



REVIEW

Digital identity technologies applied to secure authentication in decentralized ecosystems

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

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

¹Faculty of Engineering, Universidad Tecnológica del Perú, Piura, 20001, Peru

²Faculty of Engineering, Universidad de Ingeniería y Tecnología, Lima, 15063, Peru

*Corresponding Author: c27213@utp.edu.pe

Submitted: 29 May 2026 Accepted: 13 July 2026 Published online: 15 July 2026

Abstract

Ensuring secure user authentication in decentralized ecosystems is one of the most complex challenges of digital identity, given that current technologies do not offer sufficient guarantees of privacy or individual sovereignty. To address 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 is the predominant technological substrate in 91 % of the identified solutions, while the self-sovereign identity paradigm is the dominant architectural approach in 52 % of the studies. In particular, decentralized identifiers, verifiable credentials, and zero-knowledge proofs are consolidating 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

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

This is an open-access article and is distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0).

Cite as: M. Cobeñas Chanduvi and E. Tejada Gutierrez, "Digital identity technologies applied to secure authentication in decentralized ecosystems," *CISAI*, vol. 2, no. 2, pp. 82–98, July 2026, doi: 10.64439/cisai.v2i2.47.

verificables

1. Introduction

The growing digitalization of public, financial, and health services has placed digital identity at the center of contemporary trust systems. Securely managing who is who in the digital environment is no longer an exclusively technical matter, but an enabling condition for the exercise of rights, access to resources, and participation in the digital economy [1]. In this scenario, identity management has historically relied on centralized architectures in which third parties, whether technology companies, financial institutions, or public administrations, hold users' credentials and decide when and how they can be verified. This model, although functional in controlled environments, has shown deep limitations as digital ecosystems have become more open, distributed, and interoperable. Evidence of this is that more than ten billion records have been compromised in security breaches associated with centralized repositories [2], and more than one billion people remain excluded from any recognized form of digital identity [3]. When a citizen tries to prove their identity before a foreign administration and discovers that their credentials are not valid outside their country of origin, or when a user loses access to their data because the platform that held them has been breached, what is at stake is not only digital convenience, but the very possibility of participating in contemporary social and economic life.

In response to these limitations, the self-sovereign identity paradigm has emerged as a proposal to reorganize the field, whose central premise is that individuals should be able to manage their own credentials without depending on intermediaries. This approach, known as SSI (*self-sovereign identity*), relies on standards such as decentralized identifiers (DID) and verifiable credentials (VC), usually supported by blockchains or distributed ledgers (DLT) and complemented by zero-knowledge proofs (ZKP), whose adoption has extended from user environments to internet of things devices, health applications, and financial platforms [1]. However, scientific output on this paradigm, although growing, is advancing without an overall view to guide its development. At the technological level, solutions are evolving rapidly, but without an updated synthesis of which ones predominate and how they have been adopted in truly decentralized ecosystems [4]. At the methodological level, most proposals are validated under laboratory conditions, with few studies demonstrating their performance with real users [5]. As for application domains, research tends to concentrate on a few sectors, leaving unaddressed areas with high potential for social impact. Moreover, reference regulatory frameworks, such as the General Data Protection Regulation (GDPR) or the European Union digital identity wallet provided for in the eIDAS 2.0 regulation, are advancing without technical systems having reached the level of regulatory alignment they require [6, 7]. Taken together, these gaps point to the absence of a systematic review that articulates the state of the field and guides its development on a solid empirical basis.

The present work undertakes that task. Through a systematic literature review that analyzed 835 publications from the 2022–2026 period indexed in Scopus, it offers an integrative synthesis organized around four research questions that correspond, respectively, to the technological, methodological, applied, and regulatory dimensions of the field.

- **RQ1.** Which digital identity technologies predominate in decentralized ecosystems, and how has their adoption evolved between 2022 and 2026?
- **RQ2.** Which methodological approaches characterize research in this field, and what gaps persist in validation with real users?
- **RQ3.** In which application domains is research concentrated, and which show the largest gaps relative to their potential social impact?
- **RQ4.** To what extent have current regulatory frameworks permeated the design of decentralized identity systems, and what gaps persist between regulation and implementation?

The rest of the article is organized as follows: Section 2 describes the methodological protocol used, Section 3 presents the results organized around the four research questions, Section 4 discusses the findings in relation to the state of the art, and Section 5 summarizes the conclusions, contributions, and implications

for future research.

2. Methodology

The methodology was structured as a systematic review aimed at identifying, selecting, and characterizing recent scientific output on decentralized digital identity and its main technological mechanisms. To ensure the traceability of the process, the procedure was organized sequentially from the bibliographic search to the formation of the final corpus, articulating the search strategy, the inclusion and exclusion criteria, the PRISMA-based selection process, and the typological characterization of the studies. This organization made it possible to understand not only how the documents analyzed were obtained, but also how their thematic, temporal, and methodological relevance was delimited before carrying out the analyses presented in Section 3.

2.1 Search strategy

The bibliographic search was the starting point for delimiting a sufficiently broad and reproducible set of documents. Scopus was used as the primary source because of its multidisciplinary coverage and the possibility of running structured queries on the title, abstract, and keyword fields. The search was carried out on 5 May 2026 and covered publications between January 2022 and April 2026, a period selected to represent the most recent scientific output associated with the maturation of the W3C DID/VC standards [1] and with the consolidation of the European debate on digital identity and eIDAS 2.0 [6]. The query used was as follows:

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

Applying this strategy initially produced 835 records, which were exported in BibTeX format and incorporated into an analysis matrix to facilitate their organization and subsequent screening. No geographical restrictions were set, although only English-language publications were retained owing to the configuration adopted for the review. Based on the retrieved metadata, the documents were identified through controlled vocabulary related to blockchain, authentication, decentralized identity, self-sovereign identity, identity management, digital identity, and data privacy. On this basis, the logic used to delimit the document universe can be understood as the intersection of three complementary conditions, as shown in Figure 1. The first corresponds to thematic relevance with respect to decentralized digital identity, the second to the presence of technological authentication or identity management mechanisms, and the third to the methodological and temporal conditions defined for the review. Thus, the corpus was not built solely from terminological matches, but through the convergence of thematic relevance, technological support, and documentary relevance.

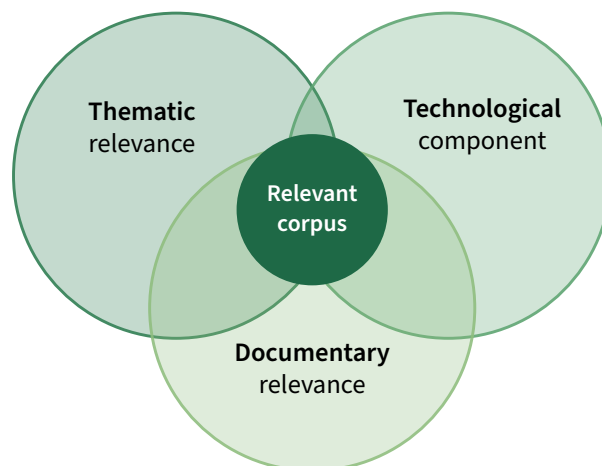


Figure 1. Convergence of criteria for the conceptual delimitation of the corpus

This representation made it possible to distinguish the initial bibliographic retrieval from the subsequent analytical selection, since the presence of terms related to digital identity did not by itself guarantee the inclusion of a document. Likewise, it was necessary to verify simultaneously its relationship with identity technologies and compliance with the documentary conditions defined for the study, a process that was formalized through the criteria described below.

2.2 Inclusion and exclusion criteria

The selection criteria were established before the final screening in order to ensure their uniform application to the retrieved records. To this end, five dimensions were considered, related to subject matter, publication period, language, source type, and the availability of sufficient content to carry out the analysis. As summarized in Table 1, this matrix made it possible to differentiate documents directly linked to decentralized digital identity from those in which blockchain appeared exclusively associated with financial applications, traceability, or other uses without an explicit identity management component.

Tabla 1. Inclusion and exclusion criteria applied to the document corpus

Dimension	Inclusion	Exclusion
Subject matter	Studies on digital identity, self-sovereign identity, decentralized identifiers, verifiable credentials, or decentralized authentication	Blockchain studies without an identity component or intended exclusively for financial applications
Period	Publications between January 2022 and April 2026	Publications prior to January 2022
Language	English-language publications	Publications in other languages
Source type	Scientific articles, papers published in indexed academic proceedings, and peer-reviewed book chapters	Grey literature and technical reports without academic review
Content	Record with an abstract sufficient to determine thematic relevance and carry out the analysis	Record without an abstract or with insufficient information to establish its relevance

The joint application of these criteria made it possible to move from a retrieval based fundamentally on search terms to a selection grounded in documentary relevance. This distinction is therefore important because it avoids treating as central evidence studies that use similar technologies but pursue objectives other than decentralized identity management. On this basis, the screening process that led from the 835 initial records to the 23 studies included in the final corpus was carried out, as explained in the next subsection.

2.3 Study selection process

The selection process followed the identification, screening, eligibility, and inclusion phases set out in PRISMA. Figure 2 summarizes the path followed by the records and shows both the progressive reduction of the document universe and the main reasons for exclusion. During identification, 835 records published between 2022 and 2026 were retrieved. In the screening phase, their titles and keywords were examined, which made it possible to exclude 53 documents related to the traceability of physical assets without an identity component and 18 publications in languages other than English. As a result, 764 documents moved on to the eligibility assessment.

Subsequently, the abstracts were read, which allowed a more specific screening of the content. In this phase, 741 records were excluded, of which 317 dealt exclusively with blockchain consensus protocols without a direct relationship to identity management, 166 had a peripheral scope or fell outside the effective analysis period, 130 did not provide sufficient technical or empirical evidence, and 128 lacked a substantive abstract allowing their relevance to be determined. Once this procedure was completed, 23 studies remained, which formed the final corpus on which the subsequent characterization and analysis were carried out.

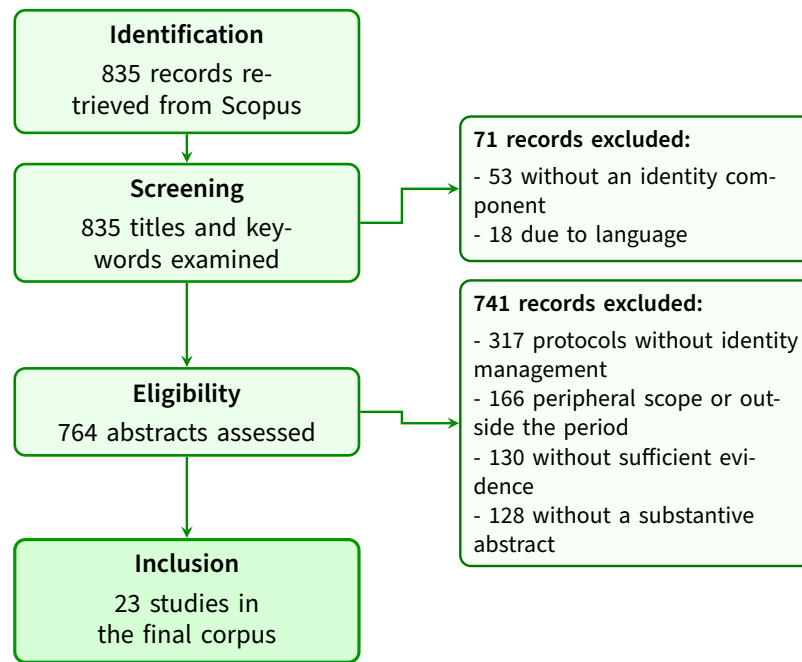


Figura 2. Identification, screening, and selection process of the document corpus

2.4 Typological characterization of the corpus

Once the final corpus was established, the studies were organized through three analytical dimensions intended to provide a common structure for their subsequent examination. The first corresponds to the methodological approach and makes it possible to distinguish between conceptual proposals, implementations, security analyses, reviews, and empirical evaluations, while the second identifies the main domain in which decentralized digital identity is applied and the third recognizes the technologies underpinning the solutions studied. Thus, the classification does not yet seek to establish the predominance of some categories over others, but to organize a corpus through comparable criteria that facilitate the subsequent identification of trends and gaps. In this regard, Table 2 summarizes the classification structure used and links each category to representative studies that preserve its traceability with respect to the literature examined.

Furthermore, the organization presented in Table 2 shows that the characterization was conceived to observe the corpus from complementary perspectives. Indeed, the methodological approach makes it possible to differentiate studies oriented toward the design of frameworks and architectures from those that advance toward implementations, security analyses, reviews, or evaluations in real scenarios. In turn, the application domain places these contributions in contexts such as the internet of things, health, finance, mobility, government, and education, which makes it possible to examine later whether the challenges of decentralized identity take on different characteristics depending on the environment in which they are implemented.

In this context, the technological dimension completes this structure by identifying the components on which the analyzed solutions are built, among them blockchain, self-sovereign identity, decentralized identifiers, verifiable credentials, zero-knowledge proofs, biometrics, artificial intelligence, and post-quantum cryptography. The dimensions were therefore considered complementary, since a study may combine different technologies and methodological approaches even when it is associated with a main application domain. Thus, the characterization is not an isolated result, but an organization that connects the selection procedure with the analysis carried out in Section 3, where these categories make it possible to examine trends, technological relationships, and less developed areas within the literature.

3. Results

This section presents the results obtained from the analysis of the 23 studies that formed the final corpus, organized into four dimensions related to technological architecture, methodological profile, application

Tabla 2. Typological characterization of the analysis corpus

Dimension	Identified category	Representative study
Methodological approach	Framework or architecture proposal	Samir et al. [8]
	Implementation and experimental prototype	Fathalla et al. [9]
	Formal security analysis	Pöhn et al. [10]
	Systematic review	Rathee et al. [11]
	Case study with real deployment	Tertulino et al. [12]
	Empirical evaluation with users	Fry and Hileman [13]
Application domain	Internet of things	Xiong et al. [14]
	Health	Bai et al. [15]
	Finance and customer identification	Ahmed et al. [16]
	Vehicles and connected mobility	An et al. [17]
	Metaverse and decentralized environments	Arshad et al. [2]
	Government and electronic identity	Hsieh et al. [18]
	Education and academic certification	Smith and Dion-Schwarz [19]
	Next-generation mobile networks	Zhang et al. [20]
	Other domains	Pava et al. [21]
Core technology	Blockchain and distributed ledgers	Ahmed et al. [3]
	Self-sovereign identity	Cucko et al. [22]
	Decentralized identifiers	Mazzocca et al. [1]
	Zero-knowledge proofs	Sassi et al. [23]
	Verifiable credentials	Mazzocca et al. [1]
	Artificial intelligence and machine learning	Emati et al. [24]
	Biometrics	Naik et al. [25]
	Post-quantum cryptography	Lee et al. [26]

domains, and regulatory and governance conditions. Their integration made it possible to examine the evidence beyond the individual description of the technologies and to identify patterns, relationships, and gaps that condition their implementation, aspects developed in the following subsections according to the findings identified in each dimension.

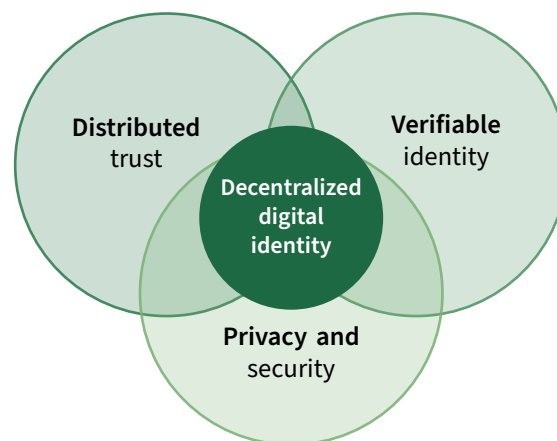
3.1 Technological architecture and evolution of solutions

From a technological perspective, the studies show an evolution from architectures centered mainly on distributed ledgers toward configurations that incorporate specialized mechanisms for identification, credentials, and privacy protection. In this regard, Ahmed et al. [3] explain blockchain as an infrastructure for establishing distributed trust, while Cucko et al. [22] broaden this perspective through self-sovereign identity and Mazzocca et al. [1] highlight the role of decentralized identifiers and verifiable credentials. Added to this structure are the zero-knowledge proofs studied by Sassi et al. [23], together with biometric mechanisms [25], artificial intelligence [24], and post-quantum cryptography approaches [26]. In terms of frequency, 21 of the 23 studies in the corpus (91 %) use blockchain or some distributed ledger as a trust substrate, while 12 of them (52 %) explicitly adopt the self-sovereign identity paradigm as their architectural approach, values that correspond to those reported in the abstract. Table 3 summarizes these components according to the role they play within the systems analyzed.

Tabla 3. Identified technologies and their role in decentralized digital identity

Technology	Identified role	Representative study
Blockchain and distributed ledgers	Establishment of distributed trust and verifiable record-keeping	Ahmed et al. [3]
Self-sovereign identity	Holder control over credentials and attributes	Cucko et al. [22]
Decentralized identifiers	Verifiable and interoperable identification	Mazzocca et al. [1]
Verifiable credentials	Issuance, presentation, and verification of digital attributes	Mazzocca et al. [1]
Zero-knowledge proofs	Verification of information with limited disclosure of attributes	Sassi et al. [23]
Artificial intelligence	Support for oversight, detection, and authentication processes	Emati et al. [24]
Biometrics	Strengthening of authentication mechanisms	Naik et al. [25]
Post-quantum cryptography	Protection against future cryptographic scenarios	Lee et al. [26]

This organization shows that the technologies do not necessarily function as independent alternatives, but as components that can be integrated within the same architecture. On this basis, Kersic et al. [27] illustrate this need by pointing out that digital wallets require coordination between on-chain and off-chain components, while Paik et al. [28] shift the problem from mere technical feasibility toward the construction of recoverable, auditable, and governable architectures. Thus, technological development can be interpreted as a transition from a distributed trust infrastructure toward an ecosystem in which identification, credentials, privacy, and authentication need to operate in a coordinated manner. In this context, and for further characterization, Figure 3 conceptually illustrates these aspects, with decentralized digital identity appearing at the convergence of three capabilities identified in the literature. Distributed trust provides a basis for registration and verification, verifiable identity makes it possible to represent subjects and entities through identifiers and credentials, and privacy and security intervene in the protection and controlled disclosure of attributes [3, 1, 23].

**Figura 3.** Convergence of technological capabilities in decentralized digital identity

From this perspective, the technological finding lies not only in identifying the components used, but in recognizing the progressive formation of composite architectures. Blockchain thus provides a trust infrastructure, while decentralized identifiers, verifiable credentials, and privacy mechanisms carry that infrastructure into concrete identification and authentication processes [1, 23]. In turn, the incorporation of biometrics, artificial intelligence, and post-quantum cryptography broadens the possibilities for protection and oversight [25, 24, 26], although it also introduces new requirements related to interoperability, credential recovery, and governance.

3.2 Methodological profile and validation

In line with the technological evolution observed, the methodological analysis shows that the literature approaches the problem through approaches that span different levels of development and validation, from the formulation of architectures to their evaluation in applied scenarios. Along this path, Samir et al. [8] focus on developing decentralized trust architectures, while Fathalla et al. [9] carry these proposals into experimental implementation and Pöhn et al. [10] examine in depth the evaluation of their security properties. These approaches are complemented by systematic reviews [11], which consolidate the available evidence, as well as by studies with applied deployment [12] and user evaluations [13], which extend validation toward contexts of use closer to real conditions. Thus, the approaches identified reflect different degrees of proximity between conceptual design and empirical verification of the solutions, whose distribution is organized in Table 4.

Tabla 4. Methodological approaches identified in the corpus

Approach	Contribution to the analysis	Representative study
Framework or architecture	Conceptual structuring of components and relationships	Samir et al. [8]
Experimental prototype	Functional verification under controlled conditions	Fathalla et al. [9]
Security analysis	Identification of threats and vulnerabilities	Pöhn et al. [10]
Systematic review	Integration and comparison of prior evidence	Rathee et al. [11]
Real deployment	Evaluation of performance in applied scenarios	Tertulino et al. [12]
User evaluation	Analysis of interaction, acceptance, and user experience	Fry and Hileman [13]

A joint reading of these approaches makes it possible to distinguish between demonstrating that an architecture can work and verifying that it retains its effectiveness when transferred to real conditions of use. In this transition, Pöhn et al. [10] and Naik et al. [25] show progress in the analysis of threats and attack surfaces, while Fathalla et al. [9] extend validation toward the experimental testing of solutions. Nevertheless, as these technologies move beyond controlled environments, evaluation no longer depends solely on their technical consistency and begins to incorporate aspects related to user experience, credential recovery, error handling, and digital inclusion, which broadens the criteria needed to determine their feasibility in real scenarios.

From this perspective, the findings reveal a gap between the technical maturity achieved and the degree of situated validation of the solutions, since having cryptographically consistent mechanisms is a necessary but not sufficient condition for guaranteeing their adoption and sustained operation. This gap therefore becomes more relevant in more complex technological scenarios, such as those analyzed by Xiong et al. [14], where identity extends to ecosystems with a large number of devices and the authenticated subject may be a person, a machine, or a connected component. Thus, broadening the application environment also changes the evaluation requirements, since it requires scalability, recovery, interaction, and credential administration to be considered jointly with security.

3.3 Application domains and implementation requirements

Having examined the methodological approaches and levels of validation used in the literature, the analysis continues with the scenarios in which decentralized digital identity solutions are implemented, in order to recognize how the characteristics of each domain condition their technological and operational requirements. From this perspective, the studies examined cover contexts such as the internet of things, health, finance, connected mobility, decentralized virtual environments, government, education, and communication networks. In the case of the internet of things, Xiong et al. [14] address identity in ecosystems

of connected devices, while Bai et al. [15] apply it to the protection of health information and Ahmed et al. [16] to financial identity verification processes. This diversity is broadened by An et al. [17], who incorporate connected mobility scenarios, and by Hsieh et al. [18] and Zhang et al. [20], whose work makes it possible to observe the requirements associated with government services and next-generation networks. This distribution therefore shows that decentralized identity responds to different needs depending on the environment in which it is incorporated, so Table 5 organizes the main areas identified and the needs associated with each.

Tabla 5. Application domains and identified needs

Domain	Associated need	Representative study
Internet of things	Device authentication and machine-to-machine communication	Xiong et al. [14]
Health	Protection of clinical data and identity verification	Bai et al. [15]
Finance	Customer identification and regulated verification	Ahmed et al. [16]
Vehicles and mobility	Identity of components and cyber-physical entities	An et al. [17]
Decentralized virtual environments	Persistence and control of digital identity	Arshad et al. [2]
Government and electronic identity	Institutional interoperability and provision of digital services	Hsieh et al. [18]
Education	Issuance and verification of academic certifications	Smith and Dion-Schwarz [19]
Next-generation networks	Distributed authentication in advanced infrastructures	Zhang et al. [20]

Based on this classification, the comparison between domains shows that the same identity architecture takes on different requirements when transferred from one context to another. In the health sector, Guerar et al. [29] relate self-sovereign identity to needs for privacy, traceability, and fraud prevention, while in the financial sector Ahmed et al. [16] incorporate identity verification into processes subject to regulatory requirements. This variation becomes even more evident in mobility, where An et al. [17] introduce a cyber-physical dimension that extends trust from people to vehicles and connected components, unlike the government sphere, in which the participation of different institutions adds requirements for interoperability and institutional recognition [18]. Thus, the application domain is not merely the setting in which the technology is deployed, but a factor that determines the conditions under which an architecture can adequately respond to identity needs.

This relationship between context and requirements leads to a closer examination of the requirements that become most relevant during implementation. In studies focused on the internet of things, authentication and scalability play a central role owing to the number and diversity of devices that must interact [14], while in health and finance the protection of sensitive information and verification obligations reinforce the importance of privacy, traceability, and authentication [15, 16]. As the scenario shifts toward mobility, these requirements are combined with the need to authenticate cyber-physical entities and maintain operation in distributed environments [17]; by contrast, in government and education, where the same credential may require recognition by different organizations, interoperability becomes more relevant [18, 19]. In this context, the differences make it possible to establish a qualitative relationship between the domains studied and the attributes that condition their implementation, summarized in Figure 4.



Figure 4. Qualitative matrix of the relationship between application domains and identified attributes

The relationships summarized in Figure 4 show that the requirements associated with decentralized digital identity are not distributed uniformly, but take on different intensities according to the operational and institutional characteristics of each domain. Thus, health and financial contexts require a particularly close articulation between privacy, authentication, and traceability [15, 16], while the internet of things and mobility increase the importance of authentication and scalability owing to the multiplicity of entities involved [14, 17]. This configuration changes again in government and education, where the need for credentials to be verified and recognized by different actors prevails [18, 19]. Indeed, the results show that the decentralized identity architecture cannot be defined as a uniform technological configuration, but as a structure that must adapt to the conditions of the domain in which it will be implemented, a relationship that leads to examining the regulatory and governance conditions that determine its recognition and operation beyond the strictly technological environment.

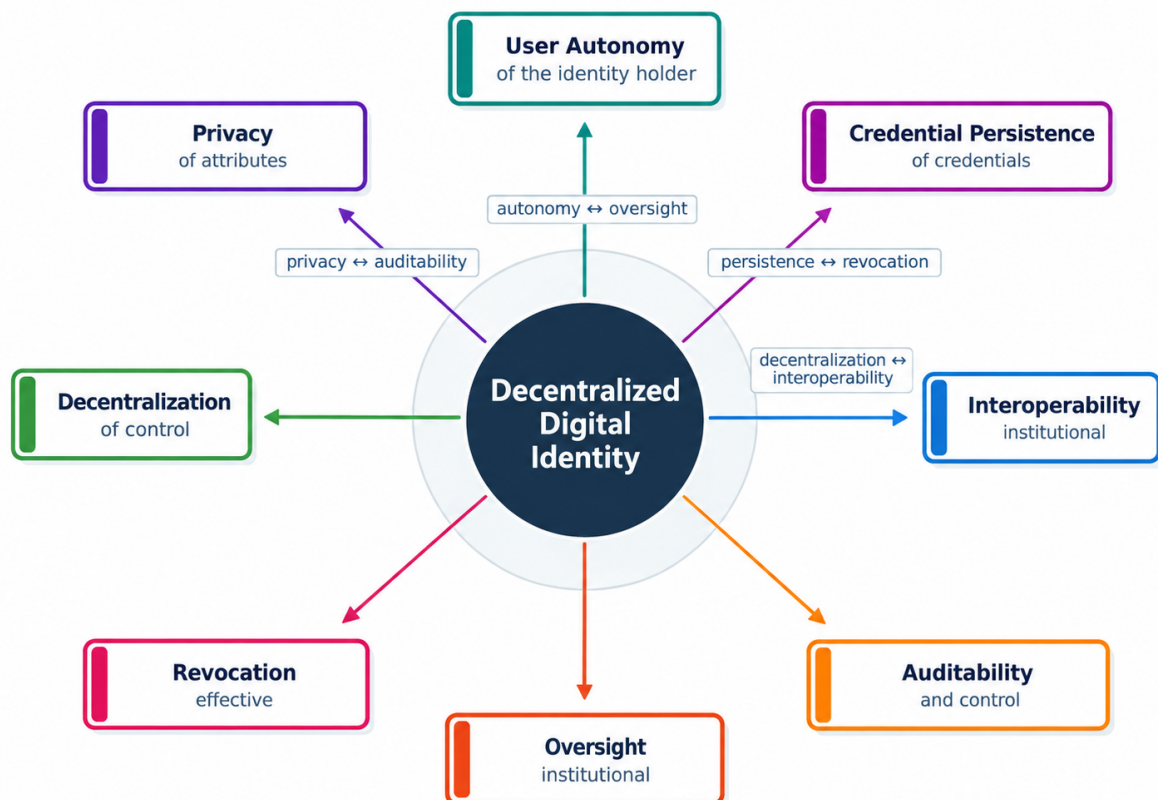
3.4 Regulatory frameworks and governance gaps

After examining how application domains introduce differentiated requirements, this subsection shifts the analysis toward the regulatory and governance conditions that come into play when solutions must operate among holders, issuers, verifiers, and institutions. At this level, the operation of decentralized digital identity incorporates issues related to consent, recognition between organizations, credential revocation, oversight, and the sustainability of security mechanisms. Lindquist [6] addresses the difficulties associated with the interoperability of consent mechanisms, while Bureaca et al. [7] propose unlinkable revocation lists for qualified electronic attestations, which addresses institutional integration in the context of eIDAS 2.0. This perspective is broadened by Lee et al. [26], who incorporate credential revocation and post-quantum preparedness, and by Chen et al. [30], who introduce oversight mechanisms into authentication processes. The presence of these components therefore makes it possible to differentiate the gaps according to the moment and function they serve within the ecosystem, from the verifiable expression of consent to the preservation of long-term security conditions, as organized in Table 6.

Tabla 6. Identified regulatory and governance gaps

Axis	Identified gap	Implication
Consent	Consent mechanisms with limited interoperability [6]	Difficulty in maintaining verifiable evidence of consent
Institutional interoperability	Uneven integration across infrastructures and jurisdictions [7]	Fragmented recognition of identities and credentials
Revocation	Need to invalidate credentials while preserving privacy [26]	Risk of invalid credentials remaining in the ecosystem
Oversight	Balance between anonymity, autonomy, and institutional control [30]	Difficulty in establishing acceptable accountability mechanisms
Future security	Still incipient incorporation of post-quantum mechanisms [26]	Risk of obsolescence of cryptographic mechanisms

The relationship between the gaps in Table 6 shows that their scope cuts across different functions of digital identity. Consent requires keeping verifiable evidence of a decision by the holder, but that evidence must be interpretable across different systems and organizations [6]; in turn, the recognition of a credential depends on issuers and verifiers sharing sufficient criteria to establish its validity [7]. Hence, revocation introduces another temporal condition, because a previously valid credential may lose that status and must be removed from the circle of trust without exposing additional information about its holder [26]. On top of these relationships comes oversight, which introduces the possibility of verifying certain actions without once again transferring full control of identity to a central authority [30]. In this way, autonomy, privacy, interoperability, and institutional control relate to one another at different moments in the life cycle of a credential, relationships represented in Figure 5.

**Figure 5.** Governance tensions associated with decentralized digital identity

The relationships represented in Figure 5 show that the attributes of decentralized identity are interdependent, so that decisions taken on one of them may generate new requirements on the others. This relationship can be seen in autonomy, whose increase reduces dependence on centralized providers, although it also requires mechanisms to deal with credential recovery, oversight, and the attribution of responsibilities [30]. A similar situation occurs with privacy, since limiting the exposure of information requires preserving the ability to verify the authenticity and validity of credentials, even when they must be revoked without enabling unnecessary correlations about the holder's activities [6, 26]. These conditions extend to interoperability, which, in addition to compatible formats and protocols, requires institutional criteria to determine who can issue, verify, accept, or revoke a credential [7], broadening the problem from the individual properties of the architecture to the relationships that must be established among the different actors involved in its operation.

Precisely when these relationships are no longer confined to a single environment and begin to involve actors from different domains, governance requirements become more complex. Deng et al. [4] illustrate this situation in fully decentralized scenarios in which multiple participants take part in verification processes, while Li et al. [5] incorporate the robustness conditions needed to sustain such interactions within distributed systems. Building on this, Chen et al. [30] address cross-domain authentication through oversight mechanisms that must coexist with privacy properties, which transforms a relationship initially centered on the holder and the verifier into a structure involving entities with differentiated capabilities and responsibilities. This diversification of actors in turn changes the way authentication, authorization, oversight, and recognition are distributed, making governance depend not only on who participates in the ecosystem, but also on the rules through which those responsibilities are articulated with the technological architecture.

The incorporation of these rules and responsibilities makes it possible to link governance with the dimensions examined previously, because the technological components and the mechanisms used to validate them acquire new conditions when transferred to scenarios involving multiple actors and institutions. A credential may be cryptographically verifiable and have shown adequate performance under experimental conditions, but its use across organizations may be limited by differences in recognition criteria, while a mechanism designed to preserve privacy may require additional procedures to manage consent and revocation. Similarly, a distributed architecture may reduce the involvement of certain intermediaries without eliminating the need to establish responsibilities for errors or misuse [28, 6, 7]. In this way, institutional conditions broaden the requirements identified during validation and deployment, extending them to the full cycle through which an identity is created, used, recognized, and eventually revoked.

When this life cycle is considered, the relationships between the four dimensions analyzed acquire greater continuity, since the distributed ledgers, decentralized identifiers, verifiable credentials, and privacy mechanisms identified in the technological dimension [3, 1, 23] perform functions that must later be validated and adapted to the conditions of each domain. DIDs make it possible to establish identifiers without necessarily depending on a central registry, although their use across environments requires common resolution and recognition mechanisms, while VCs facilitate the verifiable presentation of attributes and, as they circulate among different actors, give rise to needs related to their validity, acceptance, and revocation. These capabilities are complemented by privacy mechanisms that reduce the exposure of information without eliminating the possibility of verification and oversight [18, 28, 30], so that the decisions made in the technological architecture carry over to the forms of validation, the particular requirements of each domain, and the governance conditions involved in the implementation of decentralized digital identity.

4. Discussion

The findings of this review show that decentralized digital identity has achieved growing technical density, although its maturity as an integrated ecosystem remains partial. The field is no longer situated solely at the conceptual level of individual autonomy and presents architectures, prototypes, and sectoral applications based on blockchain/DLT, SSI, DID, VC, and ZKP. However, this evolution is not homogeneous. The distribution of the corpus reveals that the infrastructure intended to establish distributed trust has advanced faster than the mechanisms needed to turn it into a portable, recoverable, revocable, and insti-

tutionally recognizable identity. Ahmed et al. [3] position blockchain as a substrate for establishing trust among actors, while Mazzocca et al. [1] shift the problem toward interoperability between DID and VC. This distinction is fundamental, because having distributed, verifiable, and immutable ledgers does not in itself guarantee a functional sovereign identity. Therefore, the degree of technological decentralization is only part of the problem; the relevant question becomes how these technologies are articulated throughout the entire identity life cycle.

This need for articulation calls for a more cautious interpretation of a recurring premise in the literature, according to which greater decentralization would necessarily lead to greater user autonomy. The results of the review do not support such a direct relationship. The high presence of blockchain/DLT, compared with the comparatively lower incorporation of DID, VC, ZKP, and post-quantum cryptography, suggests that a significant share of proposals continues to focus on solving the trust infrastructure rather than comprehensive identity management. Although Cucko et al. [22] identify autonomy, portability, and privacy as essential properties of these systems, their fulfillment depends on mechanisms that allow them to be exercised under real conditions. A portable credential loses part of its usefulness if its revocation compromises privacy; likewise, individual control is limited when the loss of keys or devices has no secure recovery procedures. The gap observed therefore lies not only in the availability of technologies, but in their coherent integration across the processes of issuance, storage, presentation, verification, revocation, recovery, and auditing. Verifying whether that integration works outside scenarios designed by the developers themselves leads precisely to a second limitation of the field: the way in which solutions are being validated.

From this perspective, the predominantly engineering orientation identified in the corpus is both a strength and a limitation. The proliferation of frameworks, architectures, models, and prototypes demonstrates the ability to turn abstract SSI principles into technically implementable solutions. Likewise, works such as those by Pöhn et al. [10] and Naik et al. [25] show that the analysis of threats and vulnerabilities has reached a considerable degree of sophistication. Nevertheless, an architecture that is resistant to certain attacks is not necessarily robust from the perspective of the person who must use it. The scarcity of evaluations with real users reduces the available evidence on understanding of credentials, key management, trust, recovery from loss, response to errors, and accessibility. This shortcoming is especially important in SSI because some of the responsibilities traditionally assumed by centralized providers are transferred to the identity holder. Consequently, a solution that maximizes individual control without providing understandable recovery and support mechanisms may replace institutional dependence with technical complexity. This tension between autonomy and effective usability becomes even more relevant when solutions leave the laboratory and move into sectoral contexts with different users, risks, and regulatory requirements.

Indeed, the concentration of studies on IoT, health, and finance shows that adoption is advancing faster in areas where identity management responds to clearly identifiable operational needs, such as machine-to-machine authentication, the protection of sensitive information, or compliance with know-your-customer (KYC) procedures. Bai et al. [15] show the potential of ZKP to reduce information exposure in health contexts; Ahmed et al. [16] place SSI within financial processes subject to verification requirements; and Zhang et al. [20] extend these needs to 6G connectivity scenarios. These advances show that decentralized identity can add value when there is a clear relationship between problem, technology, and use case. However, the lower representation of government and e-ID reveals that this capability has not yet been transferred with the same intensity to spaces where identity acquires a citizenship dimension. This difference is not minor: success in financial, health, or cyber-physical environments demonstrates sectoral feasibility, but does not guarantee its application in public services, education, mobility, or cross-border administrative interactions. Extending the scope to these scenarios requires, in addition to technical interoperability, institutional recognition and common rules on responsibility, consent, and data protection, which places the discussion squarely on the regulatory level.

It is precisely in this dimension that the distance between technological capability and effective deployment becomes most evident. Lindquist [6] shows that consent requires verifiable and interoperable mechanisms, while Lee et al. [26] point out that revocation and preparedness for post-quantum scenarios continue to pose challenges. In turn, Bureaca et al. [7] propose, within the eIDAS 2.0 framework, mechanisms aimed at reducing linkability during the revocation of qualified attestations. Taken together, these works show

that privacy, consent, and revocation are not independent problems, but components of a single identity governance architecture. However, the corpus does not provide a widely accepted evaluation matrix that would make it possible to determine comparably the extent to which solutions meet the requirements associated with the GDPR and eIDAS 2.0. The practical consequence is significant: without verifiable compliance criteria, it is difficult to compare architectures, establish responsibilities, carry out audits, or build institutional trust for larger-scale adoption. Regulation should therefore not be understood as a layer added once technological development is complete, but as a design requirement that conditions from the outset the management of credentials, data, consent, revocation, and evidence of operations.

Based on these relationships, the results support the view that the main research frontier no longer lies exclusively in developing more sophisticated cryptographic mechanisms, but in the convergence of capabilities that have so far evolved at different paces. The maturity of decentralized digital identity requires articulating a technically interoperable architecture, sufficiently robust privacy and recovery mechanisms, empirical validation with diverse users, and auditable regulatory governance. This also implies reconsidering what “sovereign identity” means: it should not be reduced to the user controlling keys or credentials, but understood as their effective capacity to use, recover, and revoke them and to exercise rights over them within institutionally recognized ecosystems. From this perspective, privacy and oversight are not necessarily opposing objectives, provided that oversight is proportionate, traceable, and does not reintroduce unnecessary forms of centralization. The consolidation of the field will consequently depend on its ability to demonstrate that decentralization not only redistributes technological trust, but verifiably improves the autonomy, security, and inclusion of those who use digital identity. If this convergence is not achieved, the new infrastructures could reproduce the very problems that motivated the development of SSI, among them fragmentation, new dependencies, exclusion of vulnerable users, and difficulties in attributing responsibility for failures.

5. Conclusions

This systematic review characterized the state of digital identity technologies applied to secure authentication in decentralized ecosystems and reveals a technically dense field of asymmetric maturity. Blockchain remains the predominant trust substrate, on which decentralized identifiers, verifiable credentials, and zero-knowledge proofs are consolidating as the core of an architecture oriented toward authentication with minimal disclosure. However, research retains a markedly engineering profile, with little validation in real deployments and with users. In addition, it is concentrated on the internet of things, health, and finance, while government, education, and cross-border services remain underrepresented. Moreover, frameworks such as the GDPR and eIDAS 2.0 have permeated the discourse more than the design of systems, and verifiable consent, unlinkable revocation, and proportionate oversight remain unresolved in an integrated manner. The main contribution of the study is to shift the maturity criterion from the technical feasibility of components to the complete life cycle of the credential. Sovereignty should therefore be understood as the holder’s effective capacity to use, recover, and revoke their credentials in institutionally recognized ecosystems, and not as mere control of keys. The future agenda calls for developing auditable regulatory compliance matrices, revocation mechanisms compatible with the post-quantum transition, longitudinal studies with diverse users, and pilots in public electronic identity. Only then will decentralization be able to consolidate itself as a legitimate trust infrastructure, rather than as a redistribution of the dependencies it sought to overcome.

Author Contribution. The authors confirm their contribution to the article as follows: conceptualization, M.C.C. and E.T.G.; methodology, M.C.C. and E.T.G.; investigation, M.C.C. and E.T.G.; formal analysis, M.C.C. and E.T.G.; writing – original draft preparation, M.C.C. and E.T.G.; writing – review and editing, M.C.C. and E.T.G.; visualization, M.C.C. and E.T.G. All authors reviewed the results and approved the final version of the manuscript.

Acknowledgments. To the Universidad Tecnológica del Perú for the institutional support provided for the development of this research.

Funding. This study was self-funded by the authors.

Informed Consent Statement. Not applicable, since the study did not involve human participants.

Data Availability Statement. The Scopus record export, the screening matrix, and the extraction and coding matrix of the 23 studies in the corpus are available upon request from the corresponding author.

Conflicts of Interest. The authors declare no conflicts of interest.

Statement on the Use of Artificial Intelligence. Generative artificial intelligence tools were used exclusively to support text editing and typesetting. The analysis, interpretation of the results, and conclusions are the exclusive intellectual responsibility of the authors, who validated and approved the final version.

References

- [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 .