertos en Línea (MOOCs), microcredenciales, insignias y programas de certificación. Además, se afirma que se emiten típicamente en formato digital. Si bien la AACRAO se centra en las credenciales que son ofrecidas por instituciones de educación superior, las credenciales alternativas también han despertado interés fuera de las instituciones académicas tradicionales, por ejemplo, en la formación profesional para apoyar la empleabilidad. Por lo tanto, las credenciales alternativas destacan la naturaleza diversa de las actividades de aprendizaje con un enfoque en la adquisición de habilidades y competencias para apoyar el aprendizaje a lo largo de la vida y el perfeccionamiento de habilidades.

○ 2.5. Credenciales Verificables

Las Credenciales Verificables son credenciales digitales que pueden verificarse criptográficamente para asegurar su autenticidad e integridad. El término "verificable" dentro del contexto de las credenciales verificables denota la característica de las credenciales de ser confirmadas por un verificador y la posibilidad de verificarlas y autenticarlas de manera independiente para confirmar su legitimidad. Diseñadas para ser seguras, a prueba de manipulaciones y fácilmente compartibles, las credenciales verificables permiten a las personas presentar credenciales como identidad, calificaciones u otros detalles personales a organizaciones que necesiten verificarlas (como empleadores, instituciones educativas o agencias gubernamentales). A diferencia de los documentos físicos, las credenciales verificables optimizan el proceso de verificación y mejoran la seguridad al eliminar la necesidad de manejo físico, reducir el riesgo de falsificación y garantizar que las credenciales puedan ser confiadas y autenticadas digitalmente. Este proceso generalmente involucra técnicas criptográficas (Shoemaker, 2022; World Wide Web Consortium, 2022b). Esto a menudo se facilita mediante tecnologías como blockchain o registros descentralizados, que proporcionan un registro transparente e inmutable de la emisión y validez de la credencial (World Wide Web Consortium, 2022b). Las credenciales verificables pueden representar información idéntica a una credencial física. Sin embargo, la integración de tecnologías puede mejorar la naturaleza a prueba de manipulaciones y la confiabilidad en comparación con sus equivalentes físicos (World Wide Web Consortium, 2024b). Sin embargo, el hecho de que las credenciales sean verificadas no significa automáticamente que la exactitud de las afirmaciones codificadas pueda ser evaluada y validada.

Las credenciales verificables también pueden ser credenciales digitales. La distinción principal entre las credenciales digitales en su significado original y las credenciales verificables radica en la capacidad de autenticación instantánea. Las credenciales verificables, a diferencia de sus predecesoras, son versiones protegidas criptográficamente tanto de credenciales físicas como en línea (Dock Labs AG, 2023). En resumen, aunque las credenciales verificables también pueden ser electrónicas (credenciales digitales), las credenciales verificables ofrecen mayor seguridad, privacidad y facilidad de verificación independiente

mediante métodos criptográficos. Cuando se cumplen estas características, el uso del término "credencial verificable" podría ser más específico y preciso.

○ **2.6. Macro-Credenciales**

Las Macrocredenciales son calificaciones formales que denotan la finalización de programas educativos integrales, generalmente culminando en títulos académicos como títulos, diplomas, certificados y licencias. Estas credenciales cubren una amplia gama de conocimientos y habilidades adquiridas durante un período prolongado, a menudo varios años, y generalmente son otorgadas por instituciones educativas acreditadas, reconocidas o reguladas, u otras organizaciones. Las macrocredenciales significan la adquisición de un cuerpo de conocimientos completo, habilidades transferibles o competencia técnica, lo que a menudo requiere varios años para completarse. Mientras que algunas personas persiguen estas credenciales por crecimiento personal o educativo general, otras las buscan para calificar para una profesión o carrera específica (UNESCO, 2022).

La Comisión Europea (2020a) explica que las macrocredenciales se otorgan después de la finalización exitosa de programas académicos extensos. Estas credenciales abarcan múltiples materias o áreas de especialización, asegurando que el titular haya alcanzado un nivel significativo de dominio y competencia. Las macrocredenciales son esenciales para la educación superior y son con frecuencia prerrequisitos para ingresar a campos profesionales o seguir estudios avanzados adicionales.

En contraste con las microcredenciales, que se centran en habilidades específicas o resultados de aprendizaje a corto plazo, las macrocredenciales proporcionan una representación holística de los logros educativos de una persona. Involucran una evaluación rigurosa y validación por parte de instituciones acreditadas, ofreciendo así una evidencia sustancial de las calificaciones de una persona. En resumen, las macrocredenciales son calificaciones vitales que representan un aprendizaje extenso y la adquisición de habilidades, validadas a través de premios formales como títulos y diplomas. Juegan un papel crucial en el avance académico, así como en el desarrollo profesional.

○ **2.7. Insignias Digitales (Badges)**

Según AACRAO (2022), las "insignias" o "insignias digitales" se refieren al artefacto emitido y a la demostración visual de una habilidad lograda. Son "representaciones en línea que reconocen habilidades, logros, afiliación a membresías y participación". Las insignias se otorgan generalmente por completar una tarea o curso específico, pueden mostrarse en plataformas digitales, como sitios web, perfiles en redes sociales o portafolios en línea (1EdTech, 2024a), y también sirven para mostrar las habilidades y logros alcanzados a empleadores, colegas y otras partes interesadas (Khalil & Ebner, 2015).

Kato y sus colegas (2020) se refieren a una definición de SURFnet (2016) y afirman que las insignias digitales son "pictogramas o logotipos digitales que se pueden compartir en la web para mostrar el logro de ciertas habilidades y conocimientos". Estas habilidades pueden variar ampliamente en forma cuantitativa y cualitativa y no necesitan estar relacionadas con un programa de estudios académico ni con otros estándares (por ejemplo, estándares de la industria o profesionales). Por lo tanto, a menudo se utilizan para reconocer experiencias de aprendizaje informal, pero también logros formales.

La UNESCO (2018) se refiere a una definición de Lemoine y Richardson (2015) y define las insignias digitales como gráficos clicables que contienen el registro de un logro, el trabajo y la evidencia de este trabajo que se requiere para dicho logro, y la información sobre la entidad emisora. Ven las insignias como ejemplos de microcredenciales.

En el pasado, las insignias digitales ya se habían utilizado para promover la comunidad de juegos en línea a mediados de la década de 2000, por ejemplo, mediante el Gamerscore de Xbox 360 de Microsoft. En el contexto de la educación, las insignias digitales despertaron poco interés antes de la década de 2010 (Gibson et al., 2015). McDaniel y Fanfarelli (2016) publicaron un artículo que describe que puede haber bastantes objetivos comparables para recibir una insignia en los videojuegos y en la educación. En ambos contextos, las insignias digitales pueden ser efectivas para fomentar la participación y la obtención de más insignias. También en la educación superior y la formación profesional, las insignias digitales a menudo toman prestados aspectos de la gamificación y pueden otorgarse como recompensa por el esfuerzo, sin estar vinculadas a un resultado específico de las actividades de aprendizaje (Flintberg, 2022).

Si bien a veces el término "insignias digitales" se usa indistintamente con microcredenciales (Brown et al., 2021), una diferencia importante es el enfoque en la representación visual de las competencias y los resultados de aprendizaje adquiridos en las insignias digitales. Están destinadas a ser exhibidas y compartidas en línea y, por lo tanto, también pueden contener metadatos que proporcionen más información sobre la credencial real detrás de la insignia digital (Foshay & Hale, 2017; Gibson et al., 2015). No obstante, con su enfoque en la presentación visual, las insignias digitales también pueden utilizarse como un factor de motivación para promover la participación en actividades de aprendizaje más pequeñas y proporcionar una solución tecnológica para representar los resultados de aprendizaje independientemente de las calificaciones (UNESCO, 2018). De manera similar, Mah (2016) sugiere que las insignias digitales tienen cinco roles principales en el entorno educativo: motivación, reconocimiento del aprendizaje, señalización de logros, captura de trayectorias de aprendizaje y, en el sector de la educación superior, el potencial para contribuir a la retención de estudiantes.

Las insignias digitales pueden recopilarse a través de plataformas, como redes sociales, pero también en plataformas más formales de instituciones establecidas, como 1EdTech con su programa Open Badge (UNESCO, 2018). La especificación Open Badges, con su formato para insignias digitales, existe

desde 2012 y ha emitido más de 40 millones de insignias en todo el mundo. Una Open Badge consiste en la imagen y los datos sobre la credencial digital, que son legibles por máquina (1EdTech, 2024a).

○ 2.8. Micro-Credenciales

AACRAO (2022) describe una microcredencial como un reconocimiento basado en competencias o habilidades que permite a un aprendiz demostrar experiencia y aprendizaje en un área específica. Por lo general, una microcredencial representa un conjunto más pequeño de logros o resultados de aprendizaje, que no equivale a un título completo.

Las microcredenciales son indicadores a pequeña escala, pueden basarse en el desempeño o en la finalización y pueden ser proporcionadas por una variedad de entidades, incluidas empresas comerciales, proveedores privados, cuerpos profesionales, instituciones de educación y formación tradicionales, organizaciones comunitarias y diversas otras organizaciones (World Wide Web Consortium, 2022b). Las microcredenciales que se proporcionan internamente en una empresa también pueden ser menos formales y estar más orientadas hacia las habilidades adquiridas, competencias (es decir, basadas en el desempeño) y el impacto empresarial (Foshay & Hale, 2017). Aunque muchas microcredenciales reflejan los resultados de experiencias de aprendizaje convencionales, otras validan logros obtenidos a través de diferentes medios, como en el lugar de trabajo, el voluntariado o el aprendizaje por interés personal. A menudo se consideran un método efectivo para mejorar las habilidades de los trabajadores a lo largo de sus carreras (World Wide Web Consortium, 2022b).

El "Grupo de Consulta de Educación Superior sobre Microcredenciales" de la Comisión Europea ha definido una microcredencial de la siguiente manera: "Una microcredencial es una prueba de los resultados de aprendizaje que un aprendiz ha adquirido después de una experiencia de aprendizaje corta. Estos resultados de aprendizaje han sido evaluados en función de estándares transparentes" (European Commission, 2020a). Esta definición establece claramente que una microcredencial es una certificación documentada otorgada por una organización de confianza, que indica que un aprendiz ha cumplido con resultados de aprendizaje específicos a través de una evaluación, de acuerdo con estándares establecidos y principios de aseguramiento de la calidad. Implícitamente, esta definición sugiere que las microcredenciales deberían idealmente referenciarse o integrarse dentro de marcos de calificación (European Commission, 2020a).

De manera similar, el Consejo de la Unión Europea (2022) define las microcredenciales como un "registro de los resultados de aprendizaje que un aprendiz ha adquirido tras un pequeño volumen de aprendizaje". Estas experiencias de aprendizaje formales, no formales o informales que resultan en resultados de aprendizaje son evaluadas por el proveedor u otros proveedores de evaluación reconocidos con criterios claramente definidos y transparentes para asegurar la calidad, siguiendo ciertos estándares acordados en un sector o área de actividad específica.

En el contexto de las credenciales digitales, existe una gran cantidad de literatura, iniciativas y proyectos relacionados con las microcredenciales. Sin embargo, existe una comprensión muy variada del espectro de las microcredenciales, como lo ejemplifican Brown y sus colegas (2021) en su marco de ecología de credenciales. Kato y sus colegas (2020) mencionan este amplio espectro para el tamaño de las microcredenciales y el entorno de aprendizaje conectado en diferentes países de la OCDE. En los Estados Unidos, una microcredencial es una actividad de aprendizaje que es menos que un título completo, pero más que un solo curso. Además, la extensión también depende del proveedor de la definición (Pickard, 2018). La Autoridad de Cualificaciones de Nueva Zelanda (2019) define que las microcredenciales pueden variar de 5 a 40 créditos, y también los países europeos varían en su comprensión del rango de una microcredencial. En Austria, una microcredencial varía de 3 a 15 ECTS (Bundesministerium für Bildung, Wissenschaft und Forschung, s.f.) y en España una microcredencial se define como menos de 15 ECTS (Agencia Nacional de Evaluación de la Calidad y Acreditación, 2022). En Dinamarca, una microcredencial es una pequeña unidad de aprendizaje con 1-2 ECTS (Danmarks Akkrediteringsinstitution, 2021), mientras que Irlanda define las credenciales con un máximo de 30 ECTS como microcredenciales (Quality and Qualifications Ireland, 2021). Esto resalta la gran variedad de comprensiones sobre las microcredenciales.

El Consejo de la Unión Europea (2022) promueve elementos estándar europeos para describir una microcredencial. Estos elementos incluyen: a) la identificación del aprendiz, b) el título de la microcredencial, c) el país o región del emisor, d) la entidad otorgante, e) la fecha de emisión, f) los resultados de aprendizaje, g) la carga de trabajo necesaria para lograr los resultados de aprendizaje, h) el nivel de la experiencia de aprendizaje, i) el tipo de evaluación, j) la forma de participación en la actividad de aprendizaje, y k) el tipo de aseguramiento de la calidad utilizado para respaldar la microcredencial. Estos elementos se describen como obligatorios y se complementan con elementos opcionales que deben incluirse cuando sea relevante: a) los requisitos previos necesarios para inscribirse en la actividad de aprendizaje, b) supervisión y verificación de identidad durante la evaluación, c) calificación obtenida, d) opciones de integración y acumulabilidad, y e) más información.

Además de estos elementos estándar, los principios europeos para diseñar y emitir microcredenciales incluyen calidad, transparencia, relevancia, evaluación válida, apoyo a las trayectorias de aprendizaje, reconocimiento, portabilidad, enfoque en el aprendiz, autenticidad e incorporación de servicios de orientación para el aprendizaje a lo largo de la vida (Consejo de la Unión Europea, 2022).

Las microcredenciales son propiedad del aprendiz, quien puede almacenarlas y compartirlas con una parte de su elección (portabilidad) y combinarlas en credenciales más grandes (acumulabilidad), lo que no necesariamente otorga al aprendiz una calificación o un título, pero puede motivar a los aprendices y apoyar trayectorias de aprendizaje más flexibles (UNESCO, 2022). Según Wolz y sus colegas (2021), aunque las microcredenciales pueden considerarse "mini-

certificaciones", el enfoque se centra más en el contenido y menos en la sustitución de certificados tradicionales.

○ 2.9. Nano-Credenciales

Una nano-credencial representa un conjunto muy pequeño y específico de habilidades o conocimientos adquiridos a través de una breve experiencia de aprendizaje. Estas credenciales están diseñadas para ser altamente enfocadas y, a menudo, pueden completarse en cuestión de horas o días, a diferencia de las semanas o meses que suelen requerirse para otras formas de credenciales, como las microcredenciales. En general, las insignias y las nano-credenciales representan la unidad más pequeña de reconocimiento de una actividad de aprendizaje, que puede ser solo una experiencia de aprendizaje individual o una habilidad específica (West, 2023). Las nano-credenciales se utilizan a menudo para demostrar rápidamente competencia en un área o competencia particular, lo que las hace valiosas tanto para los aprendices como para los empleadores que buscan abordar brechas de habilidades inmediatas. Por lo tanto, una nano-credencial es más pequeña que una microcredencial, con la capacidad de acumularse en microcredenciales (Pahuja, 2023).

○ 2.10. Conclusión

Como se destacó anteriormente, la terminología de las credenciales (digitales) es compleja, ya que se ha convertido en un tema de tendencia en la investigación y la práctica, lo que resulta en diferentes usos y definiciones, dependiendo del contexto y el propósito de cada credencial. También es muy importante mencionar que la mayoría de los términos tienen muchos significados superpuestos, como se muestra en la Figura 1.

● 3. Aspectos Tecnológicos

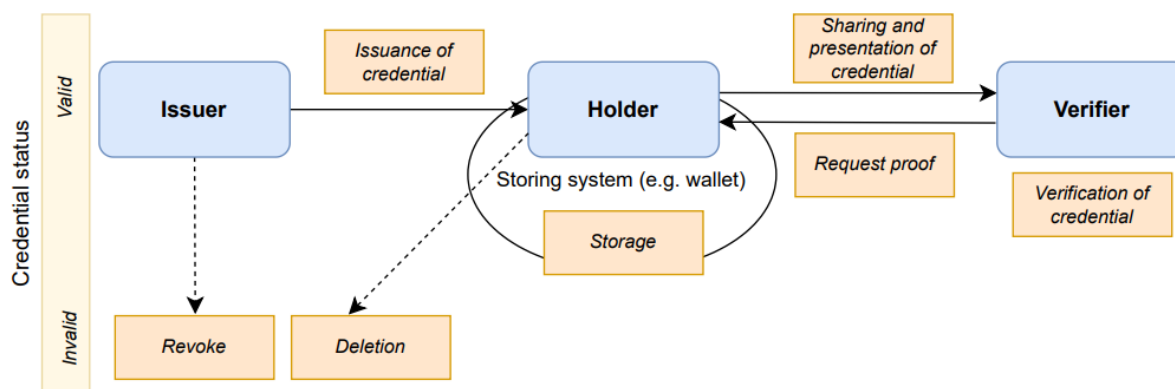
○ 3.1. Ecosistema de Credenciales Digitales

Esta sección describe los roles de los actores principales (es decir, titular, emisor, verificador) y los procesos operativos generales (es decir, emisión, almacenamiento, intercambio, verificación, revocación) dentro de un ecosistema de credenciales digitales.

Existen diferentes actores que tienen roles específicos dentro de un ecosistema de credenciales digitales. El titular es la entidad que posee una o más credenciales verificables (por ejemplo, una persona) y genera presentaciones a partir de ellas. El emisor es la entidad que crea la credencial verificable (por ejemplo, una institución de formación profesional) al hacer afirmaciones sobre el sujeto y emitir las credenciales al titular. El verificador es la entidad que solicita información sobre una credencial y recibe y verifica la presentación verificable (por ejemplo, un empleador) para tomar decisiones de confianza basadas en la información que contiene (World Wide Web Consortium, 2024b).

En las siguientes secciones, se explica el proceso operativo general dentro de un sistema de credenciales digitales, incluido el papel de los actores descritos anteriormente y los flujos de información respectivos dentro de este proceso. En la siguiente Figura (Figura 2), se representan los roles (azul), los procesos operativos (naranja) y los flujos de información (ilustrados con flechas) dentro de un ecosistema de credenciales digitales.

Figura 2: Roles, procesos de operación y flujo de información dentro de un ecosistema de credenciales digitales



3.1.1. Emisión

Emitir credenciales digitales es un proceso que implica la creación y distribución de representaciones electrónicas de calificaciones, habilidades o logros. Las credenciales digitales generalmente son emitidas por instituciones acreditadas, como universidades, organismos de certificación o agencias gubernamentales. El proceso de emisión comienza con la evaluación o verificación de los logros o calificaciones del individuo. Esto puede implicar una combinación de revisiones de documentos, exámenes o evaluaciones prácticas. Una vez confirmado, el organismo emisor crea una credencial digital, que se firma y se emite al destinatario (Chardrand et al., 2018).

3.1.2. Almacenamiento

Después de que se emite una credencial digital, el titular debe almacenarla, lo que incluye la preservación y gestión segura de las credenciales, y es fundamental para garantizar la longevidad, accesibilidad y seguridad. Una posibilidad comúnmente utilizada para almacenar credenciales digitales son las billeteras digitales, que son aplicaciones que permiten a las personas administrar sus credenciales y compartirlas según sea necesario. Estas billeteras utilizan técnicas criptográficas avanzadas para proteger las credenciales de accesos no autorizados y manipulaciones. Las soluciones de almacenamiento de credenciales digitales deben abordar varias consideraciones clave, incluida la seguridad, la privacidad, la interoperabilidad y el control del usuario (Sedlmeir et al., 2021).

La seguridad es una preocupación primordial en el almacenamiento de credenciales digitales. Se emplean métodos criptográficos, como se describe en

el capítulo 3.2, para garantizar que las credenciales permanezcan seguras y a prueba de manipulaciones. Cada credencial se firma utilizando la clave privada del emisor, y esta firma se puede verificar utilizando la clave pública del emisor, asegurando la autenticidad e integridad de la credencial (Gréther et al., 2018). Además, las billeteras digitales a menudo implementan autenticación multifactor (MFA) y cifrado para proteger aún más las credenciales almacenadas de accesos no autorizados (González et al., 2018).

Además, proteger la privacidad de las credenciales de los individuos es crucial. Los sistemas de almacenamiento, como las billeteras digitales, deben garantizar que las credenciales solo sean accesibles para las partes autorizadas y que no se exponga información sensible. Técnicas como las pruebas de conocimiento cero permiten a los individuos compartir solo la información necesaria sin revelar todos los detalles de sus credenciales. Este enfoque mejora la privacidad al minimizar la exposición de datos personales (World Wide Web Consortium, 2024b).

Para que las credenciales digitales sean ampliamente utilizables, deben almacenarse de manera que se garantice la interoperabilidad entre diferentes plataformas y sistemas. Modelos de datos como el estándar Open Badges y el estándar de Credenciales Verificables facilitan esta interoperabilidad al proporcionar un marco común para representar e intercambiar credenciales (Casilli & Hickey, 2016; World Wide Web Consortium, 2022b). Estos estándares permiten que las billeteras digitales almacenen credenciales en un formato que pueda compartirse y verificarse fácilmente por varias entidades, independientemente de la tecnología subyacente.

El control del usuario sobre las credenciales digitales es otro aspecto importante de su almacenamiento. Los individuos deben tener la capacidad de gestionar sus credenciales, decidir quién puede acceder a ellas y controlar qué información se comparte. Las billeteras digitales empoderan a los usuarios al proporcionar una interfaz fácil de usar para gestionar credenciales y establecer permisos para el acceso y el intercambio. Los marcos de identidad autosoberana (SSI), descritos en el capítulo 3.2, mejoran aún más el control del usuario al permitir que los individuos posean y gestionen sus identidades digitales de forma independiente de cualquier autoridad central (Allen, 2016).

3.1.3. Intercambio

Antes de que la respectiva credencial pueda ser verificada por un verificador, el titular de una credencial debe poder elegir si una credencial debe enviarse y presentarse a un verificador. Si el titular decide compartir una credencial o cierta información, debe ser posible restringir la cantidad de información expuesta y la duración durante la cual se comparte la información (World Wide Web Consortium, 2022b). Para compartir sus credenciales digitales, los individuos pueden proporcionar un enlace directo o un código QR que lleva a su billetera digital o repositorio, donde se puede visualizar la credencial. El uso de la tecnología blockchain en los sistemas de credenciales digitales garantiza que estos enlaces sean seguros y que las credenciales sean a prueba de

manipulaciones (Grech & Camilleri, 2017). Aspectos como las estandarizaciones y la interoperabilidad también son esenciales en este paso operativo, ya que las credenciales digitales deben compartirse de manera efectiva en varias plataformas e instituciones. Por lo tanto, formatos estandarizados para credenciales digitales, como la especificación Open Badges (1EdTech, 2024a), se han convertido en estándares en el contexto de los sistemas de credenciales digitales. Esta estandarización permite que las credenciales se compartan y reconozcan en diferentes sistemas y plataformas, facilitando un proceso de intercambio sin problemas.

Al igual que en el proceso de almacenamiento, el intercambio de credenciales digitales también plantea importantes preocupaciones de privacidad y seguridad, ya que se maneja información personal sensible. Por lo tanto, también se debe respetar la legislación respectiva en el contexto de la privacidad. Por ejemplo, en Europa, el Reglamento General de Protección de Datos (GDPR) exige que los datos personales sean procesados con el consentimiento del individuo y protegidos contra el acceso no autorizado (EUR-Lex, 2016). Por lo tanto, las plataformas de credenciales digitales deben incorporar medidas de seguridad sólidas, como la encriptación y protocolos de autenticación segura, para proteger los datos de los usuarios durante el proceso de intercambio.

3.1.4. Verificación

La verificación de una credencial ocurre cuando un tercero, como un empleador o una institución educativa, necesita validar la credencial. El verificador puede acceder a los metadatos de la credencial a través de una billetera digital o una plataforma en línea segura. Las tecnologías avanzadas como blockchain (descritas en el capítulo 3.2.5) garantizan que la información de la credencial sea inmutable y a prueba de manipulaciones, lo que proporciona un alto nivel de confianza en el proceso de verificación (Grech & Camilleri, 2017). El enfoque descentralizado elimina la necesidad de intermediarios y reduce el riesgo de fraude (Chen et al., 2018). Además, todas las transacciones de credenciales se registran públicamente y cualquier intento de alterar una credencial sería fácilmente detectable. Esta transparencia del blockchain también mejora la confianza entre las partes interesadas y es esencial para mantener la integridad del proceso de verificación (Grech & Camilleri, 2017).

Para que el proceso de verificación sea efectivo, las credenciales digitales deben adherirse a formatos estandarizados (por ejemplo, Open Badges) que garanticen la interoperabilidad entre diferentes plataformas e instituciones. Esta estandarización facilita el intercambio y la verificación sin problemas de las credenciales en varios sistemas, mejorando su utilidad y aceptación. El proceso de verificación también debe abordar las preocupaciones de privacidad y seguridad. Las credenciales digitales a menudo contienen información personal sensible, lo que requiere medidas de protección de datos sólidas. En Europa, según el Reglamento General de Protección de Datos (GDPR), los datos personales deben ser procesados de manera segura y con el consentimiento del individuo (EUR-Lex, 2016). Las plataformas de credenciales digitales deben

implementar encriptación, protocolos de autenticación segura y principios de privacidad desde el diseño para proteger los datos de los usuarios durante el proceso de verificación (Digital Credentials Consortium, 2018).

3.1.5. Revocado

El proceso de revocación generalmente comienza cuando una autoridad emisora, como una institución educativa o un organismo de certificación, determina que una credencial digital debe invalidarse. Esto puede deberse a la expiración de la credencial, al descubrimiento de una actividad fraudulenta o a que el titular de la credencial ya no cumple con los estándares requeridos (Grech & Camilleri, 2017). El proceso de revocación implica marcar la credencial como revocada en el sistema de credenciales. En la tecnología blockchain, para revocar una credencial, la autoridad emisora añade una nueva transacción a la cadena de bloques que actualiza el estado de la credencial a "revocada" (Chen et al., 2018). Esto garantiza que cualquier persona que intente verificar la credencial vea su estado revocado, evitando su uso indebido.

○ 3.2. Fundamentos Tecnológicos

La evolución de las credenciales digitales ha necesitado el desarrollo y la adopción de estándares tecnológicos para garantizar la interoperabilidad, la seguridad, la confianza y la aceptación generalizada. Estas tecnologías son cruciales para crear un ecosistema confiable y cohesivo que respalde la emisión, verificación, almacenamiento y compartición de credenciales digitales en varios sectores y regiones (Mühle et al., 2023).

En esta sección, se describen los fundamentos tecnológicos relevantes que se basan en técnicas criptográficas. Las técnicas criptográficas son métodos utilizados para asegurar la información y las comunicaciones mediante el uso de códigos, garantizando que solo aquellos a quienes está destinada la información puedan leerla y procesarla. Son esenciales para proteger los datos en las comunicaciones digitales, proteger la privacidad, garantizar la integridad y autenticidad de los mensajes, y asegurar las transacciones en varios campos. Dos técnicas criptográficas relevantes son la encriptación simétrica y asimétrica. La encriptación simétrica implica el uso de la misma clave tanto para encriptar como para desencriptar, mientras que la encriptación asimétrica utiliza un par de claves, una para encriptar (clave pública) y otra para desencriptar (clave privada) (Reynolds & Winks, 2021).

Las técnicas mencionadas en los siguientes capítulos no son independientes y autónomas, sino que se combinan y dependen entre sí en un sistema de credenciales digitales de diversas maneras. Esta interacción de los fundamentos tecnológicos se destaca al final de este capítulo en una Figura (Figura 3), que muestra un ejemplo de un sistema basado en blockchain que puede utilizarse para operar y gestionar credenciales digitales.

3.2.1 Firmas Digitales

Las firmas digitales son técnicas criptográficas que son similares a las firmas manuscritas, pero mucho más seguras. Las firmas digitales son una aplicación clave de una Infraestructura de Clave Pública (PKI, descrita en el capítulo 3.2.3), que permite a los usuarios firmar datos con su clave privada (Menezes et al., 1996). Para firmar una credencial digital, el emisor genera un hash del contenido de la credencial. Este hash es una representación única de la credencial. Luego, el emisor cifra el hash con su clave privada para crear la firma digital. Este proceso vincula la firma a la credencial, asegurando que cualquier alteración del contenido de la credencial sea detectable. Cuando un verificador recibe una credencial digital, utiliza la clave pública del emisor para descifrar la firma digital y recuperar el hash original. El verificador también genera de manera independiente un hash del contenido de la credencial recibida. Si los dos hashes coinciden, se confirma que la credencial no ha sido alterada y que fue firmada por el emisor, validando así su autenticidad (Katz & Lindell, 2007).

3.2.2. Técnica Zero-Knowledge (ZKPs)

Las técnicas de conocimiento cero (Zero-Knowledge) (ZKPs) son técnicas criptográficas que permiten a una parte demostrar a otra que una declaración es verdadera sin revelar información adicional. En el contexto de credenciales verificables, los ZKPs se pueden utilizar para probar la posesión de ciertos atributos o calificaciones sin divulgar los datos reales, mejorando así la privacidad (Goldreich et al., 1986).

3.2.3. Infraestructura de Clave Pública (PKI)

La Infraestructura de Clave Pública (PKI) es un marco para la gestión de claves digitales y proporciona encriptación mediante el uso de criptografía asimétrica con la aplicación de criptografía de clave pública. A cada entidad involucrada en el ecosistema de credenciales se le emite un par de claves públicas y privadas por una autoridad certificadora de confianza (CA). La CA maneja todos los aspectos de la gestión de credenciales y confirma que el sujeto impreso en el certificado es el propietario de la clave pública. La clave pública está destinada a la distribución pública y puede compartirse abiertamente, mientras que la clave privada se mantiene segura por el propietario. La clave pública se utiliza para cifrar datos de manera que solo el propietario pueda descifrar los datos con la clave privada. A la inversa, solo el propietario del par de claves puede cifrar datos utilizando la clave privada. Esto garantiza la autenticidad del remitente para todos los destinatarios, ya que solo la clave pública asociada descifrá los datos (Agencia de Ciberseguridad de la Unión Europea, s.f.).

Debido a la vinculación de claves públicas a entidades dentro de un sistema PKI tradicional, los identificadores centralizados juegan un papel crucial, ya que la PKI depende tradicionalmente de ellos. No obstante, hay un creciente interés y desarrollo en integrar los principios de PKI con identificadores descentralizados. Esta integración tiene como objetivo combinar la seguridad robusta y los marcos de confianza de PKI con la naturaleza descentralizada centrada en el usuario de los DIDs. La integración de los DIDs en los marcos de PKI representa un avance

significativo, abordando algunas de las limitaciones inherentes de los sistemas PKI tradicionales (Bakhtina et al., 2023; Shi et al., 2022).

Identificadores Centralizados

Los identificadores centralizados son identificadores únicos, emitidos y gestionados por una autoridad u organización centralizada, y se utilizan ampliamente en muchos sectores, incluida la educación. Los identificadores centralizados son emitidos típicamente por una autoridad central, como un gobierno, una institución educativa o una corporación. El papel de la autoridad central es garantizar la unicidad y validez de estos identificadores. Estos identificadores están diseñados para ser únicos y persistentes, lo que significa que cada identificador se asigna a una sola entidad y permanece constante en el tiempo. Ejemplos incluyen números de licencia de conducir, identificaciones de estudiantes y números de empleados. Esta unicidad y persistencia son fundamentales para mantener registros precisos y garantizar que los identificadores se vinculen de manera confiable a la misma entidad a lo largo del tiempo. El proceso de verificación de los identificadores centralizados implica consultar una base de datos central mantenida por la autoridad emisora. Por ejemplo, la verificación de un título universitario podría requerir la comprobación de los registros de la institución. Aunque los identificadores centralizados ofrecen medios estructurados y autorizados de identificación, también presentan varios desafíos. La dependencia de bases de datos centralizadas puede plantear riesgos de privacidad, ya que estos repositorios pueden ser vulnerables a brechas y mal uso. Los sistemas centralizados pueden convertirse en puntos únicos de falla, donde el compromiso de la autoridad central puede provocar problemas generalizados. Además, los usuarios y las partes interesadas deben confiar en la autoridad emisora, lo que puede no ser siempre factible en contextos transfronterizos o interorganizacionales (Sedlmeir et al., 2021).

3.2.4. Identidades Auto-soberanas (SSIs)

Las Identidades Autosoberanas (SSIs) son un modelo de identidad digital que otorga a los individuos el control sobre sus propios datos de identidad. A diferencia de los sistemas de identidad tradicionales, donde la información de identidad es gestionada por autoridades centrales como gobiernos o corporaciones (centralizados), las SSIs permiten a los usuarios poseer, gestionar y compartir su información personal de forma independiente. Los datos personales se almacenan de manera descentralizada, a menudo utilizando blockchain u otras tecnologías de libro mayor distribuido (descritas en el capítulo 3.2.5). Las SSIs están diseñadas para ser interoperables en diferentes plataformas y servicios, lo que permite a los usuarios utilizar su identidad digital en varios sistemas sin necesidad de múltiples inicios de sesión o registros (Preukschat & Reed, 2021).

Identificadores Decentralizados (DIDs)

Los Identificadores Descentralizados (DIDs) son fundamentales para el concepto de identidad autosoberana y representan un nuevo tipo de identificador diseñado para habilitar identidades digitales verificables y

autosoberanas. A diferencia de los identificadores tradicionales que son emitidos y controlados por autoridades centralizadas, los DIDs son creados, gestionados y controlados por el individuo o la entidad que identifican, sin la necesidad de un intermediario. Los DIDs están diseñados para ser interoperables en diferentes sistemas y plataformas. Siguen estándares abiertos para garantizar que puedan usarse de manera fluida en varios ecosistemas digitales (World Wide Web Consortium, 2022a). Los DIDs mejoran la privacidad al permitir a los usuarios controlar su información de identidad y compartir solo los detalles necesarios con otros. El uso de técnicas criptográficas garantiza la seguridad de los datos de identidad y los protege contra el acceso no autorizado y la manipulación. Con el uso de DIDs dentro del concepto de identidad autosoberana, los usuarios tienen control total sobre sus identidades digitales y pueden autenticarse sin depender de terceros (Preukschat & Reed, 2021).

3.2.5. Blockchain y Tecnologías de Libro Contable Distribuida (DLTs)

Los DLTs son una amplia categoría de tecnologías que abarcan varios sistemas (por ejemplo, blockchain) que permiten la emisión y verificación descentralizada de credenciales digitales. El concepto central de los DLT es la distribución descentralizada de datos entre una red de participantes, lo que reduce la necesidad de una autoridad central. Los DLTs operan en una arquitectura de red peer-to-peer donde cada participante (nodo) mantiene una copia de todo el libro mayor. Esta descentralización es fundamental para la seguridad y la confiabilidad de los DLTs, ya que elimina el riesgo de un único punto de falla y mejora la resiliencia de un sistema de credenciales (Narayanan et al., 2016; Zheng et al., 2017). Además, la descentralización mejora la confianza, ya que ninguna entidad tiene control sobre todo el sistema (Yli-Huumo et al., 2016).

Blockchain es el tipo más conocido de DLT y ofrece un registro descentralizado e inmutable de transacciones en bloques que están vinculados entre sí en una cadena. Como su nombre lo indica, blockchain contiene una cadena de varios bloques de datos. Cada bloque contiene una serie de transacciones. Una transacción puede involucrar bienes físicos, así como activos intangibles (por ejemplo, propiedad intelectual) (El Ioini & Pahl, 2018). El hash criptográfico de blockchain garantiza que, una vez que una credencial se registra en la blockchain, no puede ser alterada ni eliminada. Cualquier intento de cambiar una credencial requeriría alterar todos los bloques subsiguientes, lo cual es computacionalmente impráctico en una red blockchain bien establecida. Esta inmutabilidad es crucial para las credenciales digitales, ya que garantiza la integridad y autenticidad de las credenciales (Yli-Huumo et al., 2016).

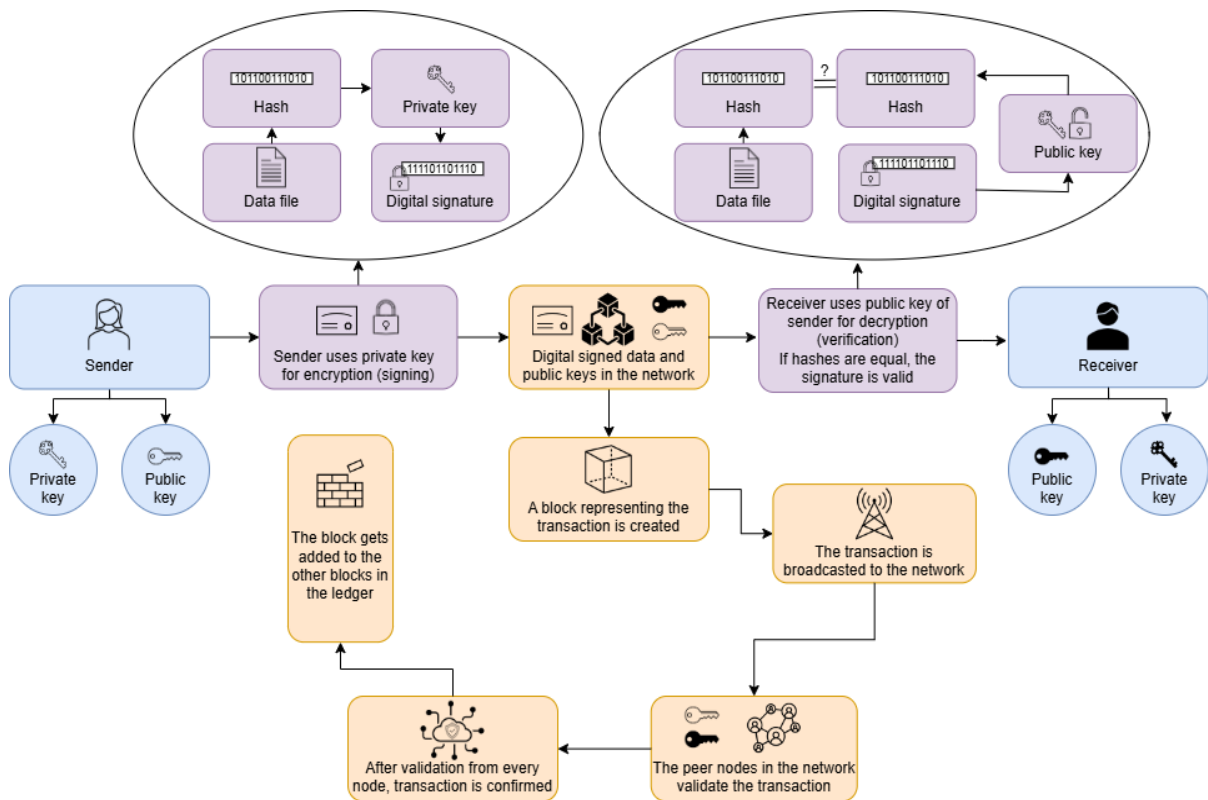
La tecnología blockchain ha surgido como una base robusta y segura para gestionar credenciales digitales, ya que sus propiedades de descentralización, inmutabilidad y transparencia la hacen particularmente adecuada para este propósito (Grech & Camilleri, 2017). Además, blockchain proporciona un registro transparente y públicamente verificable de transacciones. Para las credenciales digitales, esto significa que cualquiera puede verificar la autenticidad de una

credencial verificando la blockchain. Esta verificabilidad pública reduce el riesgo de fraude y mejora la credibilidad de las credenciales (Narayanan et al., 2016).

"Blockcerts" fue uno de los primeros estándares abiertos que utilizó la tecnología blockchain para crear, emitir y verificar certificados digitales (MIT Media Lab, 2016).

La siguiente Figura 3 muestra un ejemplo de un sistema basado en blockchain e integra los fundamentos tecnológicos descritos en los capítulos anteriores.

Figura 3: Proceso de operación de un Sistema basado en Blockchain



○ 3.3. Requerimientos Generales No-Funcionales

La implementación técnica de un sistema de credenciales digitales debe considerar tanto los requisitos tecnológicos como los sociales. Mühle y sus colegas (2023) modelaron los requisitos de un sistema de credenciales digitales basándose en la literatura existente, una multitud de proyectos y entrevistas con expertos. A continuación, se describe este marco conceptual. Tiene en cuenta requisitos integrales que consisten en siete categorías.

- **Funcionalidad Básica:** Las funcionalidades básicas de una tecnología de credenciales digitales consisten en emisión, presentación, almacenamiento, verificación y revocación (Mühle et al., 2023).

- **Controlabilidad:** La controlabilidad describe la necesidad de los usuarios de controlar las funcionalidades básicas. Comenzando con el proceso de emisión, incluye la solicitud de credenciales y el consentimiento de emisión. Después de recibir la credencial, el usuario también necesita controlar su uso posterior. Esto incluye el consentimiento para compartir, restricciones de verificación, así como notificaciones al usuario y eliminación. Este aspecto también cae bajo el término de Identidad Autosoberana (SSI), que se centra en la independencia de terceros. Da al usuario control sobre sus propios datos (Mühle et al., 2023).
- **Privacidad:** Este aspecto también se superpone con los principios de SSI. Uno de los requisitos es la seudonimización, que permite el anonimato de los usuarios, que por lo tanto no pueden ser rastreados a través de su información. Además, la minimización de datos y la divulgación selectiva son relevantes: solo se debe almacenar la información personal directamente relevante y los usuarios pueden decidir por sí mismos qué información debe revelarse (Mühle et al., 2023).
- **Usabilidad:** Otra parte esencial para el sector educativo es la consideración de funciones de conveniencia para el usuario, así como la accesibilidad, que abarca requisitos técnicos y opciones sin barreras. Las funciones convenientes incluyen la portabilidad, lo que significa poder acceder al sistema desde diferentes dispositivos, así como soluciones de almacenamiento y respaldo. Además, se debe considerar la posibilidad de una representación visual (por ejemplo, con insignias digitales), para permitir que los usuarios muestren sus logros (Mühle et al., 2023).
- **Seguridad:** Como se mencionó en capítulos anteriores, la seguridad es un aspecto crucial en muchos niveles diferentes. En primer lugar, las credenciales deben ser a prueba de manipulaciones para garantizar la integridad. La protección de datos también debe considerarse a nivel de la arquitectura del sistema. Otro requisito importante no es solo la validez de la credencial, sino la verificación de los actores (aprendiz y emisor) para establecer autenticidad y confianza en un ecosistema de credenciales digitales (Mühle et al., 2023).
- **Confianza:** Además de la seguridad a nivel técnico, también es importante considerar la confianza a nivel organizativo, no solo para los identificadores utilizados para la verificación técnica, sino la confianza en la identidad real de una organización. Para mantener la confianza en el sistema, este debe ser transparente y verificable, siguiendo una mentalidad de código abierto (Mühle et al., 2023).
- **Desplegabilidad:** Para permitir la estabilidad y la preparación para el futuro del sistema, los requisitos de escalabilidad, longevidad, interoperabilidad e integración deben contemplarse a nivel técnico y procedimental (Mühle et al., 2023).

● 4. Desarrollo Global de Credenciales Digitales

Una de las razones para el surgimiento de las credenciales digitales en la educación y la formación es el desarrollo general del sector educativo que busca una educación y formación profesional de alta calidad, por ejemplo, definida por la Agenda 2030 para el Desarrollo Sostenible de las Naciones Unidas. En esta agenda, se establecieron 17 Objetivos de Desarrollo Sostenible (ODS), uno de ellos es la educación con el objetivo general de "garantizar una educación inclusiva y equitativa de calidad y promover oportunidades de aprendizaje durante toda la vida para todos" (Naciones Unidas, 2022). Esta agenda marca el camino hacia un sistema educativo más flexible, inclusivo y de alta calidad en todo el mundo.

Nuevos requisitos y estándares, junto con las necesidades cambiantes de los aprendices y empleadores en la formación educativa, resultaron en avances tecnológicos, nuevas y más flexibles rutas de aprendizaje y entornos de aprendizaje alternativos. Paralelamente a este desarrollo, surgieron las credenciales digitales como una respuesta a las limitaciones de los certificados tradicionales en papel y comenzaron a ganar terreno a principios del siglo XXI. El concepto se popularizó en entornos de aprendizaje informal, comunidades y entre plataformas en línea, donde los participantes buscaban reconocimiento por completar tareas o cursos. En los últimos años, las instituciones de educación superior han adoptado cada vez más el uso de credenciales digitales como complemento a los títulos y certificados tradicionales (UNESCO, 2022).

La posibilidad de reconocer también volúmenes de aprendizaje más pequeños permite a los aprendices adquirir habilidades específicas que ayudan a mejorar las perspectivas de empleabilidad y avance profesional. Por lo tanto, las credenciales digitales también ganaron interés en la formación profesional, ya que el desarrollo de habilidades específicas es un factor importante en entornos laborales de rápido cambio y para las necesidades dinámicas del mercado laboral, asegurando adaptabilidad, flexibilidad y calidad del trabajo. Los siguientes capítulos ofrecen una visión general de los desarrollos regionales e internacionales, así como de los proveedores públicos y privados de credenciales digitales y gestión de credenciales. La sección concluye con las ventajas y desafíos de las credenciales digitales. Los desarrollos, iniciativas, proyectos e infraestructuras mencionados sirven como ejemplos. Dado que las credenciales digitales son un tema en auge en la educación y en otros lugares, no se pretende ofrecer un informe completo sobre los desarrollos actuales, sino más bien mostrar diversas aspiraciones con diferentes enfoques para resaltar la gran variedad y el alcance generalizado de los desarrollos en el contexto de las credenciales digitales.

○ 4.1. Europa

Europa ha estado a la vanguardia en el desarrollo e implementación de credenciales digitales para mejorar la movilidad educativa y profesional, la transparencia y el reconocimiento. El desarrollo en Europa se ve potenciado por importantes marcos e iniciativas de la Unión Europea, que buscan crear un entorno estandarizado, seguro e interoperable para la emisión, el reconocimiento y la verificación de credenciales digitales en todo el continente. Esta sección describe regulaciones generales e iniciativas ejemplares que aceleran el desarrollo y simplifican el uso de credenciales digitales en Europa.

4.1.1. Legislación

La legislación en torno a las credenciales digitales en Europa está influenciada en gran medida por las iniciativas de la Unión Europea para crear un entorno educativo y profesional más integrado y digitalizado. Sin embargo, puede haber regulaciones adicionales a nivel nacional. Estas regulaciones varían mucho entre los diferentes estados miembros, dependiendo también del sector donde se utilicen las credenciales digitales (por ejemplo, salud, educación, finanzas, etc.). A continuación, se describen dos regulaciones relevantes para Europa que sirven como base para los desarrollos nacionales en Europa.

Regulación General de Protección de Datos (GDPR)

El GDPR es una pieza fundamental de la legislación que impacta en el manejo de credenciales digitales. Establece requisitos estrictos para la protección de datos personales, lo que incluye la información contenida en las credenciales digitales. Los emisores de credenciales digitales deben garantizar que los datos personales se procesen de manera legal, transparente y segura. El GDPR es un reglamento que se aplica directamente a todos los estados miembros de la UE. El cumplimiento es obligatorio y todos los países están obligados a implementar y hacer cumplir sus disposiciones. Las autoridades nacionales de protección de datos en cada país supervisan el cumplimiento y pueden imponer sanciones por violaciones. Sin embargo, el nivel de cumplimiento y la conciencia pública pueden variar entre los estados miembros (EUR-Lex, 2016).

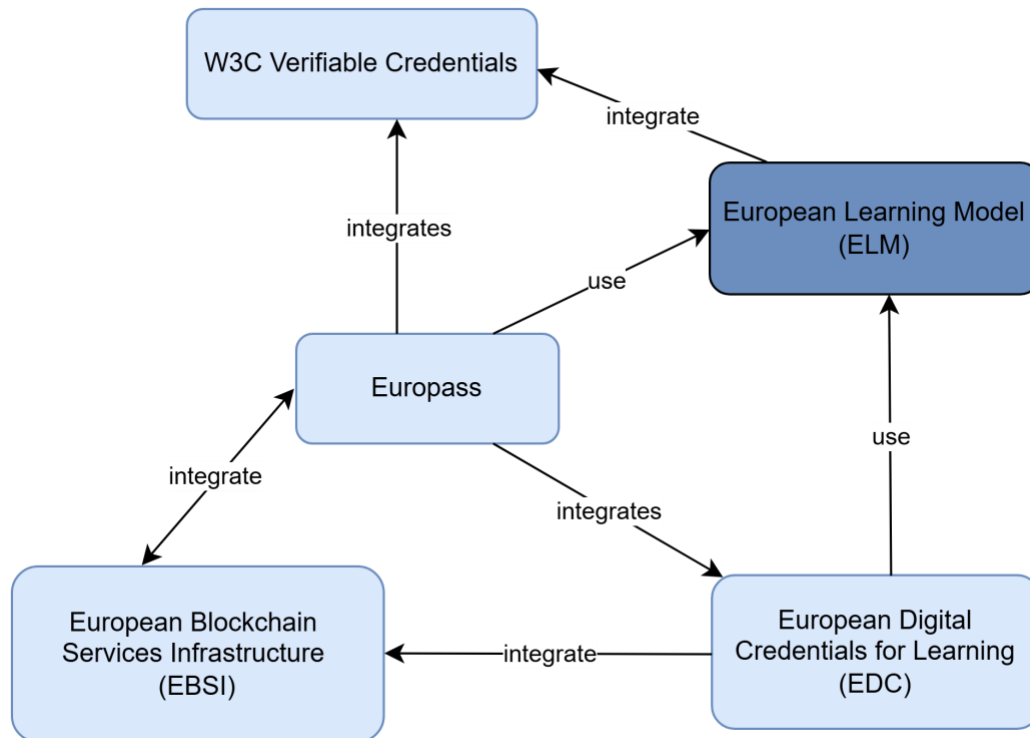
Regulación eIDAS

El Reglamento eIDAS (Identificación Electrónica, Autenticación y Servicios de Confianza) establece un marco europeo para la identificación electrónica y los servicios de confianza. Proporciona el reconocimiento legal de firmas electrónicas, sellos, marcas de tiempo y otros servicios de confianza, que son esenciales para la validez y confiabilidad de las credenciales digitales. El Reglamento eIDAS es directamente aplicable en todos los estados miembros de la UE y establece un marco para la identificación electrónica y los servicios de confianza. Si bien todos los países deben cumplir con sus requisitos, el nivel de adopción e integración de los servicios eIDAS puede diferir. Algunos países tienen sistemas avanzados de identificación digital y servicios de confianza, mientras que otros todavía están desarrollando su infraestructura (Comisión Europea, 2024).

4.1.2. Iniciativas e infraestructuras ejemplares

En los siguientes capítulos, se describen iniciativas, modelos e infraestructuras europeas relevantes. Están conectados y son complementarios, como muestra la siguiente Figura (Figura 4).

Figura 4: *Iniciativas de Sinergias Europeas, frameworks e infraestructuras*



Nota: Adaptado desde Europass (2023).

Modelo Europeo de Aprendizaje (European Learning Model) (ELM)

El Modelo Europeo de Aprendizaje (ELM) es un marco integral diseñado para apoyar el reconocimiento, validación y acreditación de los logros de aprendizaje en toda Europa. Su objetivo es garantizar que los resultados de aprendizaje, las calificaciones y las habilidades sean comprendidos y aceptados de manera uniforme en diferentes países europeos, facilitando la movilidad y el aprendizaje a lo largo de la vida (Comisión Europea, 2018).

El ELM enfatiza la importancia de resultados de aprendizaje claramente definidos, que son declaraciones de lo que se espera que un aprendiz sepa, comprenda y sea capaz de hacer después de completar un proceso de aprendizaje. Estos resultados están estandarizados para garantizar consistencia y transparencia en los diferentes sistemas educativos y de formación (Comisión Europea, 2018). El modelo promueve un enfoque basado en competencias, donde el enfoque está en las habilidades y competencias adquiridas en lugar del tiempo dedicado al aprendizaje. Este enfoque apoya las rutas de aprendizaje personalizadas y reconoce tanto las experiencias de aprendizaje formales como informales. Esto asegura que las habilidades y competencias adquiridas fuera de las instituciones educativas tradicionales, como a través de la experiencia

laboral o actividades comunitarias, sean reconocidas y valoradas (CEDEFOP, 2019). El ELM está estrechamente vinculado al Marco Europeo de Cualificaciones (EQF), que proporciona un marco de referencia común para comparar las cualificaciones de diferentes países. El EQF utiliza ocho niveles de referencia, basados en los resultados del aprendizaje, para facilitar el reconocimiento y la transferibilidad de las cualificaciones en toda Europa (Comisión Europea, 2018).

El ELM apoya el uso de herramientas y plataformas digitales para documentar y compartir logros de aprendizaje. Esto incluye el uso de credenciales digitales e insignias que pueden ser fácilmente verificadas y reconocidas a través de fronteras, mejorando la transparencia y la portabilidad de las calificaciones. El ELM se basa en la especificación de W3C Verifiable Credentials (Comisión Europea, 2020b).

Credenciales Digitales Europeas para el Aprendizaje (EDC)

Esta iniciativa es parte del esfuerzo más amplio de la Comisión Europea para promover la educación digital y la movilidad en toda Europa. El marco de Credenciales Digitales Europeas para el Aprendizaje permite a las instituciones educativas emitir diplomas digitales y otras credenciales de aprendizaje que son a prueba de manipulaciones y que pueden ser verificadas fácilmente a través de las fronteras. Este sistema es apoyado por el marco Europass, que busca estandarizar y simplificar el reconocimiento de calificaciones y habilidades en toda la UE. La adopción de las Credenciales Digitales Europeas para el Aprendizaje es un proceso en curso. Si bien el marco proporciona pautas y herramientas para la estandarización, el grado en que cada país ha integrado estas credenciales en sus sistemas educativos puede variar. Algunos países son adoptantes tempranos y han logrado avances significativos, mientras que otros todavía están en las etapas iniciales de implementación (Unión Europea, s.f.).

Europass

Europass es una iniciativa de la Unión Europea diseñada para mejorar la transparencia y la portabilidad de habilidades y calificaciones en toda Europa. Fue establecida por el Parlamento Europeo y el Consejo en 2004 como parte de los esfuerzos de la UE para promover el aprendizaje a lo largo de la vida y la movilidad dentro del mercado laboral. La iniciativa surgió de la Declaración de Copenhague de 2002, que enfatizó la necesidad de una mayor cooperación en la educación y formación profesional en toda Europa. Europass proporciona un marco estandarizado para presentar calificaciones, habilidades y experiencias, facilitando así la movilidad para estudiantes y trabajadores en los estados miembros (Unión Europea, 2004). Actualizado en 2020, el marco Europass proporciona herramientas para documentar y compartir información sobre habilidades y calificaciones. Incluye la Infraestructura de Credenciales Digitales Europass (EDCI), que permite la emisión, el intercambio y la verificación de credenciales digitales de manera segura e interoperable. Este marco asegura que las credenciales digitales sean consistentes y reconocibles en todos los estados miembros (Comisión Europea, 2023). El marco Europass está

ampliamente adoptado en los estados miembros de la UE. Proporciona un formato estandarizado para documentar y compartir calificaciones y habilidades, lo que facilita a las personas presentar sus credenciales en el extranjero. La mayoría de los países han establecido Centros Nacionales Europass para facilitar el uso de las herramientas y recursos de Europass (Comisión Europea, 2023).

Europass consta de diferentes herramientas que apoyan a las personas en su aprendizaje y desarrollo profesional: El "CV Europass" es un formato de currículum vitae integral que permite a las personas presentar sistemáticamente sus habilidades, calificaciones y experiencias. El "Pasaporte de Idiomas Europass" es una herramienta para autoevaluar las habilidades y calificaciones lingüísticas. "Europass Movilidad" es un registro de las habilidades y conocimientos adquiridos en otro país europeo a través de prácticas laborales, pasantías u otras experiencias de aprendizaje. El "Suplemento al Certificado Europass" proporciona información adicional a la incluida en los certificados oficiales, lo que facilita la comprensión de la naturaleza y el nivel de las cualificaciones. Finalmente, el "Suplemento al Título Europass" complementa los títulos de educación superior proporcionando una descripción estandarizada de la naturaleza, nivel, contexto, contenido y estatus de los estudios completados. Estas herramientas y documentos Europass se pueden acceder y completar en línea a través del portal Europass. El portal también integra varios servicios como herramientas de búsqueda de empleo e información sobre oportunidades de aprendizaje, lo que lo convierte en una plataforma integral para la gestión de carreras y la planificación educativa (Comisión Europea, 2023).

Europass ofrece varios beneficios clave. En primer lugar, proporciona un formato unificado y estandarizado para presentar calificaciones y habilidades, lo que facilita la comparación de credenciales entre diferentes países. Está disponible en varios idiomas, lo que garantiza que personas de diferentes antecedentes lingüísticos puedan utilizar las herramientas de manera efectiva. Además, la portabilidad es un beneficio importante, ya que apoya la movilidad al permitir que las personas presenten sus calificaciones de manera que sean fácilmente comprendidas y reconocidas en los estados miembros. Europass mejora la confianza en la autenticidad y validez de las calificaciones a través de la documentación estandarizada y los procesos de verificación digital, y ayuda a las personas a planificar y gestionar sus carreras al proporcionar herramientas para documentar y presentar sus habilidades y calificaciones de manera integral (Comisión Europea, 2023).

Infraestructura Europea de Servicios de Blockchain (EBSI)

La Infraestructura Europea de Servicios Blockchain (EBSI) es una iniciativa lanzada por la Comisión Europea y la Asociación Blockchain Europea (EBP) para aprovechar la tecnología blockchain en la prestación de servicios públicos transfronterizos en toda Europa. EBSI tiene como objetivo crear una infraestructura digital segura y confiable que pueda usarse para mejorar la eficiencia y la transparencia de los servicios digitales dentro de la Unión

Europea. Para garantizar la transparencia, la seguridad y la inmutabilidad de los datos, EBSI utiliza blockchain y opera a través de una red de nodos gestionados por varios países europeos. Cada nodo de la red mantiene una copia de la blockchain, lo que garantiza su fiabilidad (Comisión Europea, s.f.-b).

Uno de los objetivos principales de EBSI es facilitar la interoperabilidad entre diferentes plataformas blockchain y los sistemas informáticos tradicionales. Esto es crucial para integrar los servicios blockchain con los procesos administrativos existentes y para garantizar intercambios de datos transfronterizos sin problemas. Uno de los casos de uso principales de EBSI son las credenciales académicas que se emiten y verifican en blockchain. EBSI respalda la identidad autosoberana (SSI), que permite a los estudiantes poseer y controlar su identidad digital y credenciales. Los estudiantes reciben sus diplomas en una billetera digital, donde pueden gestionar y compartir sus credenciales según sea necesario. Se han realizado varios proyectos piloto para probar y perfeccionar el Caso de Uso del Diploma. Estos pilotos involucran a múltiples universidades e instituciones educativas en diferentes estados miembros de la UE, proporcionando información valiosa y comentarios para mejorar el sistema (Comisión Europea, s.f.-b).

La gobernanza de EBSI está gestionada por la Asociación Blockchain Europea, que incluye representantes de los estados miembros y la Comisión Europea. Esta asociación establece la dirección estratégica, supervisa la implementación y garantiza que la infraestructura esté alineada con las regulaciones y políticas de la UE. También colabora con organismos de normalización para garantizar que sus soluciones sean compatibles con los estándares globales de blockchain (Comisión Europea, s.f.-b).

○ **4.2. Latinoamérica**

Esta sección proporciona una visión general de los desarrollos clave en torno a las credenciales digitales dentro de América Latina. Al examinar iniciativas clave, esta sección tiene como objetivo proporcionar una comprensión fundamental que apoye la adopción e integración exitosa de credenciales digitales en contextos profesionales en esta región, como lo pretende el proyecto ECOCredGT (ECOCredGT, s.f.).

4.2.1. Legislación

El entorno legislativo para las credenciales digitales en América Latina es variado, lo que refleja las diversas políticas educativas e infraestructuras tecnológicas de los diferentes países.

Específicamente en Guatemala, según el conocimiento de los autores, no existe un marco legal específico dedicado a las credenciales digitales. Sin embargo, existen leyes vigentes que pueden aplicarse al procesamiento de datos personales. En particular, la Ley de Acceso a la Información Pública, aunque está destinada principalmente a las entidades estatales o aquellas financiadas por el Estado, contiene disposiciones que pueden interpretarse como aplicables

a cualquier forma de procesamiento de datos personales, incluidas las entidades privadas. Además, ha habido ambiciones proactivas en esta área, iniciando acciones legales significativas contra entidades que procesan datos personales. Esto ha llevado a la Corte Constitucional a emitir varios fallos, afirmando consistentemente la protección de los sujetos de datos. Estos fallos reconocen los derechos de los sujetos de datos en los contextos de procesamiento de datos, incluidos el consentimiento informado, el acceso, la rectificación, la cancelación y la oposición. Además, cualquier transferencia de datos personales, ya sea local o internacional, requiere el consentimiento del sujeto de los datos, proporcionado por escrito o en un formato digitalmente recuperable (OneTrust, 2024).

Guatemala está avanzando hacia la digitalización, pero enfrenta desafíos administrativos y culturales, según una publicación de blog del Programa de las Naciones Unidas para el Desarrollo (PNUD). El blog destaca la participación de Guatemala en la Evaluación de Preparación Digital (DRA) del PNUD, que tiene como objetivo fomentar la transformación digital inclusiva al involucrar a una amplia gama de partes interesadas, incluidos el gobierno, las empresas, la sociedad civil y los académicos. Guatemala obtuvo buenos resultados en áreas como la conectividad, el liderazgo político y la participación pública, pero enfrenta desafíos comunes a los esfuerzos de digitalización global. Se identificaron problemas regulatorios, particularmente en protección de datos y comercio electrónico, como áreas críticas que necesitan mejoras. Además, las lagunas en los marcos legislativos existentes podrían obstaculizar una transformación digital exitosa.

Un desafío significativo radica en la Infraestructura Pública Digital (DPI), que incluye el intercambio de datos, los pagos digitales y la identificación digital nacional. A pesar de los avances, problemas como la gestión de datos y la falta de habilidades digitales y capacidad técnica son barreras para la adopción generalizada de DPI.

El PNUD recomienda que Guatemala adopte un enfoque sostenible para DPI, enfatizando una gobernanza sólida, medidas con enfoque de género e inclusividad basada en derechos. Mejorar la conectividad y adoptar un enfoque de diseño centrado en las personas también son clave para garantizar el éxito de la transformación digital en el país (Biometrics Research Group, 2023).

4.2.2. Iniciativas e Infraestructuras ejemplares

Los desarrollos regionales en América Latina en el contexto de las credenciales digitales en la educación actualmente están más enfocados en las instituciones académicas. Sin embargo, también hay algunos ejemplos avanzados de sistemas de credenciales digitales fuera del mundo académico. En los siguientes capítulos, se describen algunas iniciativas e infraestructuras ejemplares. Esto no es exhaustivo, sino más bien una selección que debería reflejar la amplia gama de desarrollos en el contexto de las credenciales digitales en América Latina.

Instituciones Académicas

Como se mencionó anteriormente, hay varios desarrollos en el sector de la educación superior. Por mencionar algunos ejemplos nacionales, la universidad "Tecnológico de Monterrey", una de las principales universidades de México, ha implementado un sistema de credenciales digitales para mejorar el reconocimiento y la portabilidad de los logros académicos. La universidad utiliza tecnología blockchain para emitir diplomas y certificados seguros y a prueba de manipulaciones, lo que facilita la verificación para empleadores y otras instituciones educativas (Tecnológico de Monterrey, 2023).

La universidad "Universidad Nacional de Córdoba", una de las universidades más antiguas y prestigiosas de Argentina, ha comenzado a emitir insignias digitales para reconocer la participación de los estudiantes en talleres, seminarios y actividades extracurriculares. Estas insignias están diseñadas para complementar los registros académicos tradicionales y proporcionar una visión más completa de las habilidades y logros de los estudiantes (edX, 2024).

La "Universidad de Chile" ha desarrollado una plataforma de certificación digital para emitir y verificar credenciales académicas. Esta plataforma utiliza firmas digitales seguras y una base de datos centralizada para garantizar la autenticidad e integridad de los diplomas y certificados, facilitando su aceptación tanto a nivel nacional como internacional (Universidad de Chile, s.f.).

La "Pontificia Universidad Católica del Perú (PUCP)" ha ampliado su oferta de aprendizaje en línea e integrado credenciales digitales para reconocer la finalización de cursos y programas. Este enfoque apoya el aprendizaje a lo largo de la vida y proporciona a los estudiantes una prueba verificable de sus logros que pueden compartir con empleadores y otras instituciones educativas (PUCP, 2024a). Además, también ofrecen varios programas de formación con certificaciones digitales en el campo de la formación vocacional y educativa para empresas (PUCP, 2024b).

Instituciones Profesionales

En Brasil, el Servicio Nacional de Aprendizaje Industrial (SENAI), que es el centro privado de educación técnica y profesional más grande de América Latina, ha lanzado una iniciativa para proporcionar microcredenciales para varios cursos técnicos y vocacionales. Este programa tiene como objetivo satisfacer las necesidades cambiantes del mercado laboral ofreciendo oportunidades de aprendizaje flexibles y modulares que pueden ser fácilmente verificadas y reconocidas por los empleadores (Confederação Nacional da Indústria, s.f.).

El Servicio Nacional de Aprendizaje (SENA) en Colombia ha adoptado la tecnología blockchain para emitir certificados digitales para sus programas de formación profesional. SENA es una institución pública colombiana que ofrece formación técnica y profesional gratuita a unos 9 millones de colombianos cada año. Como la institución pública más grande del país, SENA tiene una cobertura nacional integral a través de 117 centros de formación específicos de la industria y una extensa plataforma en línea. Su misión es cultivar y expandir una fuerza

laboral técnicamente capacitada para satisfacer las demandas del desarrollo nacional de Colombia y una economía internacional en crecimiento (100.000 Strong in the Americas, 2024).

IDB Digital Credential Framework for Creating and Issuing Credentials

Desde 2018, el Banco Interamericano de Desarrollo (BID), que se describe a sí mismo como "la principal fuente de financiamiento para el desarrollo de América Latina y el Caribe", recompensa diferentes oportunidades de aprendizaje con credenciales digitales. En 2023, establecieron una hoja de ruta para reconocer la construcción de conocimientos y el aprendizaje con credenciales digitales, con principios y pautas claras para la creación y emisión de dichas credenciales, no solo para el Grupo BID, sino también para organizaciones y ciudadanos de la región LAC. Hasta enero de 2023, el BID ha emitido más de 200.000 insignias digitales. Esta iniciativa tiene como objetivo promover la movilidad de estudiantes y trabajadores dentro de América Latina y el Caribe mediante la creación de un marco unificado para la emisión de credenciales digitales y, por lo tanto, actúa como una iniciativa pionera en el contexto de las credenciales digitales en la región LAC (Porto & Presant, 2023).

○ 4.3. Desarrollos Internacionales

El panorama internacional de las credenciales digitales se caracteriza por una mezcla de iniciativas gubernamentales, proyectos e innovaciones del sector privado. Además, formatos estándar como la especificación Open Badges y las Credenciales Verificables de W3C se utilizan globalmente por instituciones educativas, organizaciones profesionales y plataformas de aprendizaje en línea para reconocer una amplia gama de habilidades y logros y para proporcionar un formato estándar para la creación, emisión y verificación de credenciales digitales (1EdTech, 2024a; World Wide Web Consortium, 2022b). En los siguientes capítulos, se describen iniciativas internacionales ejemplares, redes y estándares.

4.3.1. Digital Credential Consortium (DCC)

El Consorcio de Credenciales Digitales (DCC), fundado en 2019, es un ejemplo de una iniciativa que incluye socios de todo el mundo, desde Europa, Estados Unidos, Canadá y México. Están construyendo una infraestructura para credenciales académicas digitales para apoyar los sistemas educativos del futuro. DCC está explorando las posibilidades de los desarrollos recientes en estándares de datos de credenciales y métodos criptográficos para el reconocimiento de logros académicos y proporcionando diversos recursos en este contexto. Además, están diseñando un sistema de gobernanza, así como una infraestructura tecnológica para credenciales académicas. Todo el software desarrollado es de código abierto, lo que apoya la emisión de credenciales para organizaciones (MIT Open Learning, 2024).

4.3.2. Groningen Declaration Network

La Red de la Declaración de Groningen es una red internacional sin fines de lucro de individuos y organizaciones que se enfoca en la portabilidad de datos

estudiantiles digitales, basándose en la Declaración de Groningen. Hoy en día, la red cuenta con participantes y signatarios de más de 29 países en todo el mundo. El propósito de la Red de la Declaración de Groningen es desarrollar, ofrecer, apoyar y asesorar sobre la Portabilidad de Datos Estudiantiles Digitales (DSDP), centrándose particularmente en la consulta mutua y el intercambio de información entre las partes interesadas en todo el mundo, especialmente las instituciones de educación superior. Quieren desarrollar y promover mejores prácticas y estándares aceptados globalmente para consultas e intercambios de información seguros y orientados al ciudadano sobre DSDP. La Red busca lograr sus objetivos creando y facilitando una red alineada con los objetivos de la fundación, reuniendo a las partes interesadas en el campo de DSDP, utilizando multimedia para los fines de la fundación, generando publicidad por cualquier medio para apoyar los objetivos de la fundación, adquiriendo y proporcionando recursos, y participando en cualquier actividad directamente o indirectamente relacionada con estos objetivos (Groningen Declaration, s.f.).

4.3.3. Credential Engine

Credential Engine es una organización sin fines de lucro que se originó a partir de la Iniciativa de Transparencia de Credenciales (CTI) en 2013. CTI tenía como objetivo desarrollar un registro centralizado de información de credenciales, crear un lenguaje común de acreditación y construir un motor de búsqueda de credenciales. En diciembre de 2016, Credential Engine se estableció oficialmente para implementar el trabajo de CTI. Credential Engine está dedicada a mapear el panorama de las credenciales, brindando información clara y coherente. Su misión es empoderar a las personas para descubrir las mejores rutas para sus necesidades. Credential Engine ofrece una gama de servicios web, incluido el primer Registro Centralizado de Credenciales que alberga información actual sobre todo tipo de credenciales y proporciona datos estandarizados sobre los atributos de las credenciales, como sus competencias, costos y resultados, lo que facilita que los estudiantes, educadores, empleadores y legisladores las comprendan y comparen. También proporciona el Lenguaje de Descripción de Transparencia de Credenciales (CTDL), un lenguaje común que facilita la comparabilidad de credenciales y mejora la garantía de calidad, además de una plataforma para desarrollar aplicaciones personalizadas para buscar y recuperar información de credenciales. Credential Engine trabaja con estudiantes, proveedores de credenciales, empleadores y legisladores para ayudarles a comprender el valor de las credenciales digitales (Credential Engine, 2024).

4.3.4. Monitor de Credenciales Digitales

El Monitor de Credenciales Digitales es una iniciativa conjunta del Servicio Alemán de Intercambio Académico (DAAD), la Red de la Declaración de Groningen (GDN) y la UNESCO, cuyo objetivo es crear una fuente de conocimiento colaborativo sobre credenciales digitales en la educación en todo el mundo. El objetivo principal de esta iniciativa es recopilar datos sobre iniciativas, pilotos, proyectos, mejores prácticas e infraestructuras tecnológicas implementadas en todo el mundo para realizar análisis y representar los

resultados en una herramienta visual. Además, estos resultados deberían generar nuevas perspectivas sobre las credenciales digitales en diferentes países y abrir un espacio para discusiones e intercambios. La creación de la herramienta visual está basada en la comunidad, donde los datos pueden agregarse de manera individual a través de una encuesta en línea (Deutscher Akademischer Austauschdienst e.V., 2023, 2024).

4.3.5. Consorcio World Wide Web (W3C) y Credenciales Verificables (VC)

El Consorcio World Wide Web (W3C) es una organización internacional sin fines de lucro que desarrolla recomendaciones (estándares web, especificaciones técnicas y directrices) dentro de una comunidad: más de 350 organizaciones miembros de todo el mundo, personal y el público (World Wide Web Consortium, 2024a).

En el contexto de las credenciales digitales, el estándar abierto "Modelo de Datos de Credenciales Verificables v2.0" puede considerarse uno de los desarrollos internacionales más importantes. La última versión se publicó en 2024 y la especificación tiene como objetivo proporcionar un método estandarizado para expresar credenciales en la web (como licencias de conducir, títulos universitarios y pasaportes) de manera criptográficamente segura, respetuosa de la privacidad y verificable por máquina. Se basa en versiones anteriores mejorando las funciones de seguridad y privacidad, abordando problemas como el robo de dispositivos y la suplantación, y proporcionando directrices detalladas para la accesibilidad e internacionalización. Incluye secciones completas sobre los componentes de las credenciales verificables y las presentaciones, una visión general del ecosistema y consideraciones sobre privacidad. Existen diferentes roles dentro de esta especificación: el emisor, el titular y el verificador, como se describe en el capítulo 3.1. Una credencial verificable contiene información sobre el sujeto de la credencial (por ejemplo, una persona), el emisor (por ejemplo, un organismo gubernamental), las afirmaciones que se hacen (por ejemplo, la edad del sujeto) y pruebas (por ejemplo, firmas digitales) para garantizar la integridad y autenticidad de la credencial. Puede incluir datos como imágenes, nombres, números de identificación, tipo de credencial, fecha de emisión y fecha de vencimiento. El modelo de datos admite técnicas que preservan la privacidad, como las pruebas de conocimiento cero, que permiten al titular probar una declaración sin revelar todos los datos subyacentes. Además, la especificación incluye directrices para garantizar que las credenciales sean accesibles para una amplia gama de usuarios y puedan utilizarse internacionalmente, por ejemplo, con soporte para diferentes idiomas. El modelo tiene como objetivo hacer que las credenciales digitales sean más confiables y fáciles de administrar en comparación con sus contrapartes físicas. Además, el W3C busca activamente comentarios de la comunidad e implementa retroalimentación para esta especificación (World Wide Web Consortium, 2024).

4.3.6. 1EdTech, Open Badges and Comprehensive Learner Record (CLR)

1EdTech es una organización con más de 900 organizaciones miembros en más de 32 países en todo el mundo. Esta comunidad colaborativa está dedicada a crear un ecosistema de tecnología educativa abierto, confiable e innovador que aborde las necesidades de aprendizaje a lo largo de la vida de cada individuo. 1EdTech quiere empoderar a todas las partes interesadas para contribuir activamente a mejorar las oportunidades y experiencias educativas en beneficio de la sociedad (1EdTech, 2024b).

En el contexto de las credenciales digitales, uno de los desarrollos más importantes es la "Especificación Open Badges". Describe una norma sobre cómo se agrega e incorpora información sobre logros adquiridos en un archivo como una insignia digital. Además, define procedimientos para verificar la autenticidad de las insignias y una API para intercambiar información sobre las insignias. El uso de este formato estandarizado garantiza la interoperabilidad, verificabilidad y portabilidad de las insignias digitales. Los principales interesados en la especificación son los ganadores de insignias, cuyos logros están representados por las insignias. Los emisores de insignias definen, evalúan y proporcionan el logro a través de las insignias. Un visor de insignias es cualquier persona que observe las insignias para comprender el logro del estudiante, como educadores o empleadores. Además, existen validadores de insignias que son beneficiosos para examinar y reconocer el valor de las insignias. La última versión de este estándar es la "Especificación Open Badges 3.0" con la extensión de la tecnología blockchain e identificadores descentralizados en comparación con versiones anteriores. Se alinea con las convenciones del Modelo de Datos de Credenciales Verificables v2.0 (1EdTech, 2024a).

Otra especificación técnica importante establecida por 1EdTech para uso global es un estándar para registros de aprendizaje de por vida, llamado Comprehensive Learner Record (CLR). Este estándar admite el reconocimiento de una amplia variedad de logros académicos y laborales, incluidos cursos, competencias, habilidades y logros basados en el empleador. Está diseñado para ser fácil de usar y está destinado a ser utilizado, curado y controlado por el estudiante. Proporciona un formato interoperable y compatible con la web que es fácil de entender y lo suficientemente flexible como para admitir diversos casos de uso. Esta adaptabilidad garantiza que satisfaga las diversas necesidades de estudiantes, trabajadores, registradores y empleadores. Las credenciales digitales producidas con el formato de Credenciales Verificables del W3C o Open Badges se agrupan fácilmente en CLR (1EdTech, 2024c).

En el núcleo de ambos, Open Badges y CLR, está el concepto de una afirmación sobre uno o más logros. Estas afirmaciones son específicas para un estudiante e incluyen afirmaciones sobre un logro particular, junto con metadatos como emisor, estudiante, fecha de logro, fecha de vencimiento, así como posibles pruebas que respalden la afirmación (1EdTech, 2024c).

El CLR permite agrupar múltiples credenciales y crear asociaciones entre ellas. Esto puede visualizarse como agregar otra capa alrededor de las credenciales, que también son verificables individualmente. Los CLRs pueden incluir logros de varios emisores, lo que refleja la progresión de un estudiante a través de diferentes organizaciones o departamentos dentro de una gran institución educativa. Además, los emisores pueden agrupar múltiples credenciales relacionadas en transcripciones y otros registros integrales dentro de un CLR, conocido como ClrCredential. Este ClrCredential se firma de la misma manera que las credenciales individuales, garantizando su autenticidad. Además, las credenciales pueden mejorarse con un EndorsementCredential de un tercero, agregando otra capa de validación y apoyo a la calidad o relevancia de los datos de la credencial (1EdTech, 2024c).

4.3.7. Estándar Blockcerts

Desde que la tecnología blockchain evolucionó como una tecnología bien adaptada y comúnmente utilizada para la gestión de credenciales digitales, la estandarización también es relevante en este contexto. El estándar Blockcerts es un estándar abierto para crear, emitir, visualizar y verificar certificados basados en blockchain. Fue desarrollado por el MIT Media Lab en colaboración con Learning Machine, ahora Hyland Credentials (Hyland, 2024). Hyland continúa el desarrollo continuo como el principal responsable de este proyecto.

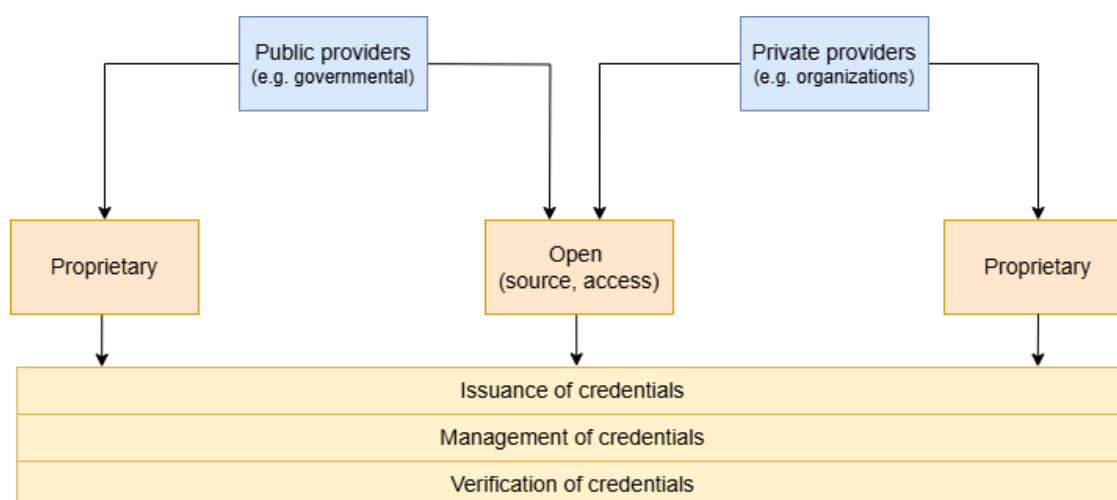
El estándar Blockcerts aprovecha las capacidades de blockchain para proporcionar un método seguro y a prueba de manipulaciones para manejar credenciales digitales. Su código y documentación son de código abierto, lo que fomenta la adopción y colaboración generalizadas, permitiendo a los desarrolladores e instituciones construir y mejorar el estándar. Aunque inicialmente diseñado para funcionar con la blockchain de Bitcoin, Blockcerts es independiente de la blockchain, lo que significa que puede implementarse en cualquier plataforma blockchain. Esta flexibilidad permite a las instituciones elegir la blockchain que mejor se adapte a sus necesidades y preferencias. Otros componentes clave del estándar son la interoperabilidad, la seguridad mejorada mediante el uso de libros de contabilidad inmutables y la verificación descentralizada. Blockcerts empodera a los destinatarios al otorgarles la propiedad de sus credenciales digitales. Las personas pueden almacenar sus certificados en billeteras digitales y compartirlos según sea necesario, controlando quién tiene acceso a su información.

Blockcerts ha sido adoptado por diversas instituciones educativas, organizaciones profesionales y organismos de certificación en todo el mundo. Tiene el potencial de optimizar los procesos de acreditación, reducir el fraude y empoderar a las personas con un mayor control sobre sus logros. El objetivo es crear recursos técnicos que otros desarrolladores puedan utilizar en sus propios proyectos. Al proporcionar un método confiable y verificable para emitir y compartir certificados digitales, Blockcerts respalda la adopción más amplia de la tecnología blockchain en la educación y más allá (MIT Media Lab, 2016).

○ 4.4. Proveedores

Los proveedores son esenciales en un ecosistema de credenciales digitales porque pueden facilitar la emisión, gestión, verificación y reconocimiento de credenciales digitales. Ayudan a garantizar que las credenciales sean seguras, confiables y reconocidas en varios sectores. Existe una amplia gama de proveedores públicos y privados para la emisión de credenciales digitales. La elección de un proveedor depende de varios factores, incluido el tipo de credencial, su uso previsto, el nivel de confianza y reconocimiento requerido, y las preferencias organizacionales (UNESCO, 2018).

Figura 5: Proveedores de credenciales digitales (sistema)



4.4.1. Proveedores Públicos

Los proveedores públicos suelen ser gubernamentales o respaldados por el estado y emiten credenciales digitales para fines oficiales. Ellos imponen estándares para que las credenciales cumplan con requisitos legales, de privacidad y seguridad específicos. Por lo tanto, son ampliamente reconocidos en diferentes sectores y a través de fronteras internacionales. Debido a su peso legal, la confianza y la legitimidad pueden mencionarse como principales ventajas. Además, ayudan a crear marcos estandarizados para la acreditación para garantizar la consistencia e interoperabilidad. Por otro lado, debido a las estructuras burocráticas, también pueden ser más lentos en la adopción de nuevas tecnologías (UNESCO, 2018).

Los proveedores públicos están conectados o son operados por el gobierno y, a menudo, emiten credenciales digitales a nivel nacional o en una determinada región. Estos incluyen los ministerios de educación de los respectivos países, otras autoridades reguladoras (por ejemplo, la Autoridad de Calidad de Habilidades de Australia) o universidades públicas.

4.4.2. Proveedores Privados

Los proveedores privados incluyen organizaciones no gubernamentales y empresas (por ejemplo, organizaciones profesionales, empresas de tecnología).

Están impulsados por el mercado y compiten con otros proveedores. A menudo se enfocan en sectores específicos, por ejemplo, certificaciones tecnológicas. Uno de los beneficios de los proveedores privados es su flexibilidad y adaptabilidad a las necesidades de la industria, y pueden ofrecer soluciones personalizadas, así como tecnologías innovadoras. Sin embargo, las credenciales de los proveedores privados pueden no tener siempre el mismo nivel de reconocimiento o confianza que las de las entidades públicas (UNESCO, 2018).

Instituciones Educativas y Plataformas de Aprendizaje Online

- **Coursera:** Coursera es una plataforma de aprendizaje en línea que ofrece cursos, especializaciones, títulos y certificados digitales para universidades y empresas en todo el mundo. Se asocia con instituciones como Stanford, Yale y Google para ofrecer una amplia gama de temas en sus cursos (Coursera, 2024).
- **edX:** edX es un proveedor conocido de cursos masivos abiertos en línea (MOOC) fundado por Harvard y MIT. Ofrece cursos a nivel universitario en una amplia gama de disciplinas, incluidos cursos gratuitos y programas para certificaciones profesionales, microcredenciales y títulos completos en línea (edX, 2024).
- **FutureLearn:** FutureLearn es una plataforma MOOC con sede en el Reino Unido, que ofrece cursos en línea y títulos de universidades e instituciones culturales de todo el mundo. Proporciona una experiencia de aprendizaje social y oportunidades para obtener certificados y microcredenciales (FutureLearn, 2012).
- **LinkedIn Learning:** LinkedIn Learning ofrece una vasta biblioteca de cursos en video sobre software, habilidades creativas y empresariales. Está integrado con los perfiles de LinkedIn, lo que permite a los usuarios mostrar certificaciones de cursos completados (LinkedIn Learning, 2024).
- **Udacity:** Udacity se enfoca en la tecnología, ofreciendo programas de "Nanodegree" diseñados para capacitar a las personas en campos como la programación, la ciencia de datos, la inteligencia artificial y el marketing digital. Colabora con líderes de la industria como Google e IBM para diseñar sus cursos (Udacity, 2011).

Organizaciones Profesionales y Empresas

- **CompTIA:** La Asociación de la Industria de Tecnología de la Computación (CompTIA) es un defensor del ecosistema global de tecnología de la información. Apoya el crecimiento de la industria a través de la educación, la formación, las certificaciones y la investigación de mercado, con el objetivo de desarrollar una fuerza laboral altamente capacitada y promover un entorno propicio para la innovación. Ha otorgado más de 2.5 millones de certificaciones en áreas como ciberseguridad, redes, computación en la nube y soporte técnico. CompTIA también mantiene un programa de socios internacionales con

miles de instituciones académicas, organizaciones sin fines de lucro, centros de empleo y otras organizaciones (CompTIA s.f.).

- **Credly:** Credly es una plataforma de acreditación digital que trabaja con organizaciones para emitir, gestionar y verificar credenciales digitales e insignias. Apoya a varias industrias e integra con sistemas de gestión del aprendizaje (Credly by Pearson, 2024).
- **IBM:** IBM ofrece credenciales digitales a través de su Programa de Insignias Digitales de IBM, que reconoce habilidades y logros en áreas como la computación en la nube, la inteligencia artificial y la ciberseguridad. Estas insignias están diseñadas para mostrar habilidades verificadas y son reconocidas en la industria (IBM, s.f.).
- **Microsoft:** Microsoft colabora con socios de la industria y la educación para proporcionar soluciones de acreditación digital. A través de su plataforma en la nube Azure, Microsoft apoya el desarrollo de credenciales verificables que se pueden compartir y verificar de manera segura (Microsoft Security, 2024).

○ 4.5. Ventajas y Posibilidades de las Credenciales Digitales

Como ya se destacó en capítulos anteriores, existen muchas posibilidades y ventajas en el uso de credenciales digitales. Además de fomentar la participación en actividades de aprendizaje, la construcción y el compromiso con la comunidad es un beneficio importante de las credenciales digitales. Diferentes estudios muestran que compartir insignias y microcredenciales obtenidas en línea motiva a los estudiantes. Además, los instructores y educadores también se involucran con la comunidad, de modo que las insignias pueden ayudar en la estandarización de los criterios de acreditación y los planes de estudio, y en la formación de una comunidad educativa colaborativa (Stefaniak & Carey, 2019; Carey & Stefaniak, 2018).

Otro beneficio de las credenciales digitales es su mayor seguridad en comparación con las credenciales tradicionales en papel. Las credenciales digitales utilizan técnicas criptográficas para evitar la manipulación y garantizar que la información permanezca inalterada y verificable (Gréther et al., 2018). El uso de la tecnología blockchain mejora aún más la seguridad al proporcionar un libro mayor descentralizado e inmutable que registra la emisión y verificación de credenciales. A cada credencial se le asigna un identificador único, lo que hace que sea casi imposible alterarla o falsificarla (Sharples & Domingue, 2016).

La interoperabilidad de las credenciales digitales es otra ventaja significativa. Las credenciales digitales pueden diseñarse para ser compatibles con varios estándares y sistemas, lo que facilita su uso en diferentes plataformas y jurisdicciones. Esta interoperabilidad es crucial para las personas que necesitan presentar sus credenciales a empleadores, instituciones educativas o agencias gubernamentales en diferentes regiones o países. Los estándares, como la

especificación Open Badges, proporcionan un marco para la creación, emisión y verificación de credenciales digitales, lo que garantiza que puedan ser ampliamente reconocidas y aceptadas (Casilli & Hickey, 2016).

La Unión Europea describe beneficios para diferentes partes interesadas: individuos, empleadores y proveedores de educación y formación. Los individuos pueden construir un portafolio en línea para rastrear todos sus logros de aprendizaje, mientras tienen el control total de sus datos. Pueden reutilizar fácilmente sus credenciales para postularse a un empleo o para continuar su formación, y pueden presentar y hacer verificar sus credenciales en cualquier momento de su carrera. Los empleadores pueden reducir significativamente el tiempo y los costos de verificación de credenciales y procesamiento de solicitudes de empleo. Pueden comprender mejor las credenciales de los candidatos, especialmente de otros estados miembros, ya que estarán traducidas a su propio idioma y podrán confiar en credenciales a prueba de manipulaciones. Los proveedores de educación y formación pueden reducir su carga administrativa y los costos de emisión de credenciales, al mismo tiempo que aceleran los procedimientos de emisión al digitalizarse (Unión Europea, s.f.).

○ 4.6. Retos e Implicaciones

Al aprovechar tecnologías como blockchain y PKI, las credenciales digitales verificables ofrecen mayor conveniencia. Sin embargo, abordar los desafíos de seguridad, privacidad, interoperabilidad y adopción es crucial para aprovechar todo su potencial.

Para que las credenciales digitales sean ampliamente aceptadas, deben ser interoperables entre diferentes sistemas y plataformas. Los estándares para formatos, tecnologías y aseguramiento de la calidad son esenciales para garantizar que las credenciales emitidas por diferentes organizaciones puedan ser comprendidas y verificadas globalmente.

Otro desafío es la falta de conciencia y comprensión entre las partes interesadas, la resistencia al cambio de los sistemas de acreditación tradicionales y la necesidad de marcos legales sólidos que respalden la validez y el reconocimiento de las credenciales digitales (van der Hijden & Martin, 2023). Además, debido a la alta relevancia y enfoque en las credenciales digitales en la investigación y la práctica, surgirán aún más iniciativas, proyectos, infraestructuras, directrices y recomendaciones. Esto puede resultar en una dificultad para mantener una visión clara en este paisaje complejo. Para evitar sobrecargar a los aprendices, así como a los posibles futuros proveedores u otras partes interesadas, las iniciativas, proyectos y redes actuales y futuras deben trabajar juntas para formar soluciones y resultados colaborativos y ampliamente aceptados para la acreditación digital.

● 5. Conclusiones

Este documento del estado del arte ha proporcionado una visión general amplia de las credenciales digitales con un enfoque en la educación y la formación profesional. Al definir las credenciales digitales, exploramos varias interpretaciones y significados de las credenciales digitales y términos y conceptos relacionados. Esto es crucial para comprender el panorama y el impacto potencial de las credenciales digitales.

Al delinear el proceso operativo de un ecosistema de credenciales digitales y las tecnologías fundamentales que permiten credenciales digitales seguras y verificables, como blockchain y la infraestructura de clave pública, destacamos los mecanismos que aseguran la integridad y confiabilidad de las credenciales digitales. Además, abordamos requisitos no funcionales críticos como la seguridad y la privacidad.

La sección sobre desarrollos globales mostró iniciativas y avances significativos en el contexto de las credenciales digitales, con un enfoque en iniciativas europeas y desarrollos actuales en América Latina, así como esfuerzos internacionales que apoyan la estandarización y la interoperabilidad de las credenciales digitales. Estas secciones proporcionaron información sobre cómo diferentes regiones están adoptando e integrando credenciales digitales para mejorar los resultados educativos y profesionales.

Aunque este informe sirve como una visión general integral, es importante tener en cuenta que no pretende ser exhaustivo. El campo en rápida evolución de las credenciales digitales está marcado por la innovación y el desarrollo continuos. Este informe tiene como objetivo proporcionar una comprensión fundamental y una instantánea del estado actual de las credenciales digitales, reconociendo que los futuros avances seguirán moldeando este paisaje dinámico.

● Referencias

- 100.000 Strong in the Americas (2024). *SENA (Servicio Nacional de Aprendizaje)*. Retrieved from <https://www.100kstrongamericas.org/sena/>
- 1EdTech (2024a). *Open Badges Specification Conformance and Certification Guide*. Retrieved from <https://www.imslobal.org/spec/ob/v3p0/cert/>
- 1EdTech (2024b). *About 1EdTech*. Retrieved from <https://www.1edtech.org/about/1edtech>
- 1EdTech (2024c). *CLR Standard*. Retrieved from <https://www.1edtech.org/standards/clr>
- American Association of Collegiate Registrars and Admissions Officers (AACRAO) (2022). *Alternative Credentials: Considerations, Guidance, and Best Practices. Alternative Credentials Workgroup Report*. Retrieved from <https://www.edalex.com/wp-content/uploads/2023/07/Alternative-Credentials-Considerations-Guidance-Best-Practices-2022.pdf>
- American Association of Collegiate Registrars and Admissions Officers (AACRAO) (2023). *Credential Confusion: A Call for Uniformity in Practice and Terminology*. Retrieved from <https://www.aacrao.org/research-publications/aacrao-research/credentials-confusion-a-call-for-uniformity-in-practice-and-terminology>
- Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA) (2022). *Microcredenciales. Formación inclusiva en todos los formatos y para todas las edades*. Retrieved from https://www.aneca.es/documents/20123/49576/MICROCREDENCIALES_Informe_V3.pdf/db424827-b464-d41d-ae09-717eb95e5742?t=1660907214565
- Allen, C. (2016, April 16). *The Path to Self-Sovereign Identity*. Life With Alacrity. <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/>
- Bakhtina, M., Leung, K. L., Matulevičius, R., Awad, A., & Švenda, P. (2023, August 29-September 01). *A decentralised public key infrastructure for X-Road* [Conference paper]. Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy. <https://doi.org/10.1145/3600160.3605092>
- Biometrics Research Group (2023, December 18). *UNDP lauds Guatemala's digital transformation efforts, offers recommendations*. Biometric Update. Retrieved from <https://www.biometricupdate.com/202312/undp-lauds-guatemalas-digital-transformation-efforts-offers-recommendations>
- Brands, S. (2002): *A Technical Overview of Digital Credentials*. Retrieved from <http://www.credentica.com/overview.pdf>

- Brown, M., Nic Giolla Mhichil, M., Beirne, E., & Mac Lochlainn, C. (2021). The Global Micro-credential Landscape: Charting a New Credential Ecology for Lifelong Learning. *Journal of Learning for Development*, 8(2), 228-254. doi:10.56059/jl4d.v8i2.525
- Bundesministerium für Bildung, Wissenschaft und Forschung (n.d.). *Micro-credentials. Positionspapier der österreichischen Hochschulbildung*. Retrieved from <https://www.bmbwf.gv.at/Themen/HS-Uni/Europ%C3%A4ischer-Hochschulraum/Die-Themen-des-Europ%C3%A4ischen-Hochschulraums/Microcred.html>
- Carey, K. L., & Stefaniak, J. E. (2018). An exploration of the utility of digital badging in higher education settings. *Educational Technology Research and Development*, 66(5), 1211-1229. <https://doi.org/10.1007/s11423-018-9602-1>
- Casilli, C., & Hickey, D. (2016). Transcending Conventional Credentialing and Assessment Paradigms with Information-Rich Digital Badges. *The Information Society*, 32(2), 117-129. <https://doi.org/10.1080/01972243.2016.1130500>
- Chen, G., Xu, B., Lu, M., & Chen, N. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, 5(1), 1-10. <https://doi.org/10.1186/s40561-017-0050-x>
- CompTIA (n.d.). *About us*. Retrieved from <https://www.comptia.org/about-us>
- Confederação Nacional da Indústria (n.d.). *Exporte seu produto com segurança e competitividade*. Retrieved from <https://www.portaldaindustria.com.br/cni/canais/assuntos-internacionais/o-que-fazemos/solucoes/certificado-de-origem-digital/>
- Council of the European Union (2022). *Proposal for a Council Recommendation on a European approach to micro-credentials for lifelong learning and employability*. Retrieved from <https://data.consilium.europa.eu/doc/document/ST-9237-2022-INIT/en/pdf>
- Coursera (2024). *Coursera: Degrees, Certificates, & Free Online Courses*. Retrieved from <https://www.coursera.org/>
- Credential Engine (2024). *Bringing Credential Transparency Through Technology*. Retrieved from <https://credentialengine.org/about-us/>
- Credly by Pearson (2024). *Unlock the Power of Your People*. Retrieved from <https://info.credly.com/>
- Danmarks Akkrediteringsinstitution (2021). *Nye fleksible uddannelsesveje gennem hele livet. Europæiske og danske perspektiver på micro-credentials på videregående uddannelsesniveau*. Retrieved from <https://akkr.dk/wp-content/filer/akkr/micro-credentials-publikation-web.pdf>
- Deutscher Akademischer Austauschdienst e.V. (2023). *Digital Credentials Initiatives Monitor*. Retrieved from <https://www.digital-credentials-monitor.com/>

- Deutscher Akademischer Austauschdienst e.V. (2024). *Digital Credentials Initiatives Monitor - Data Collection*. Retrieved from <https://www.daad.de/surveys/261944?lang=en>
- Digital Credentials Consortium (2018). *Building the digital credential infrastructure for the future*. Retrieved from <https://digitalcredentials.mit.edu/docs/white-paper-building-digital-credential-infrastructure-future.pdf>
- Dock Labs AG (2023). *What Are Digital Credentials?* Dock. Retrieved from <https://www.dock.io/post/what-are-digital-credentials>
- ECOCredGT (n.d.). *About ECOCredGT*. Retrieved from http://www.ecocredgt.org/?page_id=366&lang=en
- edX (2024). *Cursos en línea gratuitos de Universidad Nacional de Córdoba*. Retrieved from <https://www.edx.org/es/school/uncordobax>
- El Ioini, N., Pahl, C. (2018, October 22-26). *A Review of Distributed Ledger Technologies* [Conference paper]. On the Move to Meaningful Internet Systems, Valletta, Malta. https://doi.org/10.1007/978-3-030-02671-4_16
- European Centre for the Development of Vocational Training (CEDEFOP) (2019). *European guidelines for validating non-formal and informal learning*. Retrieved from <https://www.cedefop.europa.eu/en/publications/3093>
- European Centre for the Development of Vocational Training (CEDEFOP) (2024). *European qualifications framework (EQF)*. Retrieved from <https://www.cedefop.europa.eu/en/projects/european-qualifications-framework-eqf>
- Europass (2023). *Launch of the European Learning Model - Video*. Retrieved from <https://europass.europa.eu/en/node/2149>
- European Commission (2018). *European Qualifications Framework: a common reference framework*. Retrieved from <https://europass.europa.eu/en/europass-digital-tools/european-qualifications-framework>
- European Commission (2020a). *Final report: A European approach to micro-credentials. Output of the Microcredentials Higher Education Consultation Group*. Retrieved from <https://ec.europa.eu/education/sites/default/files/document-library-docs/european-approach-microcredentials-higher-education-consultation-group-output-final-report.pdf>
- European Commission (2020b). *Digital Education Action Plan 2021-2027*. Retrieved from <https://education.ec.europa.eu/focus-topics/digital-education/action-plan>
- European Commission (2023). *Europass: Improve your Career and Learning Opportunities*. Retrieved from <https://europa.eu/europass/en/about-europass>
- European Commission (2024). *eIDAS Regulation*. Retrieved from <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>

- European Commission (n.d.-a). *European Credit Transfer and Accumulation System (ECTS)*. Retrieved from <https://education.ec.europa.eu/education-levels/higher-education/inclusive-and-connected-higher-education/european-credit-transfer-and-accumulation-system>
- European Commission (n.d.-b). *Experience cross-border services with EBSI*. Retrieved from <https://ec.europa.eu/digital-building-blocks/sites/display/EBSI>
- European Union (n.d.). *European Digital Credentials for learning*. Retrieved from <https://europass.europa.eu/en/europass-tools/european-digital-credentials>
- European Union. (2004). Decision No 2241/2004/EC of the European Parliament and of the Council of 15 December 2004 on a single framework for the transparency of qualifications and competences (Europass). *Official Journal of the European Union*. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D2241>
- European Union Agency for Cybersecurity (n.d.). *Public Key Infrastructure (PKI)*. Retrieved from <https://www.enisa.europa.eu/topics/incident-response/glossary/public-key-infrastructure-pki>
- Eur-Lex (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- Flintberg, B. (2022). *Digital micro-credentials for upskilling and reskilling in the vocational sector. A study on the potential use of a blockchain-based ICT system for micro-credentials in Sweden* [Degree Project, Linnaeus University]. Retrieved from <https://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-115173>
- Foshay, W. R., & Hale, J. (2017). Application of principles of performance-based assessment to corporate certifications. *TechTrends*, 61(1), 71-76. <https://doi.org/10.1007/s11528-016-0125-5>
- FutureLearn (2012). *What could you achieve with FutureLearn?* Retrieved from <https://www.futurelearn.com/business>
- Gibson, D., Ostashewski, N., Flintoff, K., Grant, S., & Knight, E. (2015). Digital badges in education. *Education and Information Technologies*, 20(2), 403-410. <https://doi.org/10.1007/s10639-013-9291-7>
- Goldreich, O., Micali, S., & Wigderson, A. (1986). Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. *27th Annual Symposium on Foundations of Computer Science*, 174-187. doi: 10.1109/SFCS.1986.47
- González, C., Rodríguez, M., & Chamoso, P. (2018). Multi-Factor Authentication for Enhanced Security in Digital Credential Storage. *Journal of Information Security and Applications*, 42, 94-106. doi:10.3390/cryptography2010001

- Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., & Wendland, F. (2018). *Blockchain for Education: Lifelong Learning Passport* [Conference paper]. Proceedings of 1st ERCIM Blockchain Workshop 2018, Amsterdam, Netherlands. doi: 10.18420/blockchain2018_07
- Grech, A., & Camilleri, A. F. (2017). Blockchain in education. *Joint Research Centre of the European Commission*. doi:10.2760/60649. Retrieved from <https://publications.jrc.ec.europa.eu/repository/handle/JRC108255>
- Groningen Declaration (n.d.). *The Groningen Declaration Network*. Retrieved from <https://groningendeclaration.org/the-groningen-declaration-network/>
- Hyland (2024). *Hyland: Empowering innovators every day*. Retrieved from <https://www.hyland.com/en/company>
- IBM (n.d.). *IBM Innovation Center for Education (ICE)*. Retrieved from <https://www.ibm.com/support/pages/ice-digitalbadges>
- Inter-American Development Bank (IDB) (n.d.). *We are the IDB*. Retrieved from <https://www.iadb.org/en/who-we-are/about-idb>
- Kato, S., V. Galán-Muros & T. Weko (2020). The emergence of alternative credentials. *OECD Education Working Papers*, No. 216. <https://doi.org/10.1787/b741f39e-en>
- Katz, J., & Lindell, Y. (2007). *Introduction to Modern Cryptography: Principles and Protocols*. Chapman and Hall/CRC Press. <https://doi.org/10.1201/9781420010756>
- Keevy, J. and Chakroun, B. (2015). *Level-Setting and Recognition of Learning Outcomes: The Use of Level Descriptors in the Twenty-First Century*. Retrieved from <https://doi.org/10.54675/GKWN6283>
- Khalil, M., & Ebner, M. (2015). *Learning Analytics: Principles and Constraints*. [Conference paper]. Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunications, Chesapeake, Virginia. doi:10.13140/RG.2.1.1733.2083
- Lemoine, P. A. and Richardson, M. D. (2015). Micro-credentials, nano degrees, and digital badges: new credentials for global higher education. *International Journal of Technology and Educational Marketing*, 5(1), 36–49. doi: 10.4018/ijtem.2015010104
- LinkedIn Learning (2024). *A learning experience built for skill builders*. Retrieved from <https://learning.linkedin.com/>
- Mah, D. (2016). Learning analytics and digital badges: potential impact on student retention in higher education. *Technology, Knowledge and Learning*, 21(3), 285–305. <https://doi.org/10.1007/s10758-016-9286-8>

- McDaniel, R., & Fanfarelli, J. (2016). Building Better Digital Badges: Pairing Completion Logic With Psychological Factor. *Simulation and Gaming*, 47(1), 73–102. doi: 10.1177/1046878115627138
- Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press. <https://doi.org/10.1201/9780429466335>
- Microsoft Security (2024). *Microsoft Entra Verified ID - Trustworthy interactions for a digital world*. Retrieved from <https://www.microsoft.com/de-de/security/business/identity-access/microsoft-entra-verified-id>
- MIT Media Lab. (2016). *Blockcerts: Open Standard for Blockchain Certificates*. Retrieved from <https://www.media.mit.edu/projects/blockcerts>
- MIT Open Learning (2024). *Digital Credentials Consortium*. Retrieved from <https://digitalcredentials.mit.edu/our-work>
- Mühle, A., Assaf, K., Köhler, D., & Meinel, C. (2023). *Requirements of a Digital Education Credential System* [Conference paper]. IEEE Global Engineering Education Conference (EDUCON), Kuwait. doi: 10.1109/EDUCON54358.2023.10125183
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <http://dx.doi.org/10.2139/ssrn.3440802>
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press. [https://doi.org/10.1016/S1353-4858\(16\)30074-5](https://doi.org/10.1016/S1353-4858(16)30074-5)
- New Zealand Qualifications Authority (2019). *Guidelines for applying for approval of a training scheme or a micro-credential*. Retrieved from <https://www2.nzqa.govt.nz/assets/Tertiary/Approval-accreditation-and-registration/Guidelines/Guidelines-for-programme-approval-and-accreditation-L1-7-2023.pdf>
- OneTrust (2024). *Guatemala - Data Protection Overview*. Retrieved from <https://www.dataguidance.com/notes/guatemala-data-protection-overview>
- Oxford University Press (2024). *Credentials*. Oxford Learners Dictionaries. Retrieved from https://www.oxfordlearnersdictionaries.com/definition/american_english/credentials
- Pahuja, N. (2023). *Micro-Credentials: Future of Modern Skilling*. Retrieved from <https://www.ilo.org/resource/presentation-neena-pahuja-micro-credentials-future-modern-skilling>
- Pickard, L. (2018). *Analysis of 450 MOOC-Based Microcredentials Reveals Many Options But Little Consistency*. Retrieved from <https://www.classcentral.com/report/moocs-microcredentials-analysis-2018/>

- Pontificia Universidad Católica del Perú (2024a). *Oferta académica*. Retrieved from <https://educacioncontinua.pucp.edu.pe/oferta-academica/>
- Pontificia Universidad Católica del Perú (2024b). *Para organizaciones*. Retrieved from <https://educacioncontinua.pucp.edu.pe/programas-a-medida/>
- Porto, S. & Presant, D. (2023). *The IDB Digital Credential Framework: Principles and Guidelines for Creating and Issuing Credentials*. Retrieved from <https://publications.iadb.org/en/publications/english/viewer/The-IDB-Digital-Credential-Framework-Principles-and-Guidelines-for-Creating-and-Issuing-Credentials.pdf>
- Preukschat, A., & Reed, D. (2021). *Self-Sovereign Identity: Decentralized digital identity and verifiable credentials*. Manning Publications. ISBN: 9781617296598
- Quality and Qualifications Ireland (2021). *QQI early exploration into Micro-credentials in Higher Education, 2014–2020*. Retrieved from <https://www.qqi.ie/sites/default/files/2021-10/early-exploration-into-micro-credentials-in-higher-education-2014-20.pdf>
- Quigley, J. (2023). *What Are Digital Credentials and How Are They Used?* Accredible. Retrieved from <https://www.accredible.com/blog/what-are-digital-credentials>
- Reynolds, L., & Winks, J. (2021). Data Protection Techniques: A Cryptography Approach. *Journal of Technology and Systems*, 3(1), 14–21. doi: 10.47941/jts.533
- Sedlmeir, J., Smethurst, R. & Rieger, A. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*, 63, 603–613. <https://doi.org/10.1007/s12599-021-00722-y>
- Sertifier (July 24, 2023). *What is the difference between a digital certificate and digital badge?* LinkedIn. <https://www.linkedin.com/pulse/what-difference-between-digital-certificate-badge-sertifierco-1f/>
- Sharples, M., & Domingue, J. (2016). *The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward* [Conference paper]. Proceedings of the 11th European Conference on Technology Enhanced Learning (EC-TEL), Lyon, France. https://doi.org/10.1007/978-3-319-45153-4_48
- Shi, J., Zeng, X., & Han, R. (2022). A Blockchain-Based Decentralized Public Key Infrastructure for Information-Centric Networks. *Information*, 13(5), 264. <https://doi.org/10.3390/info13050264>
- Shoemaker, P. (2022). *Verifiable Credentials: The Future of Digital Identity*. Identity. Retrieved from <https://www.identity.com/what-are-verifiable-credentials/#:~:text=Verifiable%20Credentials%20%28VCs%29%20are%20digital%20credentials%20that%20use,versions%20of%20passports%2C%20driver%20licenses%2C%20and%20other%20credentials>

- Stefaniak, J., & Carey, K. (2019). Instilling purpose and value in the implementation of digital badges in higher education. *International Journal of Educational Technology in Higher Education*, 16(1), 1–21. <https://doi.org/10.1186/s41239-019-0175-9>
- SURFnet (2016). *Whitepaper on Open Badges and Micro-credentials*. Retrieved from <https://www.surf.nl/en/white-paper-on-open-badges-and-micro-credentials>
- Tecnológico de Monterrey (2023). *Tec de Monterrey launches digital credentials to certify skills*. Retrieved from <https://conecta.tec.mx/en/news/national/education/tec-de-monterrey-launches-digital-credentials-certify-skills>
- Udacity (2011). *About us*. Retrieved from <https://www.udacity.com/about-us>
- UNESCO (2018). *Digital Credentialing Implications for the recognition of learning across borders*. Retrieved from <https://oer4nosp.col.org/id/eprint/16/1/264428eng.pdf>
- UNESCO (2022). *Towards a common definition of micro-credentials*. Retrieved from <https://unesdoc.unesco.org/ark:/48223/pf0000381668#:~:text=Micro-credentials%20are%20often%20promoted%20as%20an%20efficient%20way,standards%20and%20is%20awarded%20by%20a%20trusted%20provider.>
- United Nations (2022). *The Sustainable Development Goals Report 2022*. Retrieved from <https://unstats.un.org/sdgs/report/2022/The-Sustainable-Development-Goals-Report-2022.pdf>
- Universidad de Chile (n.d.). *Information about the revalidation and recognition processes at the University of Chile*. Retrieved from <https://uchile.cl/english-version/international-relations/information-about-the-revalidation-and-recognition-processes>
- van der Hijden, P., & Martin, M. (2023). *Short courses, micro-credentials, and flexible learning pathways: A blueprint for policy development and action*. Paris: UNESCO, International Institute for Educational Planning. Retrieved from <https://www.iiep.unesco.org/en/publication/short-courses-micro-credentials-and-flexible-learning-pathways-blueprint-policy>
- West, R.E. (2023). *Flexible Open Credentials: How Micro and Nanocredentials Can Revolutionize Higher Education*. Working Paper. Center for Growth and Opportunity at Utah State University. Retrieved from <https://www.thecgo.org/research/flexible-open-credentials-how-micro-and-nanocredentials-can-revolutionize-higher-education/>
- Wolz, E., Gottlieb, M. & Pongratz, H. (2021). Digital Credentials in Higher Education Institutions: A Literature Review. *Wirtschaftsinformatik 2021 Proceedings*, 5. Retrieved from <https://aisel.aisnet.org/wi2021/KDigitalEducation15/Track15/5>
- World Wide Web Consortium (2022a). *Decentralized Identifiers (DIDs) v1.0*. Retrieved from <https://www.w3.org/TR/did-core/>

- World Wide Web Consortium (2022b). *Verifiable Credentials Data Model 1.0*. Retrieved from <https://www.w3.org/TR/vc-data-model>
- World Wide Web Consortium (2024a). *About us*. Retrieved from <https://www.w3.org/about/>
- World Wide Web Consortium. (2024b). *Verifiable Credentials Data Model v2.0*. Retrieved from <https://www.w3.org/TR/vc-data-model-2.0/>
- Yli-Huomo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PloS One*, 11(10), e0163477. <https://doi.org/10.1371/journal.pone.0163477>
- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *An overview of blockchain technology: Architecture, consensus, and future trends* [Conference paper]. IEEE International Congress on Big Data, Honolulu, USA. doi: 10.1109/BigDataCongress.2017.85