



REVISIÓN

Tecnologías de identidad digital aplicadas a la autenticación segura en ecosistemas descentralizados

Digital identity technologies applied to secure authentication in decentralized ecosystems

Manuel Cobeñas Chanduvi^{1*} · Eberth Tejada Gutierrez²

¹Facultad de Ingeniería, Universidad Tecnológica del Perú, Piura, 20001, Perú

²Facultad de Ingeniería, Universidad de Ingeniería y Tecnología, Lima, 15063, Perú

*Autor de Correspondencia: c27213@utp.edu.pe

Enviado: 29 Mayo 2026 Aceptado: 13 Julio 2026 Publicado en línea: 15 Julio 2026

Resumen

Garantizar la autenticación segura de usuarios en ecosistemas descentralizados constituye uno de los retos más complejos de la identidad digital, dado que las tecnologías actuales no ofrecen garantías suficientes de privacidad ni soberanía individual. Con el objetivo de atender este vacío, este trabajo realiza una revisión sistemática de la literatura guiada por cuatro preguntas de investigación enmarcadas en las tecnologías de identidad digital, enfoques metodológicos, dominios de aplicación y marcos normativos. Se analizaron 835 publicaciones científicas del período 2022-2026, de las cuales 23 conformaron el corpus definitivo. El análisis revela que la tecnología de cadena de bloques constituye el sustrato tecnológico predominante en el 91 % de las soluciones identificadas, mientras que el paradigma de identidad autosoberana representa el enfoque arquitectónico dominante en el 52 % de los estudios. En particular, los identificadores descentralizados, las credenciales verificables y las pruebas de conocimiento cero se consolidan como arquitectura canónica para la autenticación privada. Asimismo, los dominios vinculados al internet de las cosas, la salud digital y los servicios financieros evidencian la mayor densidad de implementaciones documentadas. Sin embargo, los retos que deja este análisis se concentran en la protección de datos y el reglamento de identidad digital, en la preparación criptográfica frente a amenazas de computación cuántica, y en la validación con usuarios en entornos reales.

Palabras clave: cadena de bloques, identidad autosoberana, identificadores descentralizados, autenticación segura, credenciales verificables

Abstract

Ensuring secure user authentication in decentralized ecosystems constitutes one of the most complex challenges of digital identity, given that current technologies do not offer sufficient guarantees of privacy or individual sovereignty. With the aim of addressing this gap, this work carries out a systematic literature review guided by four research questions framed around digital identity technologies, methodological approaches, application domains, and regulatory frameworks. A total of 835 scientific publications from the 2022-2026 period were analyzed, of which 23 formed the final corpus. The analysis reveals that blockchain technology constitutes the predominant technological substrate in 91 % of the identified solutions, while the self-sovereign identity paradigm represents the dominant architectural approach in 52 % of the studies. In particular, decentralized identifiers, verifiable credentials, and zero-knowledge proofs are consolidated as the canonical architecture for private authentication. Likewise, the domains linked to the internet of things, digital health, and financial services show the highest density of documented implementations. However, the challenges left by this analysis are concentrated in data protection and digital identity regulation, in cryptographic preparedness against quantum computing threats, and in validation with users in real-world environments.

Keywords: blockchain, self-sovereign identity, decentralized identifiers, secure authentication, verifiable credentials

Este es un artículo de acceso abierto y se distribuye bajo los términos de la Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

Citar como: M. Cobeñas Chanduvi y E. Tejada Gutierrez, "Tecnologías de identidad digital aplicadas a la autenticación segura en ecosistemas descentralizados," *CISAI*, vol. 2, no. 2, pp. 82–98, Julio 2026, doi: 10.64439/cisai.v2i2.47.

1. Introducción

La creciente digitalización de los servicios públicos, financieros y sanitarios ha colocado a la identidad digital en el centro de los sistemas de confianza contemporáneos. Gestionar de forma segura quién es quién en el entorno digital ya no es una cuestión exclusivamente técnica, sino una condición habilitante para el ejercicio de derechos, el acceso a recursos y la participación en la economía digital [1]. En este escenario, la gestión de la identidad ha recaído históricamente sobre arquitecturas centralizadas en las que terceros, ya sean empresas tecnológicas, entidades financieras o administraciones públicas, custodian las credenciales de los usuarios y deciden cuándo y cómo pueden ser verificadas. Este modelo, aunque funcional en entornos controlados, ha mostrado límites profundos conforme los ecosistemas digitales se han vuelto más abiertos, distribuidos e interoperables. Prueba de ello es que más de diez mil millones de registros han sido comprometidos en brechas de seguridad asociadas a repositorios centralizados [2], y más de mil millones de personas permanecen excluidas de cualquier forma de identidad digital reconocida [3]. Cuando un ciudadano intenta acreditar su identidad ante una administración extranjera y descubre que sus credenciales no son válidas fuera de su país de origen, o cuando un usuario pierde el acceso a sus datos porque la plataforma que los custodiaba ha sido vulnerada, lo que está en juego no es solo la comodidad digital, sino la posibilidad misma de participar en la vida social y económica contemporánea.

Ante estas limitaciones, el paradigma de identidad autosoberana ha emergido como una propuesta de reordenamiento del campo, cuya premisa central es que los individuos deben poder gestionar sus propias credenciales sin depender de intermediarios. Este enfoque, conocido como SSI (*self-sovereign identity*), se apoya en estándares como los identificadores descentralizados (DID) y las credenciales verificables (VC), habitualmente soportados por cadenas de bloques o registros distribuidos (DLT) y complementados con pruebas de conocimiento cero (ZKP), cuya adopción se ha extendido desde entornos de usuario hasta dispositivos del internet de las cosas, aplicaciones de salud y plataformas financieras [1]. Ahora bien, la producción científica en torno a este paradigma, aunque creciente, avanza sin una visión de conjunto que permita orientar su desarrollo. En el plano tecnológico, las soluciones evolucionan con rapidez, pero sin que exista una síntesis actualizada sobre cuáles predominan y cómo se han adoptado en ecosistemas realmente descentralizados [4]. En el plano metodológico, la mayor parte de las propuestas se validan en condiciones de laboratorio, con escasa presencia de estudios que acrediten su funcionamiento con usuarios reales [5]. En cuanto a los dominios de aplicación, la investigación tiende a concentrarse en unos pocos sectores, dejando sin atender áreas con alto potencial de impacto social. Más aún, los marcos normativos de referencia, como el Reglamento General de Protección de Datos (RGPD) o la cartera de identidad digital de la Unión Europea prevista en el reglamento eIDAS 2.0, avanzan sin que los sistemas técnicos hayan alcanzado el nivel de alineación regulatoria que estos exigen [6, 7]. Considerados en conjunto, estos vacíos señalan la ausencia de una revisión sistemática que articule el estado del campo y oriente su desarrollo con base empírica sólida.

El presente trabajo asume esa tarea. Mediante una revisión sistemática de la literatura que analizó 835 publicaciones del período 2022–2026 indexadas en Scopus, se ofrece una síntesis integradora organizada en torno a cuatro preguntas de investigación que corresponden, respectivamente, a la dimensión tecnológica, metodológica, aplicada y normativa del campo.

- **PI1.** ¿Qué tecnologías de identidad digital predominan en ecosistemas descentralizados y cómo ha evolucionado su adopción entre 2022 y 2026?
- **PI2.** ¿Qué enfoques metodológicos caracterizan la investigación en este campo y qué vacíos persisten en la validación con usuarios reales?
- **PI3.** ¿En qué dominios de aplicación se concentra la investigación y cuáles presentan mayores brechas respecto a su impacto social potencial?
- **PI4.** ¿En qué medida los marcos normativos vigentes han permeado el diseño de los sistemas de identidad descentralizada y qué brechas persisten entre regulación e implementación?

El resto del artículo se organiza del siguiente modo: la Sección 2 describe el protocolo metodológico empleado, la Sección 3 presenta los resultados organizados en torno a las cuatro preguntas de investigación,

la Sección 4 discute los hallazgos en relación con el estado del arte, y la Sección 5 sintetiza las conclusiones, contribuciones e implicaciones para la investigación futura.

2. Metodología

La metodología se estructuró como una revisión sistemática orientada a identificar, seleccionar y caracterizar la producción científica reciente sobre identidad digital descentralizada y sus principales mecanismos tecnológicos. Para asegurar la trazabilidad del proceso, el procedimiento se organizó de manera secuencial desde la búsqueda bibliográfica hasta la conformación del corpus definitivo, articulando la estrategia de búsqueda, los criterios de inclusión y exclusión, el proceso de selección basado en PRISMA y la caracterización tipológica de los estudios. Esta organización permitió comprender no solo cómo se obtuvieron los documentos analizados, sino también de qué manera se delimitó su pertinencia temática, temporal y metodológica antes de desarrollar los análisis presentados en la Sección 3.

2.1 Estrategia de búsqueda

La búsqueda bibliográfica constituyó el punto de partida para delimitar un conjunto documental suficientemente amplio y reproducible. Se utilizó Scopus como fuente primaria debido a su cobertura multidisciplinaria y a la posibilidad de ejecutar consultas estructuradas sobre los campos de título, resumen y palabras clave. La búsqueda se realizó el 5 de mayo de 2026 y consideró publicaciones comprendidas entre enero de 2022 y abril de 2026, período seleccionado para representar la producción científica más reciente asociada con la maduración de los estándares W3C DID/VC [1] y con la consolidación del debate europeo sobre identidad digital y eIDAS 2.0 [6]. La consulta empleada fue la siguiente:

```
("digital identity" OR "decentralized identity" OR "self-sovereign identity" OR "SSI")
AND ("authentication" OR "blockchain" OR "DID" OR "verifiable credentials" OR
"decentralized identifiers")
```

La aplicación de esta estrategia produjo inicialmente 835 registros, los cuales fueron exportados en formato BibTeX e incorporados a una matriz de análisis para facilitar su organización y posterior depuración. No se establecieron restricciones geográficas, aunque se conservaron únicamente publicaciones en inglés debido a la configuración adoptada para la revisión. A partir de los metadatos recuperados, los documentos fueron identificados mediante vocabulario controlado relacionado con cadena de bloques, autenticación, identidad descentralizada, identidad autosoberana, gestión de identidad, identidad digital y privacidad de datos. Sobre esta base, la lógica empleada para delimitar el universo documental puede entenderse como la intersección de tres condiciones complementarias, tal como se representa en la Figura 1. La primera corresponde a la pertinencia temática respecto de la identidad digital descentralizada, la segunda a la presencia de mecanismos tecnológicos de autenticación o gestión de identidad y la tercera a las condiciones metodológicas y temporales definidas para la revisión. De este modo, el corpus no se construyó únicamente a partir de coincidencias terminológicas, sino mediante la convergencia entre relevancia temática, soporte tecnológico y pertinencia documental.

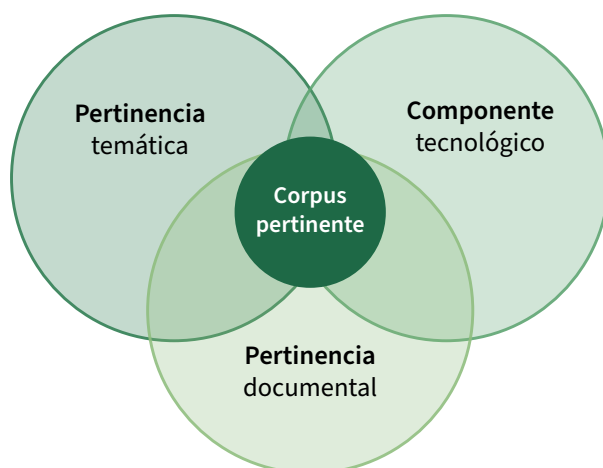


Figura 1. Convergencia de criterios para la delimitación conceptual del corpus

Esta representación permitió distinguir la recuperación bibliográfica inicial de la selección analítica posterior, ya que la presencia de términos relacionados con identidad digital no garantizó por sí sola la incorporación de un documento. De igual manera, fue necesario comprobar simultáneamente su relación con tecnologías de identidad y el cumplimiento de las condiciones documentales definidas para el estudio, proceso que se formalizó mediante los criterios descritos a continuación.

2.2 Criterios de inclusión y exclusión

Los criterios de selección se establecieron antes de la depuración definitiva con el propósito de mantener una aplicación uniforme sobre los registros recuperados. Para ello se consideraron cinco dimensiones relacionadas con la temática, el período de publicación, el idioma, el tipo de fuente y la disponibilidad de contenido suficiente para efectuar el análisis. Como se sintetiza en la Tabla 1, esta matriz permitió diferenciar los documentos directamente vinculados con identidad digital descentralizada de aquellos en los que la cadena de bloques aparecía exclusivamente asociada con aplicaciones financieras, trazabilidad u otros usos sin un componente explícito de gestión de identidad.

Tabla 1. Criterios de inclusión y exclusión aplicados al corpus documental

Dimensión	Inclusión	Exclusión
Temática	Estudios sobre identidad digital, identidad autosoberana, identificadores descentralizados, credenciales verificables o autenticación descentralizada	Estudios de cadena de bloques sin componente de identidad o destinados exclusivamente a aplicaciones financieras
Período	Publicaciones comprendidas entre enero de 2022 y abril de 2026	Publicaciones anteriores a enero de 2022
Idioma	Publicaciones en inglés	Publicaciones en otros idiomas
Tipo de fuente	Artículos científicos, trabajos publicados en actas académicas indexadas y capítulos de libros sometidos a revisión	Literatura gris e informes técnicos sin revisión académica
Contenido	Registro con resumen suficiente para determinar pertinencia temática y realizar el análisis	Registro sin resumen o con información insuficiente para establecer su pertinencia

La aplicación conjunta de estos criterios permitió pasar de una recuperación basada fundamentalmente en términos de búsqueda a una selección sustentada en pertinencia documental. Por tanto, esta distinción resulta relevante porque evita considerar como evidencia central aquellos estudios que utilizan tecnologías similares pero persiguen objetivos diferentes a la gestión descentralizada de identidad. Sobre esta base se desarrolló el proceso de depuración que condujo desde los 835 registros iniciales hasta los 23 estudios incorporados al corpus definitivo que se explica en la próxima subsección.

2.3 Proceso de selección de los estudios

El proceso de selección siguió las fases de identificación, cribado, elegibilidad e inclusión contempladas en PRISMA. La Figura 2 sintetiza el recorrido seguido por los registros y permite observar tanto la reducción progresiva del universo documental como las principales causas de exclusión. Durante la identificación se recuperaron 835 registros publicados entre 2022 y 2026. En el cribado se examinaron sus títulos y palabras clave, lo que permitió excluir 53 documentos relacionados con trazabilidad de activos físicos sin componente de identidad y 18 publicaciones en idiomas distintos al inglés. Como resultado, 764 documentos avanzaron a la evaluación de elegibilidad.

Posteriormente, se siguió con la lectura de los resúmenes, lo que permitió realizar una depuración más específica del contenido. En esta fase se excluyeron 741 registros, de los cuales 317 abordaban exclusivamente protocolos de consenso de cadena de bloques sin relación directa con la gestión de identidad, 166 presentaban un alcance periférico o se encontraban fuera del período efectivo de análisis, 130 no aportaban evidencia técnica o empírica suficiente y 128 carecían de un resumen sustantivo que permitiera determinar

su pertinencia. Una vez completado este procedimiento quedaron 23 estudios, que constituyeron el corpus definitivo sobre el cual se efectuó la caracterización y el análisis posterior.

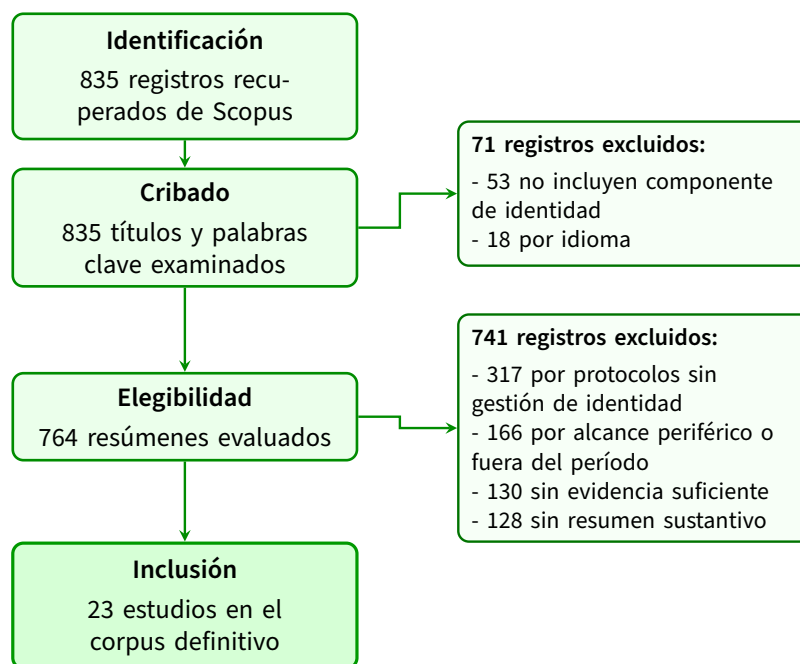


Figura 2. Proceso de identificación, depuración y selección del corpus documental

2.4 Caracterización tipológica del corpus

Una vez establecido el corpus definitivo, los estudios fueron organizados mediante tres dimensiones analíticas destinadas a proporcionar una estructura común para su posterior examen. La primera corresponde al enfoque metodológico y permite distinguir entre propuestas conceptuales, implementaciones, análisis de seguridad, revisiones y evaluaciones empíricas, mientras que la segunda identifica el dominio principal en el que se aplica la identidad digital descentralizada y la tercera reconoce las tecnologías que sustentan las soluciones estudiadas. De esta manera, la clasificación no pretende establecer todavía la predominancia de unas categorías sobre otras, sino ordenar un corpus mediante criterios comparables que faciliten la identificación posterior de tendencias y vacíos. En este sentido, la Tabla 2 sintetiza la estructura de clasificación utilizada y vincula cada categoría con estudios representativos que permiten conservar su trazabilidad respecto de la literatura examinada.

Por otro lado, la organización presentada en la Tabla 2 muestra que la caracterización fue concebida para observar el corpus desde perspectivas complementarias. En efecto, el enfoque metodológico permite diferenciar estudios orientados al diseño de marcos y arquitecturas de aquellos que avanzan hacia implementaciones, análisis de seguridad, revisiones o evaluaciones en escenarios reales. A su vez, el dominio de aplicación sitúa estas contribuciones en contextos como Internet de las cosas, salud, finanzas, movilidad, gobierno y educación, lo que permite examinar posteriormente si los desafíos de identidad descentralizada adquieren características diferentes según el entorno en el que se implementan.

En este contexto, la dimensión tecnológica completa esta estructura al identificar los componentes sobre los cuales se construyen las soluciones analizadas, entre ellos la cadena de bloques, la identidad autosoberana, los identificadores descentralizados, las credenciales verificables, las pruebas de conocimiento cero, la biometría, la inteligencia artificial y la criptografía poscuántica. Por tanto, las dimensiones fueron consideradas de manera complementaria, ya que un estudio puede combinar diferentes tecnologías y aproximaciones metodológicas aun cuando se encuentre asociado con un dominio principal de aplicación. De esta manera, la caracterización no constituye un resultado aislado, sino una organización que conecta el procedimiento de selección con el análisis desarrollado en la Sección 3, donde estas categorías permiten examinar tendencias, relaciones tecnológicas y áreas con menor desarrollo dentro de la literatura.

Tabla 2. Caracterización tipológica del corpus de análisis

Dimensión	Categoría identificada	Estudio representativo
Enfoque metodológico	Propuesta de marco o arquitectura	Samir et al. [8]
	Implementación y prototipo experimental	Fathalla et al. [9]
	Análisis formal de seguridad	Pöhn et al. [10]
	Revisión sistemática	Rathee et al. [11]
	Caso de estudio con despliegue real	Tertulino et al. [12]
	Evaluación empírica con usuarios	Fry y Hileman [13]
Dominio de aplicación	Internet de las cosas	Xiong et al. [14]
	Salud	Bai et al. [15]
	Finanzas e identificación de clientes	Ahmed et al. [16]
	Vehículos y movilidad conectada	An et al. [17]
	Metaverso y entornos descentralizados	Arshad et al. [2]
	Gobierno e identidad electrónica	Hsieh et al. [18]
	Educación y certificación académica	Smith y Dion-Schwarz [19]
	Redes móviles de nueva generación	Zhang et al. [20]
	Otros dominios	Pava et al. [21]
Tecnología central	Cadena de bloques y registros distribuidos	Ahmed et al. [3]
	Identidad autosoberana	Cucko et al. [22]
	Identificadores descentralizados	Mazzocca et al. [1]
	Pruebas de conocimiento cero	Sassi et al. [23]
	Credenciales verificables	Mazzocca et al. [1]
	Inteligencia artificial y aprendizaje automático	Emati et al. [24]
	Biometría	Naik et al. [25]
	Criptografía poscuántica	Lee et al. [26]

3. Resultados

En este apartado se presentan los resultados obtenidos a partir del análisis de los 23 estudios que conformaron el corpus definitivo, organizados en cuatro dimensiones relacionadas con la arquitectura tecnológica, el perfil metodológico, los dominios de aplicación y las condiciones regulatorias y de gobernanza, cuya integración permitió examinar la evidencia más allá de la descripción individual de las tecnologías e identificar patrones, relaciones y brechas que condicionan su implementación, aspectos que se desarrollan en las siguientes subsecciones de acuerdo con los hallazgos identificados en cada dimensión.

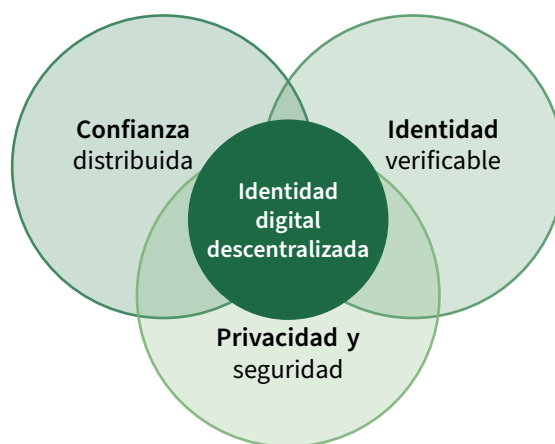
3.1 Arquitectura tecnológica y evolución de las soluciones

Desde la perspectiva tecnológica, los estudios muestran una evolución desde arquitecturas centradas principalmente en registros distribuidos hacia configuraciones que incorporan mecanismos especializados de identificación, credenciales y protección de la privacidad. En este caso, Ahmed et al. [3] explican a la cadena de bloques como infraestructura para establecer confianza distribuida, mientras que Cucko et al. [22] amplían esta perspectiva mediante la identidad autosoberana y Mazzocca et al. [1] destacan la función de los identificadores descentralizados y las credenciales verificables. A esta estructura se incorporan las pruebas de conocimiento cero estudiadas por Sassi et al. [23], junto con mecanismos biométricos [25], inteligencia artificial [24] y aproximaciones de criptografía poscuántica [26]. En términos de frecuencia, 21 de los 23 estudios del corpus (91 %) emplean la cadena de bloques o algún registro distribuido como sustrato de confianza, mientras que 12 de ellos (52 %) adoptan explícitamente el paradigma de identidad autosoberana como enfoque arquitectónico, valores que corresponden a los reportados en el resumen. La Tabla 3 sintetiza estos componentes de acuerdo con la función que desempeñan dentro de los sistemas analizados.

Tabla 3. Tecnologías identificadas y función dentro de la identidad digital descentralizada

Tecnología	Función identificada	Estudio representativo
Cadena de bloques y registros distribuidos	Establecimiento de confianza distribuida y registro verificable	Ahmed et al. [3]
Identidad autosoberana	Control de credenciales y atributos por parte del titular	Cucko et al. [22]
Identificadores descentralizados	Identificación verificable e interoperable	Mazzocca et al. [1]
Credenciales verificables	Emisión, presentación y comprobación de atributos digitales	Mazzocca et al. [1]
Pruebas de conocimiento cero	Verificación de información con divulgación limitada de atributos	Sassi et al. [23]
Inteligencia artificial	Apoyo a procesos de supervisión, detección y autenticación	Emati et al. [24]
Biometría	Fortalecimiento de los mecanismos de autenticación	Naik et al. [25]
Criptografía poscuántica	Protección frente a escenarios criptográficos futuros	Lee et al. [26]

A partir de esta organización se observa que las tecnologías no funcionan necesariamente como alternativas independientes, sino como componentes susceptibles de integrarse dentro de una misma arquitectura. Sobre esta base, Kersic et al. [27] muestran esta necesidad al señalar que las billeteras digitales requieren coordinación entre componentes registrados dentro y fuera de la cadena, mientras que Paik et al. [28] desplazan el problema desde la simple viabilidad técnica hacia la construcción de arquitecturas recuperables, auditables y gobernables. De este modo, el desarrollo tecnológico puede interpretarse como un tránsito desde una infraestructura distribuida de confianza hacia un ecosistema en el que identificación, credenciales, privacidad y autenticación necesitan operar de manera coordinada. En este contexto y para una mayor caracterización la Figura 3 ilustra conceptualmente estos aspectos, donde la identidad digital descentralizada aparece en la convergencia de tres capacidades identificadas en la literatura. De igual manera, la confianza distribuida proporciona una base para el registro y la verificación, la identidad verificable permite representar sujetos y entidades mediante identificadores y credenciales, mientras que la privacidad y la seguridad intervienen en la protección y divulgación controlada de los atributos [3, 1, 23].

**Figura 3.** Convergencia de capacidades tecnológicas en la identidad digital descentralizada

Bajo esta perspectiva, el hallazgo tecnológico no radica únicamente en identificar los componentes utilizados, sino en reconocer la formación progresiva de arquitecturas compuestas. Por tanto, la cadena de bloques proporciona una infraestructura de confianza, mientras que los identificadores descentralizados, las credenciales verificables y los mecanismos de privacidad trasladan esa infraestructura hacia procesos concretos de identificación y autenticación [1, 23]. A su vez, la incorporación de biometría, inteligencia artificial y criptografía poscuántica amplía las posibilidades de protección y supervisión [25, 24, 26], aunque también introduce nuevas exigencias relacionadas con interoperabilidad, recuperación de credenciales y gobernanza.

3.2 Perfil metodológico y validación

En correspondencia con la evolución tecnológica observada, el análisis metodológico muestra que la literatura aborda el problema mediante aproximaciones que recorren distintos niveles de desarrollo y validación, desde la formulación de arquitecturas hasta su evaluación en escenarios aplicados. En este recorrido, Samir et al. [8] se orientan al desarrollo de arquitecturas de confianza descentralizada, mientras que Fathalla et al. [9] trasladan estas propuestas hacia la implementación experimental y Pöhn et al. [10] profundizan en la evaluación de sus propiedades de seguridad. A estos enfoques se suman las revisiones sistemáticas [11], que consolidan la evidencia disponible, así como los estudios con despliegue aplicado [12] y las evaluaciones con usuarios [13], que amplían la validación hacia contextos de uso más próximos a condiciones reales. De este modo, los enfoques identificados reflejan diferentes grados de aproximación entre el diseño conceptual y la comprobación empírica de las soluciones, cuya distribución se organiza en la Tabla 4.

Tabla 4. Enfoques metodológicos identificados en el corpus

Enfoque	Aporte al análisis	Estudio representativo
Marco o arquitectura	Estructuración conceptual de componentes y relaciones	Samir et al. [8]
Prototipo experimental	Comprobación funcional en condiciones controladas	Fathalla et al. [9]
Análisis de seguridad	Identificación de amenazas y vulnerabilidades	Pöhn et al. [10]
Revisión sistemática	Integración y comparación de evidencia previa	Rathee et al. [11]
Despliegue real	Evaluación del funcionamiento en escenarios aplicados	Tertulino et al. [12]
Evaluación con usuarios	Análisis de interacción, aceptación y experiencia de uso	Fry y Hileman [13]

La lectura conjunta de estos enfoques permite distinguir entre demostrar que una arquitectura puede funcionar y comprobar que conserva su eficacia cuando se traslada a condiciones reales de utilización. En esta transición, Pöhn et al. [10] y Naik et al. [25] evidencian avances en el análisis de amenazas y superficies de ataque, mientras que Fathalla et al. [9] extienden la validación hacia la comprobación experimental de las soluciones. No obstante, a medida que estas tecnologías superan los entornos controlados, la evaluación deja de depender únicamente de su consistencia técnica y comienza a incorporar aspectos vinculados con la experiencia del usuario, la recuperación de credenciales, la gestión de errores y la inclusión digital, lo que amplía los criterios necesarios para determinar su viabilidad en escenarios reales.

Bajo esta perspectiva, los hallazgos evidencian una distancia entre la madurez técnica alcanzada y el grado de validación situada de las soluciones, puesto que disponer de mecanismos criptográficamente consistentes constituye una condición necesaria, pero no suficiente, para garantizar su adopción y funcionamiento sostenido. Por tanto, esta brecha adquiere mayor relevancia en escenarios tecnológicos más complejos, como los analizados por Xiong et al. [14], donde la identidad se extiende hacia ecosistemas con gran cantidad de dispositivos y el sujeto autenticado puede corresponder a una persona, una máquina o un componente conectado. Así, la ampliación del entorno de aplicación modifica también las exigencias de evaluación, al requerir que la escalabilidad, la recuperación, la interacción y la administración de credenciales sean consideradas de manera articulada con la seguridad.

3.3 Dominios de aplicación y exigencias de implementación

Una vez examinados los enfoques metodológicos y los niveles de validación empleados en la literatura, el análisis continúa con los escenarios donde las soluciones de identidad digital descentralizada son implementadas, con el propósito de reconocer cómo las características de cada dominio condicionan sus requerimientos tecnológicos y operativos. Desde esta perspectiva, los estudios examinados abarcan contextos como Internet de las cosas, salud, finanzas, movilidad conectada, entornos virtuales descentralizados, gobierno, educación y redes de comunicación. En el caso del Internet de las cosas, Xiong et al. [14] abordan la identidad en ecosistemas de dispositivos conectados, mientras que Bai et al. [15] trasladan su aplicación

hacia la protección de información sanitaria y Ahmed et al. [16] hacia procesos financieros de verificación de identidad. Esta diversidad se amplía con An et al. [17], quienes incorporan escenarios de movilidad conectada, y con Hsieh et al. [18] y Zhang et al. [20], cuyos trabajos permiten observar las exigencias asociadas con servicios gubernamentales y redes de nueva generación. Por tanto, esta distribución evidencia que la identidad descentralizada responde a necesidades distintas según el entorno en el que se incorpora, por lo que la Tabla 5 organiza los principales ámbitos identificados y las necesidades asociadas a cada uno.

Tabla 5. Dominios de aplicación y necesidades identificadas

Dominio	Necesidad asociada	Estudio representativo
Internet de las cosas	Autenticación de dispositivos y comunicación entre máquinas	Xiong et al. [14]
Salud	Protección de datos clínicos y verificación de identidad	Bai et al. [15]
Finanzas	Identificación de clientes y verificación regulada	Ahmed et al. [16]
Vehículos y movilidad	Identidad de componentes y entidades ciberfísicas	An et al. [17]
Entornos virtuales descentralizados	Persistencia y control de la identidad digital	Arshad et al. [2]
Gobierno e identidad electrónica	Interoperabilidad institucional y prestación de servicios digitales	Hsieh et al. [18]
Educación	Emisión y verificación de certificaciones académicas	Smith y Dion-Schwarz [19]
Redes de nueva generación	Autenticación distribuida en infraestructuras avanzadas	Zhang et al. [20]

Sobre la base de esta clasificación, la comparación entre los dominios permite observar que una misma arquitectura de identidad adquiere requerimientos diferentes cuando se traslada de un contexto a otro. En el ámbito sanitario, Guerar et al. [29] relacionan la identidad autosoberana con necesidades de privacidad, trazabilidad y prevención del fraude, mientras que en el sector financiero Ahmed et al. [16] incorporan la verificación de identidad dentro de procesos sujetos a exigencias regulatorias. Esta variación se hace aún más evidente en movilidad, donde An et al. [17] introducen una dimensión ciberfísica que extiende la confianza desde las personas hacia vehículos y componentes conectados, a diferencia del ámbito gubernamental, en el que la participación de distintas instituciones incorpora requerimientos de interoperabilidad y reconocimiento institucional [18]. De este modo, el dominio de aplicación no constituye únicamente el escenario donde se despliega la tecnología, sino un factor que determina las condiciones bajo las cuales una arquitectura puede responder adecuadamente a las necesidades de identidad.

Esta relación entre contexto y requerimientos conduce a examinar con mayor detalle las exigencias que adquieren mayor relevancia durante la implementación. En los estudios orientados a Internet de las cosas, la autenticación y la escalabilidad adquieren un papel central debido a la cantidad y diversidad de dispositivos que deben interactuar [14], mientras que en salud y finanzas la protección de información sensible y las obligaciones de verificación refuerzan la importancia de la privacidad, la trazabilidad y la autenticación [15, 16]. A medida que el escenario se desplaza hacia la movilidad, estas exigencias se combinan con la necesidad de autenticar entidades ciberfísicas y mantener la operación en entornos distribuidos [17]; en cambio, en gobierno y educación, donde una misma credencial puede requerir reconocimiento por diferentes organizaciones, la interoperabilidad adquiere mayor relevancia [18, 19]. En este contexto, las diferencias permiten establecer una relación cualitativa entre los dominios estudiados y los atributos que condicionan su implementación, sintetizada en la Figura 4.

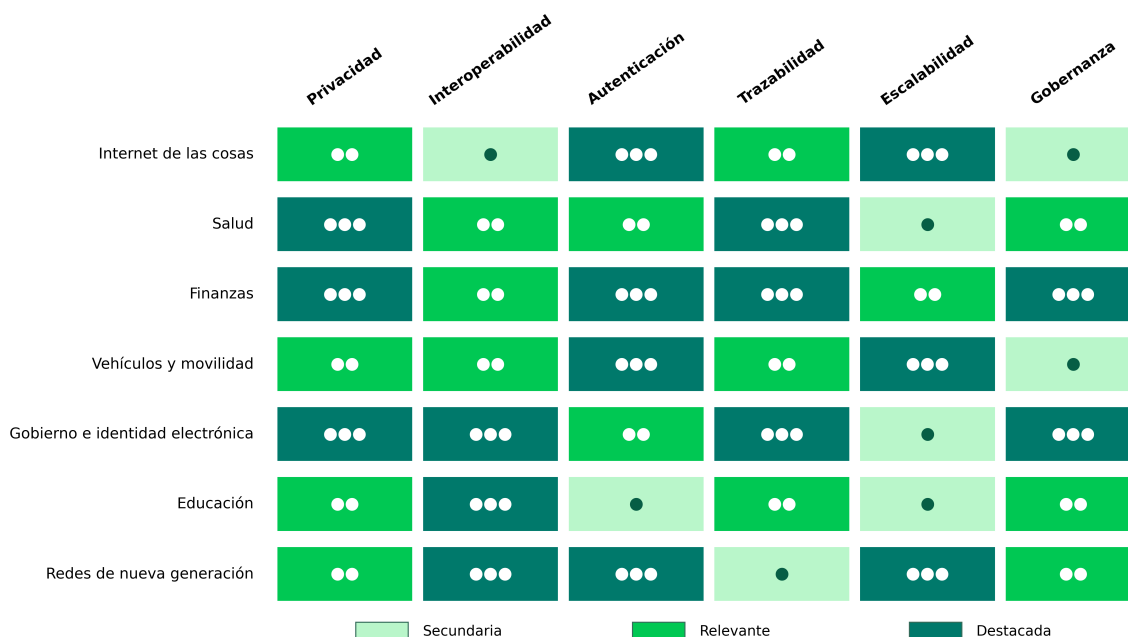


Figura 4. Matriz cualitativa de relación entre dominios de aplicación y atributos identificados

A partir de las relaciones sintetizadas en la Figura 4, se observa que las exigencias asociadas con la identidad digital descentralizada no se distribuyen de manera uniforme, sino que adquieren distinta intensidad según las características operativas e institucionales de cada dominio. Así, los contextos sanitarios y financieros requieren una articulación especialmente estrecha entre privacidad, autenticación y trazabilidad [15, 16], mientras que Internet de las cosas y movilidad incrementan la importancia de la autenticación y la escalabilidad debido a la multiplicidad de entidades que intervienen [14, 17]. Esta configuración cambia nuevamente en gobierno y educación, donde prevalece la necesidad de que las credenciales puedan ser verificadas y reconocidas por diferentes actores [18, 19]. En efecto, los resultados muestran que la arquitectura de identidad descentralizada no puede determinarse como una configuración tecnológica uniforme, sino como una estructura que debe adaptarse a las condiciones del dominio en el que será implementada, relación que conduce a examinar las condiciones regulatorias y de gobernanza que determinan su reconocimiento y funcionamiento más allá del entorno estrictamente tecnológico.

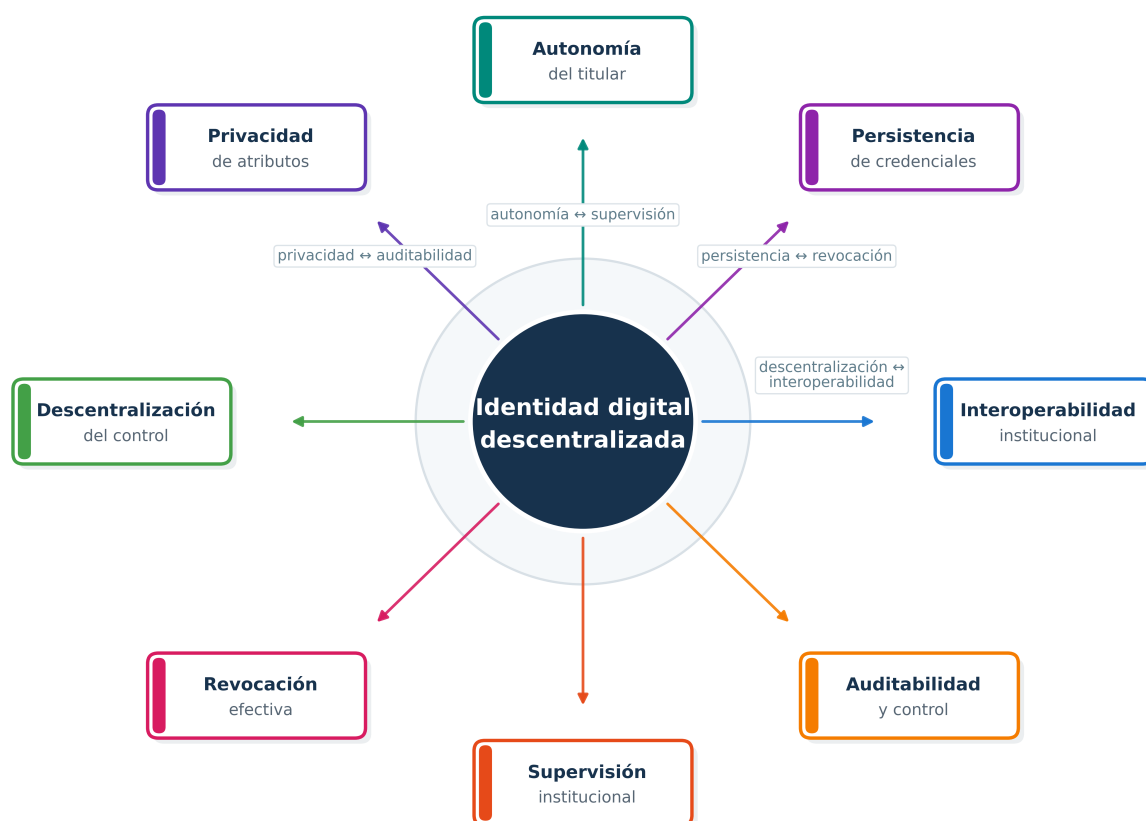
3.4 Marcos normativos y brechas de gobernanza

Tras examinar cómo los dominios de aplicación introducen requerimientos diferenciados, esta subsección desplaza el análisis hacia las condiciones normativas y de gobernanza que intervienen cuando las soluciones deben operar entre titulares, emisores, verificadores e instituciones. En este nivel, el funcionamiento de la identidad digital descentralizada incorpora cuestiones relacionadas con el consentimiento, el reconocimiento entre organizaciones, la revocación de credenciales, la supervisión y la sostenibilidad de los mecanismos de seguridad. Lindquist [6] aborda las dificultades asociadas con la interoperabilidad de los mecanismos de consentimiento, mientras que Bureaca et al. [7] proponen listas de revocación no vinculables para atestaciones electrónicas calificadas, lo que aborda la integración institucional en el contexto de eIDAS 2.0. Esta perspectiva se amplía con Lee et al. [26], quienes incorporan la revocación de credenciales y la preparación poscuántica, y con Chen et al. [30], que introducen mecanismos de supervisión en los procesos de autenticación. Por tanto, la presencia de estos componentes permite diferenciar las brechas según el momento y la función que cumplen dentro del ecosistema, desde la manifestación verificable del consentimiento hasta la conservación de condiciones de seguridad a largo plazo, tal como se organiza en la Tabla 6.

Tabla 6. Brechas regulatorias y de gobernanza identificadas

Eje	Brecha identificada	Implicación
Consentimiento	Mecanismos de consentimiento con interoperabilidad limitada [6]	Dificultad para mantener evidencia verificable del consentimiento
Interoperabilidad institucional	Integración desigual entre infraestructuras y jurisdicciones [7]	Fragmentación del reconocimiento de identidades y credenciales
Revocación	Necesidad de invalidar credenciales preservando la privacidad [26]	Riesgo de mantener credenciales inválidas dentro del ecosistema
Supervisión	Equilibrio entre anonimato, autonomía y control institucional [30]	Dificultad para establecer mecanismos aceptables de rendición de cuentas
Seguridad futura	Incorporación todavía incipiente de mecanismos poscuánticos [26]	Riesgo de obsolescencia de los mecanismos criptográficos

La relación entre las brechas de la Tabla 6 permite observar que su alcance atraviesa diferentes funciones de la identidad digital. El consentimiento requiere conservar evidencia verificable de una decisión del titular, pero esa evidencia debe poder interpretarse entre sistemas y organizaciones diferentes [6]; a su vez, el reconocimiento de una credencial depende de que emisores y verificadores compartan criterios suficientes para establecer su validez [7]. Por ello, la revocación introduce otra condición temporal, debido a que una credencial previamente válida puede perder esa condición y debe ser retirada del circuito de confianza sin exponer información adicional sobre su titular [26]. Sobre estas relaciones aparece la supervisión, que incorpora la posibilidad de verificar determinadas actuaciones sin trasladar nuevamente el control completo de la identidad hacia una autoridad central [30]. De esta manera, autonomía, privacidad, interoperabilidad y control institucional se relacionan en distintos momentos del ciclo de una credencial, relaciones que se representan en la Figura 5.

**Figura 5.** Tensiones de gobernanza asociadas con la identidad digital descentralizada

Las relaciones representadas en la Figura 5 permiten observar que los atributos de la identidad descentralizada mantienen una relación de dependencia, de modo que las decisiones adoptadas sobre uno de ellos pueden generar nuevas exigencias sobre los demás. Esta relación se aprecia en la autonomía, cuyo incremento reduce la dependencia de proveedores centralizados, aunque también exige mecanismos que permitan afrontar la recuperación de credenciales, la supervisión y la atribución de responsabilidades [30]. Una situación similar ocurre con la privacidad, ya que limitar la exposición de información requiere conservar la posibilidad de verificar la autenticidad y vigencia de las credenciales, incluso cuando estas deben ser revocadas sin facilitar correlaciones innecesarias sobre las actividades del titular [6, 26]. Estas condiciones se extienden hacia la interoperabilidad, que además de formatos y protocolos compatibles requiere criterios institucionales para determinar quién puede emitir, verificar, aceptar o revocar una credencial [7], ampliando el problema desde las propiedades individuales de la arquitectura hacia las relaciones que deben establecerse entre los diferentes actores que participan en su funcionamiento.

Precisamente, cuando estas relaciones dejan de limitarse a un mismo entorno y comienzan a involucrar actores pertenecientes a dominios diferentes, las exigencias de gobernanza adquieren una mayor complejidad. Deng et al. [4] muestran esta situación en escenarios completamente descentralizados donde múltiples participantes intervienen en los procesos de verificación, mientras que Li et al. [5] incorporan condiciones de robustez necesarias para sostener dichas interacciones dentro de sistemas distribuidos. Sobre esta ampliación, Chen et al. [30] abordan la autenticación entre dominios mediante mecanismos de supervisión que deben coexistir con las propiedades de privacidad, lo que transforma una relación inicialmente centrada en el titular y el verificador en una estructura donde participan entidades con capacidades y responsabilidades diferenciadas. Esta diversificación de actores modifica, a su vez, la forma en que se distribuyen la autenticación, la autorización, la supervisión y el reconocimiento, haciendo que la gobernanza dependa no solo de quién participa en el ecosistema, sino también de las reglas mediante las cuales esas responsabilidades se articulan con la arquitectura tecnológica.

La incorporación de estas reglas y responsabilidades permite enlazar la gobernanza con las dimensiones examinadas previamente, debido a que los componentes tecnológicos y los mecanismos utilizados para validarlos adquieren nuevas condiciones cuando se trasladan hacia escenarios donde intervienen múltiples actores e instituciones. Una credencial puede ser criptográficamente verificable y haber demostrado un funcionamiento adecuado en condiciones experimentales, pero su utilización entre organizaciones puede verse limitada por diferencias en los criterios de reconocimiento, mientras que un mecanismo diseñado para preservar la privacidad puede requerir procedimientos adicionales para gestionar el consentimiento y la revocación. De forma similar, una arquitectura distribuida puede disminuir la participación de determinados intermediarios sin eliminar la necesidad de establecer responsabilidades frente a errores o usos indebidos [28, 6, 7]. De esta manera, las condiciones institucionales amplían las exigencias identificadas durante la validación y el despliegue, al trasladarlas hacia el ciclo completo mediante el cual una identidad es creada, utilizada, reconocida y eventualmente revocada.

Al considerar ese ciclo de vida, las relaciones entre las cuatro dimensiones analizadas adquieren mayor continuidad, puesto que los registros distribuidos, los identificadores descentralizados, las credenciales verificables y los mecanismos de privacidad identificados en la dimensión tecnológica [3, 1, 23] cumplen funciones que posteriormente deben ser validadas y adaptadas a las condiciones de cada dominio. Los DID permiten establecer identificadores sin depender necesariamente de un registro central, aunque su utilización entre entornos requiere mecanismos comunes de resolución y reconocimiento, mientras que las VC facilitan la presentación verificable de atributos y, al circular entre diferentes actores, incorporan necesidades relacionadas con su vigencia, aceptación y revocación. Estas capacidades se complementan con mecanismos de privacidad que reducen la exposición de información sin eliminar las posibilidades de verificación y supervisión [18, 28, 30], haciendo que las decisiones adoptadas en la arquitectura tecnológica se proyecten hacia las formas de validación, las exigencias particulares de cada dominio y las condiciones de gobernanza que intervienen durante la implementación de la identidad digital descentralizada.

4. Discusión

Los hallazgos de esta revisión muestran que la identidad digital descentralizada ha alcanzado una creciente densidad técnica, aunque su madurez como ecosistema integral continúa siendo parcial. El campo ha dejado de situarse únicamente en el plano conceptual de la autonomía individual y presenta arquitecturas, prototipos y aplicaciones sectoriales sustentadas en *blockchain*/DLT, SSI, DID, VC y ZKP. Sin embargo, esta evolución no se produce de manera homogénea. La distribución del corpus revela que la infraestructura destinada a establecer confianza distribuida ha avanzado con mayor rapidez que los mecanismos necesarios para convertirla en una identidad portable, recuperable, revocable e institucionalmente reconocible. Ahmed et al. [3] permiten situar a *blockchain* como sustrato para establecer confianza entre actores, mientras que Mazzocca et al. [1] trasladan el problema hacia la interoperabilidad entre DID y VC. Esta distinción resulta fundamental, porque disponer de registros distribuidos, verificables e inmutables no garantiza por sí mismo una identidad soberana funcional. Por ello, el grado de descentralización tecnológica constituye solo una parte del problema; la cuestión relevante pasa a ser cómo esas tecnologías se articulan durante todo el ciclo de vida de la identidad.

Esta necesidad de articulación permite interpretar con mayor cautela una premisa recurrente en la literatura, según la cual una mayor descentralización conduciría necesariamente a una mayor autonomía del usuario. Los resultados de la revisión no respaldan una relación tan directa. La elevada presencia de *blockchain*/DLT, frente a la incorporación comparativamente menor de DID, VC, ZKP y criptografía poscuántica, sugiere que una parte importante de las propuestas continúa concentrándose en resolver la infraestructura de confianza antes que la gestión integral de la identidad. Aunque Cucko et al. [22] identifican autonomía, portabilidad y privacidad como propiedades esenciales de estos sistemas, su cumplimiento depende de mecanismos que permitan ejercerlas en condiciones reales. Una credencial portable pierde parte de su utilidad si su revocación compromete la privacidad; del mismo modo, el control individual resulta limitado cuando la pérdida de claves o dispositivos no dispone de procedimientos seguros de recuperación. La brecha observada no radica, por tanto, únicamente en la disponibilidad de tecnologías, sino en su integración coherente a lo largo de los procesos de emisión, almacenamiento, presentación, verificación, revocación, recuperación y auditoría. Precisamente, comprobar si esa integración funciona fuera de escenarios diseñados por los propios desarrolladores conduce a una segunda limitación del campo: la forma en que las soluciones están siendo validadas.

Desde esta perspectiva, la orientación predominantemente ingenieril identificada en el corpus constituye simultáneamente una fortaleza y una limitación. La proliferación de *frameworks*, arquitecturas, modelos y prototipos demuestra capacidad para transformar principios abstractos de SSI en soluciones técnicamente implementables. Asimismo, trabajos como los de Pöhn et al. [10] y Naik et al. [25] evidencian que el análisis de amenazas y vulnerabilidades ha adquirido un grado apreciable de sofisticación. No obstante, una arquitectura resistente frente a determinados ataques no necesariamente es robusta desde la perspectiva de quien debe utilizarla. La escasez de evaluaciones con usuarios reales reduce la evidencia disponible sobre comprensión de credenciales, gestión de claves, confianza, recuperación ante pérdidas, respuesta frente a errores y accesibilidad. Esta carencia adquiere especial importancia en SSI porque una parte de las responsabilidades tradicionalmente asumidas por proveedores centralizados se traslada al titular de la identidad. En consecuencia, una solución que maximice el control individual sin proporcionar mecanismos comprensibles de recuperación y asistencia puede sustituir dependencia institucional por complejidad técnica. Esta tensión entre autonomía y capacidad efectiva de uso adquiere todavía mayor relevancia cuando las soluciones abandonan el laboratorio y se trasladan a contextos sectoriales con usuarios, riesgos y exigencias regulatorias diferentes.

En efecto, la concentración de estudios en IoT, salud y finanzas muestra que la adopción avanza con mayor rapidez en ámbitos donde la gestión de identidad responde a necesidades operativas claramente identificables, como la autenticación máquina-máquina, la protección de información sensible o el cumplimiento de procedimientos de conocimiento del cliente (KYC, *know your customer*). Bai et al. [15] muestran el potencial de ZKP para reducir la exposición de información en contextos sanitarios; Ahmed et al. [16] sitúan SSI dentro de procesos financieros sujetos a requisitos de verificación; y Zhang et al. [20] extienden estas necesidades hacia escenarios de conectividad 6G. Estos avances demuestran que la identidad descentral-

izada puede aportar valor cuando existe una relación clara entre problema, tecnología y caso de uso. Sin embargo, la menor representación de gobierno y e-ID revela que esa capacidad todavía no se ha trasladado con la misma intensidad hacia espacios donde la identidad adquiere una dimensión de ciudadanía. Esta diferencia no es menor: el éxito en entornos financieros, sanitarios o ciberfísicos demuestra viabilidad sectorial, pero no garantiza su aplicación en servicios públicos, educación, movilidad o interacciones administrativas transfronterizas. Ampliar el alcance hacia estos escenarios exige, además de interoperabilidad técnica, reconocimiento institucional y reglas comunes sobre responsabilidad, consentimiento y protección de datos, lo que sitúa la discusión directamente en el plano regulatorio.

Es precisamente en esta dimensión donde la distancia entre capacidad tecnológica y despliegue efectivo se hace más evidente. Lindquist [6] muestra que el consentimiento requiere mecanismos verificables e interoperables, mientras que Lee et al. [26] señalan que la revocación y la preparación frente a escenarios poscuánticos continúan planteando desafíos. A su vez, Bureaca et al. [7] proponen, en el marco de eIDAS 2.0, mecanismos orientados a disminuir la vinculabilidad durante la revocación de atestaciones cualificadas. Considerados conjuntamente, estos trabajos muestran que privacidad, consentimiento y revocación no constituyen problemas independientes, sino componentes de una misma arquitectura de gobernanza de la identidad. Sin embargo, el corpus no evidencia una matriz de evaluación ampliamente aceptada que permita determinar de forma comparable hasta qué punto las soluciones satisfacen exigencias asociadas con RGPD y eIDAS 2.0. La consecuencia práctica es relevante: sin criterios verificables de conformidad resulta difícil comparar arquitecturas, establecer responsabilidades, realizar auditorías o generar confianza institucional para su adopción a mayor escala. Así, la regulación no debería entenderse como una capa posterior que se incorpora una vez concluido el desarrollo tecnológico, sino como un requisito de diseño que condiciona desde el inicio la gestión de credenciales, datos, consentimiento, revocación y evidencia de las operaciones.

A partir de estas relaciones, los resultados permiten sostener que la principal frontera de investigación ya no se encuentra exclusivamente en el desarrollo de mecanismos criptográficos más sofisticados, sino en la convergencia de capacidades que hasta ahora han evolucionado a ritmos diferentes. La madurez de la identidad digital descentralizada requiere articular una arquitectura técnicamente interoperable, mecanismos de privacidad y recuperación suficientemente robustos, validación empírica con usuarios diversos y una gobernanza regulatoria susceptible de auditoría. Esto implica también reconsiderar qué significa “identidad soberana”: no debería reducirse a que el usuario controle claves o credenciales, sino comprender su capacidad efectiva para utilizarlas, recuperarlas, revocarlas y ejercer derechos sobre ellas dentro de ecosistemas institucionalmente reconocidos. Bajo esta perspectiva, privacidad y supervisión no son necesariamente objetivos contrapuestos, siempre que la segunda sea proporcional, trazable y no restablezca formas innecesarias de centralización. La consolidación del campo dependerá, en consecuencia, de su capacidad para demostrar que la descentralización no solo redistribuye la confianza tecnológica, sino que mejora de manera verificable la autonomía, seguridad e inclusión de quienes utilizan la identidad digital. De no alcanzarse esta convergencia, las nuevas infraestructuras podrían reproducir problemas que precisamente motivaron el desarrollo de SSI, entre ellos la fragmentación, nuevas dependencias, exclusión de usuarios vulnerables y dificultades para atribuir responsabilidades frente a fallos.

5. Conclusiones

Esta revisión sistemática caracterizó el estado de las tecnologías de identidad digital aplicadas a la autenticación segura en ecosistemas descentralizados y muestra un campo técnicamente denso pero de madurez asimétrica. La cadena de bloques se mantiene como sustrato de confianza predominante, sobre el cual los identificadores descentralizados, las credenciales verificables y las pruebas de conocimiento cero se consolidan como núcleo de una arquitectura orientada a la autenticación con divulgación mínima. Sin embargo, la investigación conserva un perfil marcadamente ingenieril, con escasa validación en despliegues reales y con usuarios. Además, se concentra en el internet de las cosas, la salud y las finanzas, mientras el gobierno, la educación y los servicios transfronterizos permanecen infrarrepresentados. A ello se suma que marcos como el RGPD y eIDAS 2.0 han permeado el discurso más que el diseño de los sistemas, y el consentimiento verificable, la revocación no vinculable y la supervisión proporcional siguen sin resolverse de forma integrada. La principal contribución del estudio consiste en desplazar el criterio de madurez desde

la viabilidad técnica de los componentes hacia el ciclo de vida completo de la credencial. Por tanto, la soberanía debe entenderse como la capacidad efectiva del titular para utilizar, recuperar y revocar sus credenciales en ecosistemas institucionalmente reconocidos, y no como el mero control de claves. La agenda futura exige desarrollar matrices auditables de conformidad regulatoria, mecanismos de revocación compatibles con la transición poscuántica, estudios longitudinales con usuarios diversos y pilotos en identidad electrónica pública. Solo así la descentralización podrá consolidarse como una infraestructura de confianza legítima, y no como una redistribución de las dependencias que pretendía superar.

Contribución del autor. Los autores confirman su contribución al artículo de la siguiente manera: conceptualización, M.C.C. y E.T.G.; metodología, M.C.C. y E.T.G.; investigación, M.C.C. y E.T.G.; análisis formal, M.C.C. y E.T.G.; redacción – preparación del borrador original, M.C.C. y E.T.G.; redacción – revisión y edición, M.C.C. y E.T.G.; visualización, M.C.C. y E.T.G. Todos los autores revisaron los resultados y aprobaron la versión final del manuscrito.

Agradecimientos. A la Universidad Tecnológica del Perú por el apoyo institucional brindado para el desarrollo de esta investigación.

Financiamiento. El estudio ha sido autofinanciado por los autores.

Declaración de consentimiento informado. No aplica, dado que el estudio no involucró participantes humanos.

Declaración de disponibilidad de datos. La exportación de registros de Scopus, la matriz de cribado y la matriz de extracción y codificación de los 23 estudios del corpus pueden solicitarse al autor de correspondencia.

Conflictos de intereses. Los autores declaran no tener conflictos de intereses.

Declaración de uso de inteligencia artificial. Se emplearon herramientas de inteligencia artificial generativa exclusivamente para apoyar la edición del texto y la maquetación. El análisis, la interpretación de los resultados y las conclusiones son responsabilidad intelectual exclusiva de los autores, quienes validaron y aprobaron la versión final.

Referencias

- [1] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, “A survey on decentralized identifiers and verifiable credentials,” *IEEE Communications Surveys and Tutorials*, 2025. doi: 10.1109/COMST.2025.3543197.
- [2] U. Arshad, A. Tubaishat, S. Anwar, Z. Halim, A. Abualkishik, and A. Ullah, “Web3-based identity and kyc innovations for next-generation fintech,” *ACM Transactions on the Web*, 2026. doi: 10.1145/3771991.
- [3] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, “Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey,” *IEEE Access*, vol. 10, pp. 113 436–113 481, 2022. doi: 10.1109/ACCESS.2022.3216643.
- [4] H. Deng, J. Liang, C. Zhang, X. Liu, L. Zhu, and S. Guo, “FutureDID: A fully decentralized identity system with multi-party verification,” *IEEE Transactions on Computers*, 2024. doi: 10.1109/TC.2024.3365271.
- [5] Z. Z. Li, H. Cui, A. C. Y. Leung, D. Y. W. Liu, J. K. Liu, J. Yu, and D. Gasevic, “DisIMS: A distributed identity management system via blockchain,” *IEEE Transactions on Dependable and Secure Computing*, 2026. doi: 10.1109/TDSC.2025.3624710.
- [6] J. Lindquist, “Introducing privacy receipts into DLT and eIDAS,” *Journal of ICT Standardization*, vol. 11, no. 3, pp. 177–202, 2023. doi: 10.13052/jicts2245-800X.1132.

- [7] E. Bureaca, R.-A. Leanca, I. Ciobanu, A. Brinzea, and I. Aciobaniței, “Unlinkable revocation lists for qualified electronic attestations: A blockchain-based framework,” *Electronics*, vol. 14, no. 14, p. 2795, 2025. doi: 10.3390/electronics14142795 .
- [8] E. Samir, H. Wu, M. Azab, C. Xin, and Q. Zhang, “DT-SSIM: A decentralized trustworthy self-sovereign identity management framework,” *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8688–8701, 2022. doi: 10.1109/JIOT.2021.3112537 .
- [9] E. S. Fathalla, M. Azab, C. Xin, and H. Wu, “PT-SSIM: A proactive, trustworthy self-sovereign identity management system,” *IEEE Internet of Things Journal*, vol. 10, no. 6, pp. 5401–5415, 2023. doi: 10.1109/JIOT.2022.3222610 .
- [10] D. Pöhn, M. Grabatin, and W. Hommel, “Modeling the threats to self-sovereign identities,” in *Proceedings of the Open Identity Summit 2023*, 2023. doi: 10.18420/OID2023_07 .
- [11] T. Rathee and P. Singh, “A systematic literature mapping on secure identity management using blockchain technology,” *Journal of King Saud University – Computer and Information Sciences*, vol. 34, no. 8, pp. 5782–5796, 2022. doi: 10.1016/j.jksuci.2021.03.005 .
- [12] R. Tertulino, F. Vidal, and N. Ivaki, “A decentralized architecture for electronic health records to enhanced security and privacy,” in *Proceedings – 2025 20th European Dependable Computing Conference Companion Proceedings, EDCC-C 2025*, 2025, pp. 174–179. doi: 10.1109/EDCC-C66476.2025.00052 .
- [13] J. Fry and G. Hileman, “Challenges of user data privacy in self-sovereign identity verifiable credentials for autonomous building access,” *Frontiers in Blockchain*, vol. 7, p. 1374655, 2024. doi: 10.3389/fbloc.2024.1374655 .
- [14] R. Xiong, W. Ren, X. Hao, J. He, and K.-K. R. Choo, “BDIM: A blockchain-based decentralized identity management scheme for large scale internet of things,” *IEEE Internet of Things Journal*, 2023. doi: 10.1109/JIOT.2022.3228219 .
- [15] T. Bai, Y. Hu, J. He, H. Fan, and Z. An, “Health-zkidm: A healthcare identity system based on fabric blockchain and zero-knowledge proof,” *Sensors*, vol. 22, no. 22, p. 8586, 2022. doi: 10.3390/s22228586 .
- [16] I. Ahmed, K. Toyoda, T. Nakano, S. Kasahara, S. R. Goyal, and T. H. Tran, “A systematic review on blockchain-enabled eKYC: Leveraging SSI and DID for secure and efficient identity verification,” *IEEE Internet of Things Journal*, 2025. doi: 10.1109/JIOT.2025.3597356 .
- [17] Q. An, F. Jiang, C. Dong, S. Pal, J. Li, A. G. Neiat, and W. Yeoh, “A blockchain-powered secure architecture for cyber marketplaces of electric vehicles,” *IEEE Transactions on Industry Applications*, vol. 61, no. 3, pp. 4198–4213, 2025. doi: 10.1109/TIA.2025.3536421 .
- [18] Y.-H. Hsieh, C.-H. Tseng, B.-Y. Luo, and S.-M. Yuan, “Cross-border digital identity system based on ethereum layer 2 architecture,” *Electronics*, vol. 15, no. 3, p. 708, 2026. doi: 10.3390/electronics15030708 .
- [19] S. M. Smith and C. Dion-Schwarz, “Mechanisms for digital transformation in the education and healthcare sectors utilizing decentralized self-sovereign identity,” *International Journal of Network Security and Applications*, vol. 15, no. 2, 2023. doi: 10.5121/ijnsa.2023.15201 .
- [20] G. Zhang, Q. Hu, Y. Zhang, and T. Jiang, “A blockchain-based user-centric identity management toward 6G networks,” *Digital Communications and Networks*, 2026. doi: 10.1016/j.dcan.2025.05.009 .
- [21] R. A. Pava-Diaz, J. Gil-Ruiz, and D. A. Lopez-Sarmiento, “Self-sovereign identity on the blockchain: Contextual analysis and quantification of ssi principles implementation,” *Frontiers in Blockchain*, vol. 7, p. 1443362, 2024. doi: 10.3389/fbloc.2024.1443362 .
- [22] S. Cucko, S. Becirovic, A. Kamisalic, S. Mrdovic, and M. Turkanovic, “Towards the classification of self-sovereign identity properties,” *IEEE Access*, vol. 10, pp. 60 908–60 928, 2022. doi: 10.1109/ACCESS.2022.3166866 .

- [23] Z. B. Sassi, C. C. Yaici, J. Xiang, O. Salem, and A. Mehaoua, "Benchmarking zero-knowledge proof-based authentication protocols," in *Proceedings of IEEE SOFTT 2025*, 2025. doi: 10.1109/SOFTT67007.2025.11212915 .
- [24] J. H. M. Emati, V. K. Tchendji, and M. Djam-Doudou, "A zero-trust decentralized identifier specification based machine learning against cyber-attacks in blockchain based self-sovereign identity," *Journal of Cloud Computing*, 2026. doi: 10.1186/s13677-026-00862-0 .
- [25] N. Naik, P. Grace, P. Jenkins, K. Naik, and J. Song, "An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity," *Computers & Security*, vol. 114, p. 102808, 2022. doi: 10.1016/j.cose.2022.102808 .
- [26] Y. Lee, H. Shin, and D. Choi, "A survey on credential revocation and DID deactivation in self-sovereign identity systems," *IEEE Access*, 2026. doi: 10.1109/ACCESS.2025.3649792 .
- [27] V. Kersic, U. Vidovic, A. Vrecko, M. Domajnko, and M. Turkanovic, "Orchestrating digital wallets for on- and off-chain decentralized identity management," *IEEE Access*, vol. 11, pp. 13 126–13 147, 2023. doi: 10.1109/ACCESS.2023.3242817 .
- [28] H.-Y. Paik, Y. Liu, Q. Lu, and S. S. Kanhere, "Decentralized identity management and blockchains: Design patterns and architectures," *Advances in Information Security*, vol. 100, 2024. doi: 10.1007/978-3-031-32146-7_15 .
- [29] M. Guerar, M. Migliardi, E. Russo, D. Khadraoui, and A. Merlo, "SSI-MedRx: A fraud-resilient health-care system based on blockchain and SSI," *Blockchain: Research and Applications*, vol. 6, no. 1, 2025. doi: 10.1016/j.bcra.2024.100242 .
- [30] C. Chen, G. Yang, D. Zhang, W. Wang, Q. Chen, and J. Li, "S3Cross: Blockchain-based cross-domain authentication with self-sovereign and supervised identity management," *IEEE Transactions on Network and Service Management*, 2026. doi: 10.1109/TNSM.2025.3642315 .