frontiers | Frontiers in Blockchain

TYPE Original Research
PUBLISHED 03 December 2025
DOI 10.3389/fbloc.2025.1696955

OPEN ACCESS

EDITED BY
Roben Castagna Lunardi,
Federal Institute of Rio Grande do Sul (IFRS), Brazil

REVIEWED BY
Chengzu Dong,
Lingnan University, Hong Kong SAR, China
Musawer Hakimi,
Osmania University, India

*CORRESPONDENCE
Sangmi Chai,
smchai@ewha.ac.kr

RECEIVED 01 September 2025
REVISED 04 October 2025
ACCEPTED 31 October 2025
PUBLISHED 03 December 2025

CITATION
Hwang H, Park M, Oh H and Chai S (2025) Towards a refined architecture for socio-technical decentralized identity services. *Front. Blockchain* 8:1696955. doi: 10.3389/fbloc.2025.1696955

Towards a refined architecture for socio-technical decentralized identity services

Hwajeong Hwang[1], Minjung Park[2], Hyunyoung Oh[3] and Sangmi Chai[4]*

[1]Department of Business Administration, Ewha Womans University, Seoul, Republic of Korea, [2]Department of Business Administration, Kumoh National Institute of Technology, Gumi-si, Republic of Korea, [3]Department AI Software, Gachon University, Gyeonggi-do, Republic of Korea, [4]Department of Business Administration, Ewha Womans University, Seoul, Republic of Korea

The accelerating adoption of artificial intelligence, together with escalating incidents of identity theft, account hacking, and large-scale personal data breaches, is driving a global shift toward secure, user-centric identity management systems. Blockchain-based Decentralized Identity (DID) services, grounded in the principles of Self-Sovereign Identity (SSI), are increasingly recognized as a foundational technology for safeguarding personal data and enabling user-controlled identity management. However, existing DID research and implementations remain predominantly technology-focused, often overlooking socio-technical factors such as governance, usability, operational effectiveness, and stakeholder trust. To address this gap, this study proposes an STS-based (Socio-Technical Systems) framework to guide the practical and scalable adoption of DID services, integrating both social components (e.g., governance, sustainability, user-centric design) and technical components (e.g., decentralization, privacy preservation, interoperability, security). Using an integrative research review methodology, the framework was developed through systematic analysis of global standards, industry cases, and academic literature, and was further refined and validated through multidisciplinary expert consultation. Building on this framework, we introduce a Refined DID Service Architecture optimized for enterprise-level deployment, incorporating privacy-preserving mechanisms at the infrastructure level, consensus-based governance, and standardized UI/UX guidelines. The proposed architecture addresses key barriers to adoption--such as interoperability gaps, regulatory inconsistencies, and limited user engagement--while ensuring scalability and compliance with global standards. This study contributes to both theory and practice by (1) framing DID as a socio-technical system, (2) providing an actionable evaluation framework for developers, regulators, and service providers, and (3) offering a globally adaptable architecture that balances technological robustness with social acceptance, thereby supporting the broader diffusion of DID services in real-world ecosystems.

KEYWORDS

blockchain, decentralized identity (DID), digital identity, DID ecosystem, self-sovereign identity (SSI), socio-technical systems (STS)

1 Introduction

Digital identity systems are rapidly becoming a critical component of digital economies, enabling secure authentication, trusted transactions, and cross-border service delivery. Yet, the global surge in identity theft, account hacking, and large-scale personal data breaches has exposed the vulnerabilities of conventional, centralized identity models (Gartner, 2024). In response, Decentralized Identity (DID)—particularly blockchain-based implementations aligned with the Self-Sovereign Identity (SSI) paradigm—has emerged as a promising solution for enhancing privacy, user control, and interoperability.

Governments and industry leaders are actively pursuing DID initiatives. The European Union is deploying the EUDI Wallet under eIDAS 2.0 to provide digital credentials to all citizens by 2026 (EUDI, 2024a), while U.S. states such as New York are piloting mobile driver's licenses (mDL) with a focus on interoperability (Hochul, 2024). However, adoption remains uneven: in South Korea, despite a government-led launch of mobile ID cards in 2022, uptake remains limited to four million users, hindered by complex issuance procedures, limited use cases, and insufficient public awareness (Policy Briefing, 2024).

More critically, current DID deployments tend to emphasize technical design—ledger structures, cryptographic protocols, and credential formats—while neglecting socio-technical dimensions such as governance frameworks, regulatory alignment, user experience, and trust-building mechanisms (Satybaldy et al., 2024). This gap is significant: without integrating social, organizational, and institutional factors, DID systems risk poor adoption, interoperability failures, and erosion of public trust (Beduschi, 2021; Norman, 2016).

To address this challenge, we adopt the Socio-Technical Systems (STS) theory as a guiding lens. STS theory emphasizes the interplay between technological infrastructure and social context, highlighting that sustainable innovation requires the alignment of technical robustness, governance adaptability, and user-centric design. By conceptualizing DID services as socio-technical systems, this study bridges the divide between technology-driven models and socially sustainable deployment strategies.

The objectives of this study are threefold:

1. To develop a comprehensive STS-based framework for the practical and scalable adoption of DID services.
2. To identify the architectural challenges—both technical (e.g., interoperability, decentralization trade-offs) and social (e.g., governance, trust, policy)—that impede implementation; and
3. To propose an improved DID service architecture that balances scalability, usability, and privacy protection in alignment with the derived framework.

To address this objective, the study poses the following research questions:

Research Question 1. What socio-technical framework can facilitate the practical implementation and scalable adoption of decentralized identity (DID) services, grounded in Socio-Technical Systems (STS) theory?

Research Question 2. What social and technical architectural challenges arise in implementing DID-based decentralized identity services within the proposed socio-technical framework?

Research Question 3. How can the DID-based decentralized identity authentication ecosystem be architecturally improved to ensure scalability, enhance usability, and protect data privacy, in alignment with the socio-technical framework derived from this study?

To answer these questions, this study employs an integrative research review methodology, synthesizing existing global frameworks, academic literature, and industry case studies related to decentralized identity. Based on STS perspective, the study derives a structured evaluation framework that captures both social and technical dimensions. A refined DID service architecture is proposed through iterative design grounded in this framework, and its validity is verified through expert review by professionals in blockchain, security, and DID domains. This study makes the following key academic and practical contributions. First, it conceptually advances the understanding of DID services by framing them as socio-technologies, moving beyond purely technical perspectives to highlight the dynamic interplay between technological systems and social structures. Second, it proposes a realistic evaluation framework and system architecture that address practical constraints such as interoperability and governance adaptability, enhancing feasibility for enterprise-level deployment. Third, it provides actionable policy and design insights for developers, regulators, and service providers seeking to implement secure and user centric DID systems. The remainder of this paper is organized as follows. Chapter II provides the theoretical foundation by introducing Socio-Technical Systems (STS) theory as the conceptual lens for understanding DID services and systematically examines both social components (user-centricity, mutual trust, governance, and sustainability) and technical components (decentralization, privacy preservation, interoperability, and security) that constitute DID ecosystems. Chapter III presents the research methodology, detailing the five-stage integrative research review process encompassing problem formulation, data collection from global frameworks and academic literature, data assessment, framework development and expert validation, and analysis procedures. Chapter IV presents the research results, introducing the Proposed Refined DID Service Architecture with its four-layer structure, validation through mobile driver's license (mDL) case analysis, and comprehensive responses to the three research questions. ChapterV discusses the study's implications from technological, market, and policy perspectives, offering actionable recommendations for enterprise-level DID deployment and ecosystem expansion. Finally, Chapter VI concludes by synthesizing the key contributions, acknowledging research limitations, and proposing directions for future research including empirical validation and integration with emerging Web3 and AI technologies.

2 Theoretical background

2.1 Socialtechnologysystemtheory

DID services are not simply technologies that store "digital identity information," but rather large socio-technical

systems(STS) in which various stakeholders, such as users, issuing agencies, government and financial institutions, and regulatory authorities, interact with each other. Digital identity platforms operate in complex fields where various actors, interests, and technologies coexist and interact (Beduschi, 2021). The STS theory perspective is based on the premise that "technology does not develop in isolation but evolves and develops alongside social factors," and it points out that emphasizing technology alone can lead to significant failures during actual implementation. Chai and Kim support the findings of Davenport and Prusak, highlighting that emphasizing only the technical elements in an STS can result in severe failures (Chai and Kim, 2012). According to Davenport and Prusak, organizations generally regard technological infrastructure as the most essential element, leading them to focus solely on the technical aspects of a system during its implementation (Chai and Kim, 2012; Davenport and Prusak, 1998). This means that if technology does not consider the interaction between social or environmental factors, it may fail to achieve its original purpose or, in some cases, lead to serious situations if its original purpose is distorted or misused. From this perspective, preliminary research on SSIs has revealed that system users frequently encounter difficulties with fundamental concepts, such as the management of data, the acceptance of credentials, and the navigation within digital wallets. This phenomenon is primarily attributable to the absence of user-centric design and inadequate guidance (Khayretdinova et al., 2023).

2.2 Key elements of DID services from an STS perspectives

From an STS perspective, the sustainable expansion of DID services within broader ecosystems depends on the continuous evolution and development of both social and technological components through iterative interactions with societal demands and user requirements.

2.2.1 Socio components of STS in DID services

Through prior research, it has been confirmed that DID services, when approached through the STS framework, are socially significant components characterized by user-centricity, mutual trust, governance, and sustainability.

- User-Centric: Guaranteed privacy rights, usability, and accessibility, transparency, and trust
- Mutual Trust: System availability, stability, integrity, transparency, and consensus-based trust registry
- Governance: Compliance with laws and regulations, accountability, risk management system
- Sustainability: Efficiency in terms of economic and environmental costs, scalability, and inclusiveness

Firstly, when considering DID services from a social perspective, the user perspective should be prioritized as the foremost consideration. According to Donald Norman, the founder of cognitive science and user experience (UX), "user-centricity" is at the core of all STS (Norman, 2016). Systems used by general users should be designed to be more easily accepted and provide greater value to stakeholders (Baxter and Sommerville, 2011). DID services are provided to general users as apps, allowing them to store their identity/credentials on their mobile devices and submit only the minimum required information when needed. The visible form of DID services, where control over issuers and verifiers is transferred to users (Preukschat and Reed, 2022), is a digital wallet in the form of an app. Therefore, the app of a decentralized identity verification service will provide users with trust in terms of data privacy protection by allowing them to confirm the basic details of what information is being submitted and utilized. Additionally, consistent user experience when moving to similar services is important. This study suggests that the social factors of DID services should be user-centric, with a user-friendly UI/UX that provides an intuitive and seamless experience. According to research by Statybaldy et al., the importance of developing user-friendly solutions from the user's perspective is emphasized as one of the challenges of SSI systems (Satybaldy, Ferdous, and Nowostawski, 2024), which supports this study.

Secondly, according to the World Economic Forum (WEF), which addresses global economic conditions and business collaboration agendas, in the digital identity ecosystem, "Mutual Trust" is defined as a set of commonly accepted definitions, principles, rules, and standards (including laws, standards, and principles for the ecosystem) that organizations within the ecosystem agree to follow (Forum, 2021), emphasizing the importance of trust.

Thirdly, Dixon (2019) of the World Privacy Protection Association asserts that "governance" is a pivotal yet frequently disregarded component in the management of the digital identity ecosystem. This assertion underscores the imperative for the establishment of comprehensive legal and policy safeguards prior to the implementation of a digital identity ecosystem. The absence of centralized control over decentralized identity services necessitates the establishment of an effective governance framework to ensure stable operation and sustained development. This is because the involvement and collaboration of various stakeholders are essential prerequisites, resulting in a greater necessity for established rules concerning the operation of services and systems, methods for resolving disputes, and guidelines for changes and upgrades, including compliance. Dixon (2019) of the World Privacy Protection Association asserts that "governance" is a pivotal yet frequently disregarded component in the management of the digital identity ecosystem. This assertion underscores the imperative for the establishment of comprehensive legal and policy safeguards prior to the implementation of a digital identity ecosystem. The absence of centralized control over decentralized identity services necessitates the establishment of an effective governance framework to ensure stable operation and sustained development (NETZPOLITIK.org, 2024). This is because the involvement and collaboration of a range of stakeholders are essential, thereby increasing the necessity for established guidelines regarding alterations and enhancements, encompassing operational protocols for services and systems, methods for resolving disputes, and regulations concerning compliance. In this regard, Goodell proposed the establishment of protocols that facilitate interaction among various stakeholders, drawing parallels with the SWIFT open standard that has gained prominence in the financial sector (Goodell, 2019). In accordance with the SSI framework, Trust Over IP (ToIP) signifies a shift in focus from

machines and technology to people and policy, thus playing a pivotal role in both technology and governance within the SSI stack. Governance may be defined as a conduit between pragmatic considerations pertaining to business, legal and social requirements.

Lastly, one of the crucial social factors within ecosystem governance is "sustainability." Korhonen (2004) advanced the argument that, within the context of a strategic sustainable development model, industrial ecology can be strategically applied by fostering diversity, interdependence, connectivity, and cooperation within the ecosystem, thereby engendering sustainability analogous to that observed in natural ecosystems. Norman defined STS as a complex system of technologies, people, and human behavior, emphasizing robustness and resilience centered on sustainability (Norman, 2016). According to Norman, sustainability in STS refers to the ability to self-recover when damaged, with minimal negative impacts due to the interconnectedness of all members of society. The ID4D (Identification for Development) initiative, which aims to ensure the right to identity and access to services and economic opportunities for all, is promoting an inclusive and trustworthy ID system with a focus on long-term financial and operational sustainability (WorldBank, 2024).

2.2.2 Technical components of STS for decentralized identity services

In order to identify the technical components of a decentralized identity verification service, we first confirmed the design objectives of DID and VC, which are the implementation technologies. The design of DID and VC can be summarized into four categories: "decentralization by eliminating dependence on central authorities," "user privacy protection," "security through encryption," and "interoperability." Previous studies have also confirmed that decentralization, privacy preservation, security, and interoperability are important technical components of DID services based on the STS approach, which eliminates dependence on central authorities (Kim et al., 2023).

- Decentralization: A decentralized network structure that does not depend on central authorities.
- Privacy Preserving: Minimization of personal information exposure, selective disclosure, censorship resistance
- Interoperability: Ability to connect with various platforms and institutions, standard-centric design
- Security: Encryption algorithms, authentication systems, access control, internal security processes

Regarding "decentralization," Kemppainen et al. (2023) identified practical limitations. Specifically, since all social infrastructure is currently designed around identity systems dependent on central authorities, transitioning to a decentralized digital identity ecosystem raises questions about its practicality. Specifically, a study examining the development and transfer of eID technology in the context of a public-private partnership in Finland, through a STS perspective, confirmed that society cannot avoid having some central components, and thus theoretical solutions cannot be limited to a single identity. The study proposed a hybrid solution combining elements of centralized ID models with peer-to-peer (P2P) solutions among users (Kemppainen et al., 2023). According to Satybaldy et al., who studied the challenges of SSI system DID service expansion, among the complex technical, legal, and social challenges, they pointed out the limitations of decentralized networks regarding the complexity of decentralized network structures and consensus mechanisms (Satybaldy et al., 2024). These include potential vulnerabilities within blockchain networks for decentralization, performance issues in public networks due to their permissionless nature, scalability limitations of private blockchains, and unresolved trust governance issues when recording public keys in ledger-based DIDs. This study aims to examine these issues using actual implemented architecture cases (Kemppainen et al., 2023; Satybaldy et al., 2024).

"Privacy protection" refers to the collection of personal information based on user consent and the principle of data minimization, ensuring that only necessary information is collected. It also grants users detailed control over the data shared and the recipients of such data, along with clear explanations of how the data is used and protected, thereby requiring transparency in the system (EUDI, 2024a; Guzmán-Castillo et al., 2024; Dib and Toumi, 2020). The Open Wallet Foundation uses the term "Privacy Preserving" (Graham, 2023), which means that users can control their personal data and digital identity information and selectively disclose them only when necessary. Therefore, this study also adopts the term "Privacy Preserving" as a technological component from the STS perspective (EUDI, 2024b; Guzmán-Castillo et al., 2024; Dib and Toumi, 2020; Graham, 2023). Similar approaches have also been demonstrated in UAV communication systems: Dong et al. (2021) proposed a blockchain-aided self-sovereign identity framework for edge-based UAV delivery systems, illustrating how token-based identifiers, verifiable credentials, and decentralized coordination can protect user data and ensure resilience under dynamic edge conditions. More recently, Dong et al. (2024) presented a blockchain-based SSI system for Know-Your-Customer (KYC) processes, showing how selective disclosure and credential governance mechanisms enable privacy-preserving compliance in regulated environments. Building on these lines of work, Dong et al. (2025) proposed a privacy-aware task distribution architecture that employs token-based identifiers and decentralized coordination to ensure privacy and resilience under dynamic conditions. Their design heuristics—privacy-aware access tokens, selective disclosure, credential governance, and fallback mechanisms—provide relevant insights for strengthening privacy-preserving architectures in DID services.

"Security" can be broadly defined as providing sufficient security to enable requesters to rely on DID documents for the level of assurance they need in decentralized identity services (W3C 2022), as well as identifying and mitigating potential vulnerabilities throughout the design process (Nicolae and Alexandrescu, 2024; W3C, 2022; Nicolae and Alexandrescu, 2024). This includes encryption algorithms, authentication systems, access control mechanisms, and internal security processes. Similar security-oriented approaches have also been applied in decentralized identity frameworks for edge environments. For example, Dong et al. (2021) proposed a blockchain-aided self-sovereign identity framework for edge-based UAV delivery systems, incorporating verifiable credentials, cryptographic authentication, and

distributed trust coordination to ensure secure and resilient operations under dynamic edge conditions. Their design heuristics—combining encryption, access control, and decentralized verification—offer practical insights for strengthening the security dimension of DID services.

"Interoperability" remains a significant challenge confronting the worldwide dissemination of decentralized identity (DID) services pertain to the absence of interoperability. The question of whether technical implementations differ between countries and platforms is a subject of ongoing research. This has resulted in a fragmented identity ecosystem, where identity credentials issued on one platform cannot be properly recognized or utilized on other platforms. Differences in technical implementations between countries and platforms have produced a fragmented identity ecosystem where credentials issued on one platform cannot be properly recognized or utilized on another. Inconsistencies in protocols, data schemas, credential formats, and verification methods further exacerbate this bottleneck (W3C, 2022).

In this regard, prior work has explored how blockchain-enabled self-sovereign identity models may help mitigate interoperability challenges in regulated domains. For example, Dong et al. (2024) presented a blockchain-based SSI system for Know-Your-Customer (KYC) processes, illustrating how tokenized credentials, selective disclosure, and registry-based governance mechanisms can support aspects of privacy-preserving compliance and improve prospects for controlled interoperability across multiple stakeholders. Likewise, Dong et al. (2020) introduced BBM, a blockchain-based self-sovereign identity model for open banking that integrates credential issuance, revocation, and governance to achieve auditability and regulatory compliance. While these studies do not fully resolve interoperability, they offer concrete architectural patterns and proof-of-concept insights that inform efforts to overcome the interoperability bottlenecks currently impeding the expansion of DID ecosystems.

The fundamental cause of this bottleneck is the presence of inconsistencies in protocols, data schemas, credential formats, and verification methods. Whilst there are DID solutions which are unequivocally compliant with W3C international standards, there are others which rely on proprietary extensions or network-based approaches. It is evident that the interpretation and application of verifiable credential (VC) generation methods, storage methods and locations, DID methods, and encryption methods vary considerably. This poses a significant challenge to interoperability. Moreover, the absence of a cohesive governance framework, encompassing trust frameworks and issuer registries, further exacerbates interoperability challenges (W3C, 2022). As Yildiz et al. (2023) have highlighted, various DID service implementations have emerged in recent years based on the SSI paradigm, some of which utilize different underlying technologies. These technical discrepancies frequently result in interoperability impediments between software applications across disparate implementations. While this is a common issue, there is no shared understanding of interoperability in the context of self-sovereign identity Mühle et al. (2018).

While international organizations such as the Decentralized Identity Foundation (DIF), Trust Over IP (ToIP), and W3C Credentials CG are working to ensure interoperability, a practical solution is difficult without not only technical standardization but also legal and institutional consistency and policy coordination. In this regard, prior work demonstrates how blockchain-enabled SSI modesls can help address interoperability challenges across different domains. Fore example, Dong et al. (2021) proposed a blockchain-aided SSI framework for edge-based UAV delivery systems, showing how token-based identifiers and decentralized coordination can maintain privacy and operational resilience in dynamic edge environments. More recently, Dong et al. (2024) introduced a blockchain-based SSI system for Know-Your-Customer (KYC) processes, illustrating how selective disclosure and registry-based governance mechanisms enable privacy-preserving compliance across multiple stakeholders. Likewise, Dong et al. (2020) introduced BBM, a blockchain-based self-sovereign identity model for open banking, which integrates tokenized credentials and registry governance to achieve privacy, auditability, and regulatory compliance. Collectively, these studies highlights architectural patterns—credential issuance, revocation selective disclosures, and decentralized governance that support controlled interoperability in multi-stakeholder ecosystems, offering a practical reference for DID-based identity frameworks.

The present study builds on these insights to examine why interoperability remains a key bottleneck in the expansion of the DID ecosystem. This fragmentation creates strong dependencies on specific vendors or platforms, which runs counter to the core values of autonomy and mobility that DIDs are designed to promote. For businesses and government agencies, the absence of structural compatibility presents a significant challenge, impeding the process of integration and constraining the scope of mutual verification when seeking to employ external credentials.

In summary, the basis for DID services to continue expanding within the ecosystem as a useful technology-based service is that, from the STS perspective, socio and technological components can evolve and develop through repeated interactions with the demands of members of society.

3 Research methodology

The methodology of this study followed five sequential stages, as illustrated in (Figure 1) Integrative Research Review Methodology, (Cooper, 1982) in accordance with the Integrative Research Review approach: 1. Problem Formulation, 2. Data Collection, 3. Data Assessment, 4. Data Analysis, and 5. Results and Discussion. This phased and integrated research process was designed to develop a refined DID service architecture.

In the first stage, Problem Formulation, the scope, and purpose of the study were defined, clear research questions were established, and the overall direction of the analysis was determined.

The second stage, Data Collection, involved gathering a comprehensive set of resources, including global frameworks, academic literature, industry reports, and unpublished materials related to digital identity and SSI.

In the third stage, Data Assessment, the collected information was systematically organized to identify relevant design principles and the social and technical components of DID services. This assessment included an in-depth review of the status and requirements for DID deployment, leading to the initial formulation of a socio-technical framework.

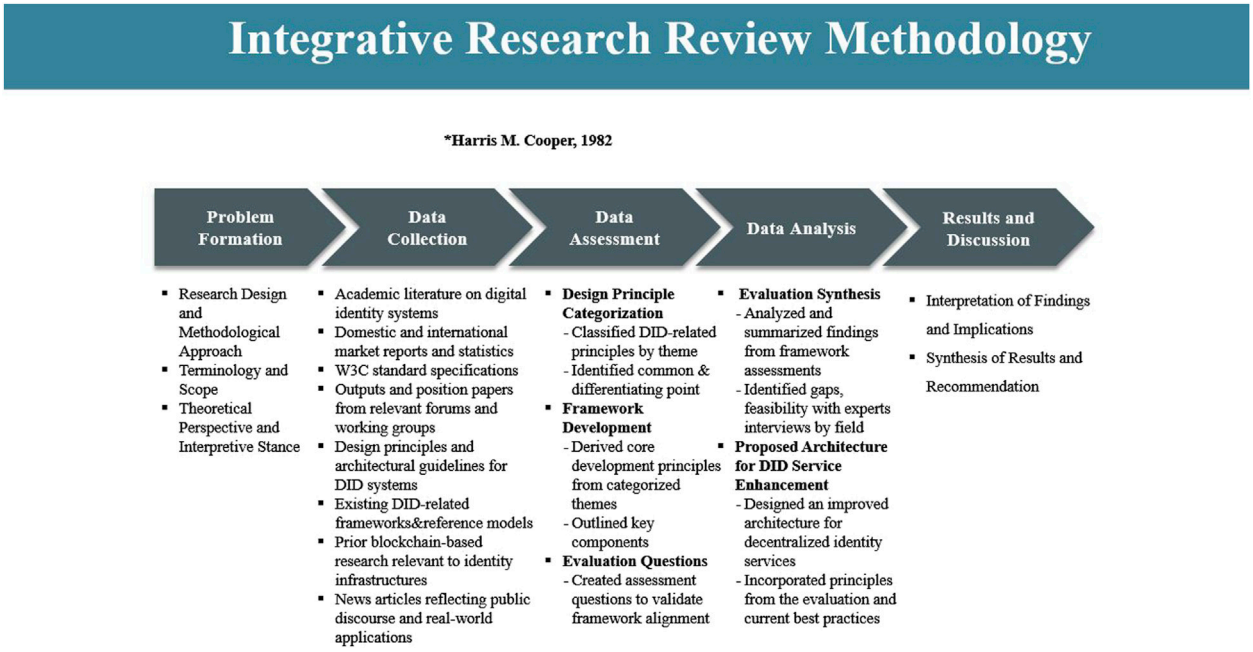

FIGURE 1
Integrative Research Review Methodology: The methodology adopted in this study is illustrated.

The fourth stage, Data Analysis, applied the derived framework to design enhanced architecture for DID services. The framework was structured to include evaluation principles, components, and assessment questions. Its validity was confirmed through expert reviews from specialists in blockchain, DID, and security.

Finally, in the Results and Discussion stage, key findings were synthesized, their policy and practical implications were discussed, and the study's limitations and directions for future research were proposed.

3.1 Problem formulation

This study defines the research problem from two complementary perspectives: technical and social. From the technical perspective, it addresses challenges related to data privacy protection and the establishment of secure, interoperable DID services. From the social perspective, it examines the current state of DID service adoption and identifies factors influencing the expansion of the broader decentralized identity ecosystem.

3.2 Data collection

3.2.1 Multi-source data collection framework

To ensure both conceptual rigor and practical applicability, data collection was systematically organized across five complementary categories. This multi-source approach enabled comprehensive coverage of the decentralized identity (DID) domain while aligning with real-world implementation requirements.

1. Prior Research on Architecture–Reviewed academic literature on digital identity architecture using Google Scholar, focusing on search terms such as "Decentralized Identity," "DID Architecture," "Blockchain-based Identity Management," and "SSI". The review targeted publications from 2019 onward, following the establishment of the W3C's Verifiable Credential (VC) standard.
2. Frameworks for Decentralized Identity Verification–Collected representative frameworks including Trust Over IP (ToIP), the Architecture and Reference Framework (ARF) for the EUDI Wallet, the Open Wallet Foundation Framework, and national frameworks from countries such as the UK and France.
3. Standards and Open-Source Platforms–Reviewed materials from international standardization bodies such as W3C, as well as global open-source platforms including GitHub. References included W3C specifications, mDL standard documents, the Decentralized Identity Foundation (DIF), the Open Wallet Foundation, Hyperledger Indy, Aries, and AnonCreds.
4. Industry and Policy Reports–Collected reports from consulting firms (e.g., Gartner, Deloitte), as well as documents from the World Economic Forum, the World Privacy Forum, and various SSI-related publications.
5. Domestic Sources and Market Data–Reviewed press releases and websites of domestic public institutions, news articles, market trend data related to identity verification, research institution reports, corporate materials, and other gray literature.

By synthesizing these five categories, the proposed DID framework was designed to be theoretically robust while also reflecting socio-cultural, institutional, and technical diversity. Importantly, the framework and architecture design were

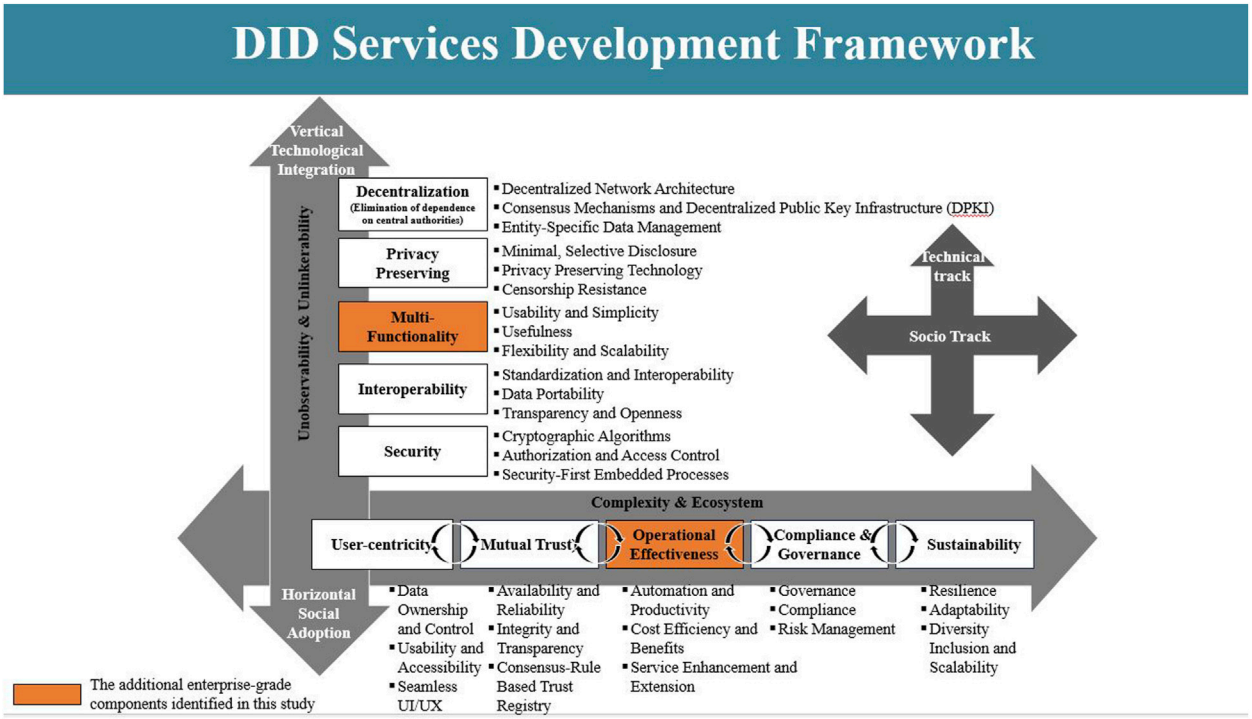

FIGURE 2
DID (Decentralized Identity Service) Development Framework: Development Framework Proposes a framework derived and validated from prior research and expert interviews.

constructed on the basis of publicly available data. By clearly distinguishing the role of public and restricted sources, the study ensures both transparency and reproducibility.

3.3 Data assessment

3.3.1 Development of a framework for DID services

This study proposes a DID service framework, as illustrated in (Figure 2) DID Service Development Framework, developed with reference to multidisciplinary design principles and prior literature on decentralized identity verification.

The framework comprises two main dimensions: socio components and technical components. The socio components, positioned along the horizontal axis, emphasize factors that facilitate broad social adoption and diffusion. The technical components, positioned along the vertical axis, address technical diversity and depth required for robust system implementation.

The distinction between these two dimensions is essential because they capture fundamentally different but complementary conditions for adoption. Socio components focus on trust, governance, and legitimacy that determine acceptance and diffusion in institutional contexts, whereas technical components ensure privacy preservation, scalability, and interoperability that guarantee the reliability of implementation. By treating them as separate yet interdependent dimensions, the framework systematically accounts for both institutional and technological requirements, avoiding reductionist explanations and ensuring a balanced socio-technical perspective.

By integrating these two dimensions, the framework highlights the multiple challenges—technical, social, and institutional—that must be addressed to enable the successful real-world deployment of the DID services.

3.3.2 Socio components

The socio components aim to promote horizontal service diffusion and are derived from five core principles: user-centricity, mutual trust, operational effectiveness, compliance and governance, and sustainability.

While user-centricity, mutual trust, compliance, and sustainability are widely recognized in existing trust frameworks, operational effectiveness has received less attention. Omar (Dib and Toumi, 2020) emphasizes that operational effectiveness should include considerations such as transaction costs and payment mechanisms, which are critical for service scalability and adoption. To address this gap, this study incorporates operational effectiveness as a distinct socio component, thereby adding a novel element not found in most existing frameworks. The detailed definitions of each component are provided in (Table 1) Socio Components and Details.

Within the social perspective, we introduce operational effectiveness as a novel component. While prior studies have emphasized user-centricity, trust, governance, and sustainability, recent scholarship highlights that operational effectiveness is socially embedded in blockchain-based identity services. Governance research shows that blockchain mechanisms directly shape coordination and efficiency in socio-technical networks (Beck and Kranz, 2020; Schletz and Fischinger, 2021), and that governance arrangements provide mechanisms for effective

TABLE 1 Socio components and details: It shows the socio components extracted based on previous studies and literature review.

Socio components	Attributes and definition(in details)	References
User-Centricity	① Data Ownership and Control Users must retain explicit control over their personal data, including the ability to verify which information has been shared, and to provide such data based on informed and transparent consent	EUDI Wallet SSI Principles SSI Digital Wallet STS DesignPrinciples WEF Digital Identity Ecosystem Deloitte Digital ID Ecosystem (Dib and Toumi, 2020) Kuperberg, (2020) Satybaldy, Ferdous, and Nowostawski, (2024)
	② Usability and Accessibility Users should be able to access the service without discrimination, and the service must deliver convenient, valuable, and contextually relevant experiences	
	③ Seamless UI/UX The user interface and overall experience should be optimized for user-centric interaction across the entire service journey, ensuring contextually relevant and seamless integration with diverse service environments	
Mutual Trust	① Availability and Reliability Identity and credential interactions must remain consistently available and reliably delivered. Even in cases where an issuer is decommissioned, credentials must retain their validity within the defined time frame	ToIP Framework Trust Registry Query Protocol Specification V2.0 (ToIP 2024) WEF Digital Identity Ecosystem STS Design Principles Deloitte Digital ID Ecosystem (Ertresvag, 2024) Lim et al. (2022)
	② Integrity and Transparency The risk of identity credential forgery or misuse must be eliminated through secure handling and verification mechanisms. The system must operate within a transparent governance structure supported by clear legal protections.	
	③ Consensus-Based Trust Registry Trust between credential holders and verifying service providers must be anchored in a consensus-based trust registry, where verification is governed by shared and secure validation rules among trusted entities	
Operational Effectiveness	① Automation and Productivity Manual processes related to identity issuance and verification—such as mobile app and web service development—should be automated to enhance operational efficiency and overall productivity	WEF Digital Identity Bochnia (2023) Kuperberg (2020) Dib and Toumi (2020) Chu (2022) Glöckler et al. (2023)
	② Cost Efficiency and Benefits Service operations should pursue total cost of ownership (TCO) benefits through the utilization of public infrastructure as utilities and the development of sustainable business models by private and stakeholder entities	
	③ Service Enhancement and Extension The system should continuously monitor and improve the user experience, evolving into an extensible service ecosystem that users are willing to pay for	
Compliance and Governance	① Governance Governance includes collectively agreed-upon definitions, principles, policies, and procedures endorsed by all participants in the digital identity ecosystem. This encompasses system operation rules, dispute resolution mechanisms, upgrade procedures, clearly defined roles and responsibilities, and audit requirements	WEF Digital Identity OWF Safewallet ToIP Framework WPF Safewallet (Robels-Carrillo, 2024; Nicolae and Alexandrescu, 2024) Wang et al. (2023) Bochnia et al. (2024) Bauer et al. (2023) Satybaldy, Ferdous, and Nowostawski, (2024)
	② Compliance Compliance ensures that operational rules and regulatory requirements are enforceable, effectively monitored, and supported by a defined hierarchy of sanctions	
	③ Risk Management Risk management involves the identification, assessment, and mitigation of potential risks, supported by clear accountability, transparency, and strategic safeguards	

(Continued on following page)

TABLE 1 (*Continued*) Socio components and details: It shows the socio components extracted based on previous studies and literature review.

Socio components	Attributes and definition(in details)	References
Sustainability	① Resilience The system must be equipped with resilience and preparedness mechanisms to enable rapid recovery from crises such as natural disasters, cyberattacks, and data breaches	STS Design Principles Journal of the Korea Information Processing Society, Vol. 31, No. 3, September 2024ID Principles.org (Wang et al., 2023) Satybaldy, Ferdous, and Nowostawski, (2024) Bauer et al. (2023)
	② Adaptability Organizational and procedural structures should support sensing of emerging technologies, integration of new service models, and proactive adaptation to evolving digital identity environments and market dynamics	
	③ Diversity Inclusion and Scalability The system should embrace diversity and scalability by extending core services across heterogeneous industries and supporting various methods of authentication and verification to ensure long-term sustainability	

service delivery in decentralized environments (Lumineau et al., 2021).

Empirical studies further support this dimension, showing that blockchain applications improve automation and productivity (Bai, 2024), enhance cost efficiency in public services (Shahaab et al., 2022), extend supply chain performance (Culot et al., 2024), and increase organizational efficiency via smart contracts (Xiong et al., 2023). Collectively, these findings indicate that operational effectiveness is a decisive factor for adoption, legitimacy, and the practical viability of DID services.

It is crucial to distinguish operational effectiveness from sustainability. Whereas sustainability emphasizes long-term resilience and institutional durability (Mulligan et al., 2024; Thanasi-Boçe and Hoxha, 2025), operational effectiveness addresses short-term efficiency, cost management, and service flexibility that drive user acceptance at the point of delivery. As Difrancesco, Meena, and Kumar (2023) demonstrate, blockchain adoption can enhance both sustainability and operational efficiency, confirming that the two are distinct yet complementary. Accordingly, we position operational effectiveness as an essential social component that captures the practical efficiency conditions under which DID ecosystems are adopted, trusted, and maintained.

3.3.3 Technical components

The technical components represent foundational design principles intended to ensure vertical integration across the system architecture. Among these, this study highlights multifunctionality principle occasionally referenced in prior literature but insufficiently emphasized. For DID services, which must operate as fully integrated systems, multifunctionality involves coordinating system analysis, design, development, testing, deployment, and operations. This includes developing databases, application systems, and mobile applications that span both hardware and software infrastructures.

To achieve this, modular and scalable application systems and mobile apps should be designed to reduce technical complexity and remain accessible to developers with limited expertise in cryptographic operations. Architecture should incorporate flexible, extensible, plugin-based components from the outset. Furthermore, the user interface of decentralized identity digital wallets should accommodate differentiated branding, features, and user experiences. These elements must be iteratively tested, implemented, and standardized through phased deployment, with UI/UX considerations prioritized throughout development.

We introduce multifunctionality as a core technical dimension, composed of three interrelated elements: usability and simplicity, usefulness, and flexibility and scalability. Prior research highlights that blockchain systems must secure scalability and modularity to accommodate evolving service demands. Surveys of blockchain systems identify throughput, cost, and functional expansion as persistent challenges. Scalability studies further demonstrate that systems must adapt at both architectural and protocol levels to meet changing workloads and functionalities (Chen et al., 2024). At the network level, sharding-based designs are evaluated not only for their security but also for their capacity to sustain diverse functions under heavy load (Bulgakov et al., 2024). Similarly, decentralized application design emphasizes modular structures and "scaling tiers" as critical enablers of extensibility and system evolution (Pop et al., 2020).

Beyond technical performance, multifunctionality must also encompass usefulness, a well-established determinant of adoption in the Technology Acceptance Model. Empirical evidence shows that blockchain services with strong system quality and user enjoyment enhance perceived usefulness, thereby increasing usage intention (Shrestha and Vassileva, 2019). Keaney (2025) further demonstrates that engineered trust features influence adoption only when perceived as useful, while HCI-focused reviews warn that features detached from user needs can impede adoption (Fröhlich et al., 2022).

Taken together, these insights establish multifunctionality not as a supplementary attribute but as a structurally essential technical dimension. It ensures that DID systems remain user-friendly, deliver meaningful value, and flexibly expand to meet evolving service demands without compromising efficiency or usability.

3.3.4 Redefining decentralization as a technical design principle

This study also reconceptualizes decentralization as a realistic and actionable design principle. In enterprise contexts, complete removal of centralized authorities is often impractical due to regulatory obligations, operational requirements, and accountability needs. Instead, decentralization should be defined as the functional distribution of identity-related roles—such as issuance, verification, and storage—across multiple mutually trusted actors operating under a shared governance framework.

TABLE 2 Technical Components and Details: It shows the technical components extracted based on prior research and literature.

Technical components	Attributes and definition(in details)	References
Decentralization (Elimination of dependence on central authorities)	① Decetralized Network Architecture Identity and credential management operates within a decentralized network where identifiers are not controlled by a centralized authority. Architecture eliminates intermediaries, ensuring that trust and operations are maintained without reliance on a single point of control	DID design principles (W3C 2022) SSI Principles (Sovrin Foundation, 2020) ToIP Framework Guzmán-Castillo el at. (2024) Farmer el at. (2021) Toth and Anderson-Priddy, (2019) Bochnia et al. (2024) (Farmer et al., 2021; Goodell, 2019) Avellaneda et al. (2019)
	② Consensus Mechanism and Decentralized Public Key Infrastructure (DPKI) The system utilizes a decentralized public key infrastructure (DPKI) built on distributed ledger technology. It is governed by a consensus mechanism among participating nodes, enabling secure and transparent management of key lifecycle processes, including registration of service information, generation, distribution, storage, verification, and revocation of public keys	
	③ Entity-Specific Data Management Data is decentralized and managed independently based on the role of each entity. Issuers write to a verifiable distributed ledger; users store credentials on personal devices or private cloud storage; and verifiers validate credentials without querying the issuer or a central authority, relying only on publicly accessible information for verification	
Privacy Preserving	① Minimal and Selective Disclosure Data subjects retain ownership and full control over their identifiers and attribute data, enabling them to disclose information minimally and selectively. Disclosure occurs only with the subject's consent and under their direct control, preserving privacy and autonomy	DID design principles OpenWalletFoundation design principles (Avellaneda et al., 2019) Graham, (2023) Wallet Safety Guide (GroupSafe Wallet Special Interest, 2024) SSI Digital Wallet Goodell (2019) Farmer el at. (2021) Althlhi et al. (2021)
	② Privacy-Preserving Technologies The system incorporates privacy-preserving technologies by design. These include cryptographic techniques that allow provers to demonstrate claims without revealing sensitive information, anonymous credential protocols based on public standards, and mechanisms that enforce the separation of issuers and verifiers. Such measures ensure data confidentiality in peer-to-peer interactions	
	③ Censorship Resistance The architecture implements technical safeguards such as encryption and anonymization to protect users from unwanted surveillance and tracking. Personally identifiable information (PII) is never exposed during credential exchange, ensuring that users' digital identifiers remain resistant to censorship and coercive data collection	
Multi-Functionality	① Usability and Simplicity The system ensures that procedures such as credential issuance are easy for users to understand and navigate. The user interface is designed to be intuitive, consistent, and convenient, minimizing cognitive load and promoting accessibility	VC design principles OpenWalletFoundation design principles Wallet Safety Guide (GroupSafe Wallet Special Interest, 2024) STS Web of system, general design principles Guzmán-Castillo (2024)
	② Usefulness The service is designed to support users in achieving their intended goals. System functionalities are aligned with the user's contextual needs, ensuring that they provide practical value and relevance within defined use cases	

(Continued on following page)

TABLE 2 (*Continued*) Technical Components and Details: It shows the technical components extracted based on prior research and literature.

Technical components	Attributes and definition(in details)	References
	③ Flexibility and Scalability The architecture supports modular and reduced-functionality design to facilitate simple implementation and deployment. It enables adaptability to changing environments and allows for seamless integration of additional services as needed	
Interoperability	① Standardization and Interoperability The system utilizes open, public, and royalty-free standards to enable secure, interoperable representation, exchange, protection, and verification of digital identity data. Standardized protocols allow for seamless and trustworthy credential verification among authorized entities, facilitating reliable and secure data exchange	DID design principles OWF design principles EUDI Wallet SSI Digital Wallet SSI Principles (Sesana 12 May 2021) WEF Digital identity ecosystem (Forum, 2021) Goodell (2019) Deloitte (Toth and Anderson-Priddy, 2019)
	② Data Portability Through the implementation and use of open standards, data controllers retain the ability to transfer their wallet information at any time to another provider's wallet or to a self-hosted solution, ensuring user autonomy and vendor independence	
	③ Transparency and Openness Systems used to manage and operate identity networks must be open in terms of functionality, governance, and update mechanisms. Algorithms should be free, open-source, well-documented, and architecture-independent, enabling anyone to review and understand how the system works	
Security	① Cryptographic Algorithms The system applies robust encryption algorithms to ensure the security and trustworthiness of DID documents and all related data. Credential data and other sensitive information are protected from malware and external threats through secure key generation, management, end-to-end encryption, and secure data handling practices	DID design principles OWF design principles EUDI Wallet Wallet Safety Guide (GroupSafe Wallet Special Interest, 2024)SSI Digital Wallet Farmer el at. (2021) Muhtasim et al. (2022) Althlhi et al. (2021) Ministry of Science and ICT, Korea Internet and Security Agency, and Korea Zero Trust Forum 2023)
	② Authorization and Access Control Applications are developed based on secure coding principles and enforce the principle of least privilege. Administrative privileges for identity systems are strictly segregated by role, with clear procedures for account creation, modification, and deletion. Logs for authorization, activity monitoring, and access control are implemented to support traceability and security governance	
	③ Embedded Security-First Processes The system incorporates proactive, built-in security processes that respond rapidly to emerging threats. It minimizes attack surfaces and integrates security policies, protocols, and response mechanisms directly into system tools to ensure automation, data-driven management, and strong cyber resilience	

This revised interpretation reduces reliance on single points of control while maintaining integrity and accountability. In this light, hybrid architecture combining decentralized technologies (e.g., distributed ledgers) with centralized components (e.g., trust registries)—are proposed as a viable and scalable approach. Such models enable incremental adoption, leverage existing institutional infrastructure, and provide a transitional framework for the broader diffusion and institutionalization of DID services.

The integration of multifunctionality and this redefined approach to decentralization is summarized in (Table 2) Technical Components and Details, which presents the core technical components and their detailed configurations.

3.4 Data analysis

3.4.1 Framework verification and derivation of framework-based evaluation items

The reliability and content validity of the proposed framework were assessed through a review of relevant literature and multi-

TABLE 3 Expert interview results by sector: These are the interview results by sector to validate the framework. Experts in each sector were interviewed.

Area of expertise	Key insights 1	Key insigts 2
Blockchain/DID Expert	Removing dependence on central authorities is more critical than decentralization; in enterprise settings, the concept of "eliminated central dependency" is more suitable	When operating on a mainnet, it is essential to establish a trust registry and governance framework. Given current limitations in data portability caused by DID and VC, ensuring interoperability is urgent. DID systems should actively integrate privacy-enhancing technologies such as encryption, anonymity, and blind signatures
Security Expert	Privacy protection and security technologies must be clearly distinguished; strong encryption algorithms and protocols such as TLS 1.3 or higher are required	DID systems must implement privacy-preserving measures such as multiple DID usage and frequent public key rotation. All security design should adhere to the Zero Trust principle, and multilayered defense mechanisms must be established across all operational stages, not just issuance and verification
Cloud Architect	Security and firewall configurations vary across cloud environments such as AWS, Azure, and GCP; fine-grained security management should be automated using appropriate tools	Mobile ID functionality must be flexibly designed to accommodate various OS environments. Infrastructure and deployment processes must support irregular updates and diverse mobile platforms with a stable and adaptable setup
Application Developer	Backend and frontend should be designed in an integrated manner to synchronize logic and interface updates. Modularization is essential to support various service types	Personal data protection, identity verification protocols, and legal compliance must be consistently maintained. Systems handling identity issuance and verification should meet regulatory requirements and ensure secure communication between backend and frontend
Mobile App Developer	OS-specific factors such as Android and iOS approval processes and ethical UI considerations must be reflected in the app design. Device diversity and screen variability must also be taken into account	The success of mobile ID apps depends heavily on early-stage UX planning. Interfaces should be intuitive and efficient in terms of both quality and cost
UI/UX Expert	Whether B2B or B2C, the essence of user experience remains the same. Mobile identity services should prioritize intuitive interaction and fundamental usability	Interfaces must be easily accessible for diverse user groups, including the elderly, and instill confidence that personal information is being securely protected

domain expert consultation. As summarized in (Table 3) Expert interview results by sector, the expert group included specialists in blockchain/DID, security, cloud architecture, application system development, mobile application development, and UI/UX design. This composition was intended to ensure that both the social and technical dimensions of the framework were accurately and comprehensively reflected.

The expert selection process was guided by three core criteria: standards alignment, developer-oriented implementation, and user-centered evaluation.

First, to ensure standards-based validation, the panel included blockchain and DID experts familiar with international specifications, such as the W3C standards and the Decentralized Identity Foundation (DIF) guidelines, as well as security professionals capable of assessing compliance with privacy protection and cybersecurity requirements.

Second, from a developer-oriented perspective, application developers and cloud infrastructure specialists with hands-on experience in implementing and deploying decentralized identity solutions within enterprise environments were included to evaluate practical feasibility and scalability.

Third, to incorporate a user-centered perspective, UI/UX specialists and user experience designers participated in assessing usability, adoption potential, and overall accessibility of the services.

This strategic composition provided a balanced evaluation, ensuring that the proposed DID service framework was examined in terms of technical robustness, implementation feasibility, and user acceptance—three critical factors for the design and deployment of enterprise-level DID architectures.

3.4.2 Expert consultation

3.4.2.1 Expert composition

To ensure balanced coverage of both social and technical factors, this study conducted expert consultations with a total of eight specialists across six domains: blockchain/DID, security, cloud architecture, application development, mobile app development, and UI/UX. Experts were selected based on a minimum of 10 years of professional experience, domain expertise, and affiliation with either academic or industry institutions. Detailed expert profiles are presented in (Table 4) Expert Profiles.

3.4.2.2 Data collection protocol

The consultations were conducted through semi-structured in-depth interviews. The protocol included 30 pre-defined questions derived from the framework developed in this study, consisting of 15 items addressing the social perspective and 15 items addressing the technical perspective. Full details of the interview protocol are provided in (Table 5) Interview Protocol. All interviews were audio-recorded, fully transcribed, and subsequently condensed into extended summaries for analysis.

All participants were fully informed of the study's objectives and procedures and provided written consent prior to participation, in accordance with institutional ethical guidelines.

3.4.2.3 Analysis and synthesis

Interview materials were independently reviewed by the researchers, followed by a consensus process through which thematic coding and clustering were performed. Expert feedback was mapped to the key dimensions of the framework, including governance, privacy/security, infrastructure, operational effectiveness, and multifunctionality. The integration of expert

TABLE 4 Expert Profiles: It shows expert profiles. All experts had a minimum of 10 years of experience in their field and were selected for their domain expertise. Affiliations represent major domestic IT enterprises. Individual names are withheld to preserve anonymity.

Domain	Domain of expertise (number of interviewee)	Position and background	Affiliation	Interview timing
Blockchain/DID	Blockchain Expert/DID Expert (2)	Senior Architect and Computer Science PhD/ Contributor to open-source DID projects 15 years of industry exp. both	Domestic IT Company A(both)	July 2024
Security	Security Expert (1)	Chief Security Officer, 15+ yrs in cybersecurity industry expert (architect)	Domestic IT Company A	July 2024
Cloud Architecture	Cloud Solution Architect (1)	Cloud Solution/Infrastructure Architect AWS/Azure certified	Domestic IT Company B	September 2024
Application Development	Application Development (1)	Lead Developer, Senior Backend/Frontend Lead, 12 years exp Identity Systems regulatory compliance expertise	Domestic IT Company B	October 2024
Mobile App Development	Mobile App Developers (2)	Mobile Engineers (iOS/Android each), 10+ years industry practitioner	Domestic IT Company C	September 2024
UI/UX	UI/UX (1)	UX Designer >10 years experience in HCI/UX; project manager; experience with mobile ID usability	Domestic IT Company A	October 2024

TABLE 5 Interview Protocol: It shows how the expert interview conducted.

Format	Prepared questions	Duration	Data recording and processing
Semi-structured interviews, in-depth oral interview	Pre-defined 30 questions of developed framework on this study(15 out of Socio and 15 out of technical components)	60–90 min 1 or 2 sessions	Audio-recorded, transcribed, condensed, thematically coded and synthesized

TABLE 6 Detailed Expert Interview Summaries: It is the detail interviews summaries.

Domain expert	Interview summaries
Blockchain/DID Expert	• The framework appropriately reflects blockchain considerations such as decentralized networks, consensus mechanisms, and data management • The term 'elimination of central dependency' is more relevant than 'decentralization' for enterprise settings • Trust registries and governance frameworks are essential for mainnet operations • Privacy preservation should include protocols, encryption, anonymity, and blind signatures • Operational effectiveness should account for infrastructure and indirect costs • Interoperability of DID/VC is still limited but under active standardization • Big Tech initiatives (e.g., ToIP, Hyperledger, OWF contributions) must be closely tracked
Security Expert	• Privacy technologies and security technologies should be clearly distinguished • Strong encryption protocols (TLS 1.3 or higher) are necessary • Privacy-preserving measures such as multiple DID usage and frequent public key rotation are required • Credential storage should rely on hardware secure environments (e.g., TEE) • Zero Trust has become the guiding principle and should inform the framework
Cloud Architect	• Different cloud providers (AWS, Azure, GCP) require fine-grained configuration • Mobile ID updates are irregular, and infrastructure must support flexible deployment • Security/firewall tools must adapt continuously as new threats emerge
Application Developer	• Backend and frontend must be modular and synchronized • Backend should include access control, regulatory compliance, and protocol consistency • Frontend must provide intuitive, secure, and accessible interfaces • Secure backend–frontend communication is essential
Mobile App Developer	• Approval processes differ significantly between Android and iOS. • Device diversity introduces complexity in app performance and testing • Early UX design has strong implications for cost and quality
UI/UX Expert	• User experience encompasses perception, attitude, and behavior across B2B and B2C contexts • Mobile ID services should prioritize intuitive interaction and accessibility • Trust in privacy protection is essential for adoption

TABLE 7 Summary of Expert Feedback and Integration into Framework: It shows how the expert feedback was relected and mapped with the developed framework.

Domain of expertise	Key insights (condensed)	Integration into framework
Blockchain/DID Expert	Elimination of central dependency; governance and trust registries; interoperability challenges; privacy-preserving technologies	Governance, Privacy/Security, Operational Effectiveness
Security Expert	Privacy vs. security distinction; Zero Trust; encryption and key management; layered defense	Privacy/Security
Cloud Architect	Security/firewall variation across AWS/Azure/GCP; adaptability for updates and diverse platforms	Infrastructure
Application Developer	Backend–frontend integration; modularization; regulatory compliance; secure communication	Technical Governance, Operational Effectiveness
Mobile App Developer	OS-specific approval and UI/UX constraints; device diversity; UX quality; cost implications	Usability, Operational Effectiveness
UI/UX Expert	Intuitive, seamless UX; accessibility for elderly; trust in privacy protection	Multifunctionality (usability, usefulness, scalability)

insights into the framework is summarized in (Table 6) Summary of Expert Feedback and Integration into Framework.

3.4.2.4 Synthesized findings

The consultations produced the following key findings:

- The elimination of central dependency and the establishment of governance structures are essential.
- Distinguishing between security and privacy, and implementing multi-layered defense mechanisms, are critical.
- Scalability and modularity must be secured at both the cloud and system levels.
- Intuitive user experience (UX), accessibility, and usefulness play a decisive role in the adoption of DID services.

In sum (Table 7), Summary of Expert Feedback and Integration into Framework shows that the expert consultations validated the legitimacy of the framework and evaluation questions, thereby strengthening the practical relevance and credibility of the study.

3.4.3 Proposed refined DID service architecture

The primary objective of the proposed architecture is to enhance usability and foster the ecosystem expansion of enterprise-centric DID services that safeguard data privacy through SSI principles in the globally hyperconnected AI era. We designate this model as the "Proposed Refined DID Service Architecture," reflecting its intent to retain the overarching structure of existing architectures while improving internal components in alignment with enterprise-level feasibility, goal orientation, adherence to SSI principles, and enhanced technical interoperability. This designation captures both the structural continuity and the targeted refinements introduced in this study.

The architecture adopts a four-layer structure, each forming a foundational element of decentralized identity management:

- Trusted Ledger Layer (Verifiable Ledger Layer): A blockchain-based decentralized ledger infrastructure that stores DID registries and credential definitions, removing reliance on central authorities and achieving decentralization.
- DID/VC Service Application Layer: Facilitates interactions among holders, issuers, and verifiers, and ensures privacy protection during issuance and verification via digital wallets.
- Governance Layer: Establishes trust registries, identity verification institutions, and operational rules, ensuring ecosystem reliability through consensus-based governance mechanisms.
- Ecosystem Layer: Builds a cross-industry digital identity ecosystem, enabling global interoperability of DID services.

The architecture emphasizes core functional mechanisms—such as embedded data privacy protection and secure communication protocol design—rather than only surface-level structures. It incorporates technical and policy recommendations, including the adoption of standardized protocols, consensus-based governance design, and harmonized UI/UX improvements, while identifying cost efficiency and privacy protection as key ongoing challenges (Figure 3). Proposed Refined DID Service Architecture illustrates the proposed architecture.

3.5 Structured empirical validation framework

To strengthen the rigor of this study and address the limitation of lacking empirical testing, we propose a structured and comparative empirical validation framework for the proposed architecture. This framework is designed to systematically evaluate both socio-technical and technical dimensions of DID-based services in a manner that is verifiable, replicable, and sensitive to contextual variation.

For the purpose of validation, we selected two domestic organizations that have already deployed DID-based "mobile employee ID" services. These organizations provide an appropriate comparative context for three reasons. First, both institutions operate the same service type, thereby ensuring consistency of comparison. Second, they cover similar service functions across offline domains such as building access, cafeterias, fitness centers, and libraries, as well as online domains such as system login and certificate issuance, which enables a direct comparability of features. Third, each institution manages more than 10,000 active users, thereby guaranteeing a sufficient scale of data for representative evaluation.

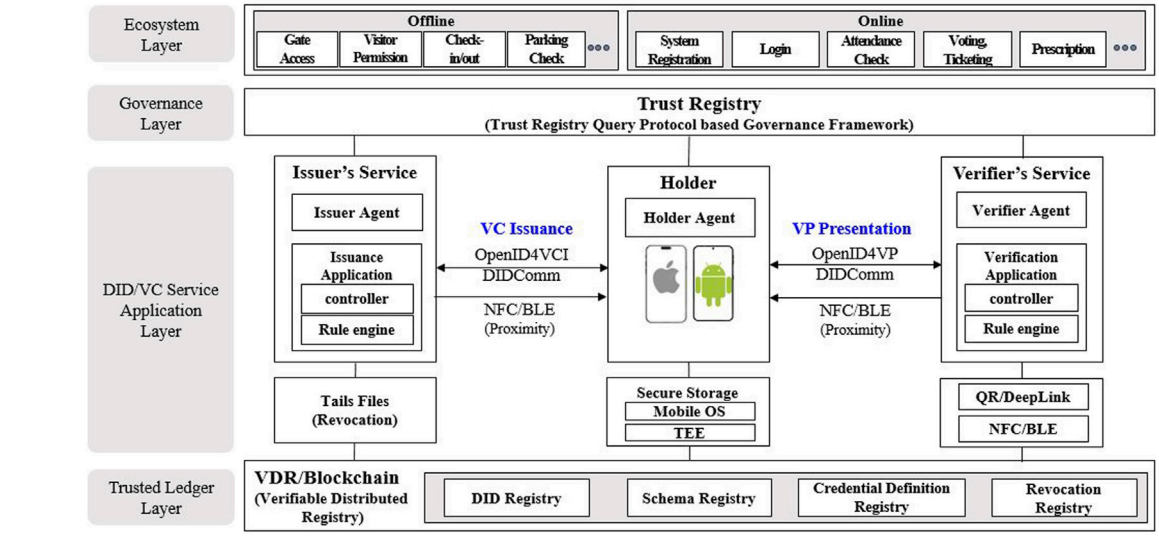

FIGURE 3
Proposed architecture for improved DID service: Synthesizes the recommendations for an improved architecture of DID services.

At the same time, the two organizations diverge significantly in their technological choices and ecosystem dependencies. One institution relies on a globally available open-source DID platform, while the other utilizes a locally customized solution developed by a domestic technology provider. This contrast allows us to investigate not only functional and organizational factors but also to empirically assess how different implementation strategies—open-source versus proprietary customization—affect interoperability, governance, and sustainability.

The validation framework consists of 30 indicators in total, divided equally between socio-technical and technical dimensions. The socio-technical indicators are grounded in Science and Technology Studies (STS) and focus on governance, usability, interoperability, and organizational adaptation. The technical indicators examine privacy preservation, security, decentralization, interoperability, and performance. Each indicator has been operationalized with measurable rubrics, and the technical metrics are explicitly aligned with international standards (ISO/IEC 18013-5/-7) to enhance comparability and methodological rigor.

Data collection will be conducted through semi-structured interviews with project managers and decision-makers, complemented by internal document analysis where possible. By triangulating these data sources and applying a balanced set of socio-technical and technical criteria, the framework provides a systematic pathway for empirical validation. In doing so, it not only strengthens the methodological foundations of this study but also enables a meaningful comparison of DID implementations in real-world organizational contexts.

4 Research results

4.1 Integrated research findings

This study identified the socio-technical barriers limiting the practical adoption and scalability of DID-based decentralized identity services and proposed a set of theoretical and practical solutions. Drawing on Socio-Technical Systems (STS) theory, we developed a comprehensive framework that supports both horizontal diffusion and vertical integration, while incorporating enterprise-specific requirements—such as operational efficiency and multifunctionality—that have been overlooked in prior research.

The framework's theoretical rigor and practical relevance were validated through expert consultation, forming the basis of the Refined DID Service Architecture. This architecture embeds privacy-preserving mechanisms directly into its infrastructure, allowing users to achieve socially acceptable levels of data privacy automatically, without additional configuration, while ensuring high usability and scalability.

When technical design, policy support, and social acceptance are organically integrated, the proposed framework and architecture offer a concrete, actionable pathway for the practical adoption and sustainable growth of DID services.

4.2 Proposed architecture validation

The proposed architecture was evaluated through a case analysis of mobile driver's license (mDL) deployments, yielding the following implications:

1. UI/UX Guidelines–Government-issued apps performed well in balancing privacy and accessibility, e.g., unlocking sensitive information only via intentional actions (e.g., shaking the device). In contrast, Samsung Wallet displayed sensitive data on the initial screen, causing inconvenience. Consistent, user-centric UI/UX guidelines are essential when expanding to platforms such as Kakao and Naver.
2. Openness of Trust Registries–Current systems rely on centralized trust authority reviews, limiting the diversity of verifiable credentials. Introducing private trust registries could enable micro-ecosystems (e.g., restaurant reservations, loyalty programs), though this requires extensive governance discussions and preparation.
3. Verification App Adoption–Despite free availability to small businesses, verification app usage is low, with many institutions (e.g., hospitals, polling stations) relying on visual checks. Practical government support measures are needed to drive adoption.
4. Vendor Lock-In and Interoperability–The existing mDL solution, developed by a single vendor, is closed-source and lacks global interoperability. Its planned transition to open-source could create long-term opportunities for international standardization and adoption in developing countries, but sustained community-building efforts will be critical.

Building on these case-level findings, the validation framework was further designed to ensure methodological rigor and broader applicability. The evaluation metrics were systematically derived from ISO/IEC 18013-5 and ISO/IEC 18013-7, which define essential criteria for mDL systems such as privacy, performance, interoperability, and conformity with international security and trust models. These standards also specify implementation requirements—including physical characteristics, machine-readable technologies, access control, integrity verification, and mobile application interfaces—that collectively establish the benchmarks for privacy and performance in mDL systems (Kim et al., 2022; Mulligan et al., 2024). Complementary studies on blockchain-enabled identity frameworks highlight the importance of governance structures, interoperability, and privacy-preserving technologies for trustworthy deployment (Beck and Kranz, 2020; Schletz and Fischinger, 2021).

Each evaluation item in the framework was explicitly mapped to international standards and established best practices. Privacy indicators were operationalized using ISO-defined requirements such as access control and data minimization; performance indicators were derived from conformity checks addressing system responsiveness and availability; and interoperability indicators were evaluated through documented benchmarks for cross-platform integration. To improve readability and transparency, a summary table was added that consolidates the applied standards, referenced literature, evaluation categories, and their mapping to the framework, providing readers with a clear overview of the validation process.

Through this structured, evidence-based methodology, the proposed architecture is validated against measurable, standards-based, and literature-supported criteria. This approach strengthens methodological rigor while ensuring both the technical robustness and the socio-technical applicability of the framework.

Summary of Responses to Research Questions:

- RQ1: Developed a comprehensive STS-based framework enabling both horizontal diffusion and vertical integration of DID services, incorporating enterprise-specific requirements, and validated through expert consultation.
- RQ2: Identified major technical challenges—such as lack of interoperability standards, complexity in key management and recovery, integration difficulties with legacy systems, performance limitations of privacy-preserving technologies, and practical constraints of full decentralization—and social challenges, including absence of trust governance, stakeholder conflicts, unclear regulatory frameworks, and limited public awareness.
- RQ3: Proposed a Refined DID Service Architecture embedding privacy-preserving mechanisms at the infrastructure level to ensure automatic privacy protection without user intervention, while maintaining scalability and alignment with global standards.

5 Discussion

This study presents a practical and scalable DID architecture for global enterprise deployment addressing the limitations of existing models from technological, market, and policy perspectives. The key recommendations are summarized in (Table 8) Synthesis of key suggestions for proposed refined architecture.

From a technological perspective, architecture prioritizes the adoption of open-source technologies that have been globally validated in real-world DID and VC applications. While proprietary vendor-specific systems may offer certain privacy-enhancing features, they often limit interoperability and create vendor lock-in. To ensure machine-readable interoperability across diverse platforms, globally standardized open protocols should be adopted. As most DID services are delivered via mobile digital wallets, harmonized UI/UX guidelines are essential to ensure accessibility and ease of use. Additional measures, such as Trusted Execution Environments (TEEs), are recommended to enhance key management security and wallet reliability. The term of TEE was originally defined in the Advanced Trusted Environment: OMTP TR1 standard as "a set of hardware and software components providing facilities necessary to support applications," with two security profiles addressing software-only and combined hardware-software threats (Open Mobile Terminal Platform, 2009). Today, TEEs—secure hardware-software enclaves—are increasingly utilized in blockchain and IoT contexts to ensure secure asset storage by isolating sensitive operations from external threats. A fully decentralized network architecture that minimizes reliance on central authorities, combined with open and interoperable standard protocols, is critical to safeguarding data privacy.

Our proposed architecture incorporates three key components inspired by prior research: 1. a Privacy-Aware Access Control Token to protect sensitive attributes, 2. a Decentralized Trust Coordination Structure to distribute verification without central dependency, and 3. a Resilience Mechanism to ensure continuous operation under node failures or network fluctuation. In our proposed architecture,

TABLE 8 Synthesis of key suggestions for proposed refined architecture: This table is a summary of the proposals of this study and is organized in terms of technology, society, and policy.

구분	Research finding summary
Technological Perspective	1. Introduction of Harmonized, User-Centric UI/UX Guidelines The study emphasizes the need for implementing cohesive, user-centric UI/UX design guidelines that enhance usability across identity-related services 2. Application of Globally Verified Open Privacy Technologies To ensure data privacy, the study recommends the adoption of internationally recognized, open-source privacy-preserving technologies 3. Use of Open Protocols for Interoperability Technical interoperability should be secured by utilizing open and standardized communication protocols in decentralized identity architectures 4. Secure Digital Wallets through Trusted Execution Environments (TEEs) The study highlights the importance of strengthening digital wallet security by integrating hardware-based protection such as TEEs
Supplemetnary Market Perspecive	1. Beyond Simple ID: Expansion to Diverse Credential-Based Services The identity ecosystem is evolving from simple ID verification to a diverse range of credential-based services. The study highlights the global scalability of these models and their potential to reshape the digital identity landscape 2. Subscription-Based Business Models for Sustainability Sustainable Decentral Identity Ecosystems require viable business models. The study proposes subscription-based approaches to support ongoing operations, innovation, and user engagement 3. Ecosystem-Based Trust Registries and Public Governance Discourse Trust registries serve as verifiable anchors for ecosystem participants. The study calls for the adoption of trust registries and emphasizes the need for open public discourse regarding their governance and operational mechanisms
Market Ecosystem Policy Proposals	1. Shift to Negative Regulation for Autonomy and Ecosystem Vitalization The study recommends transitioning from prescriptive regulatory models to a negative regulation approach, enabling greater autonomy and innovation within the identity service ecosystem 2. Fostering a Digital Innovation Environment for User-Centric Privacy Protection Policy initiatives should encourage enterprises to adopt digital identity technologies that prioritize user-centric privacy, promoting responsible data handling and trust-driven service design 3. Cross-Industry Process Integration through Interoperability Solving interoperability challenges is essential for connecting core processes across heterogeneous industries, allowing for seamless service coordination and shared value creation

● It should be noted that Supplementary Appendices is also submitted as separate Excel files. Please therefore check that these are as expected.
Please refer to the Social Component Evaluation Questions and the Technical Component Evaluation Questions outlined in Supplementary Appendix.

we propose to implement a Privacy-Aware Access Control Token—a privacy-preserving digital credential that functions like a temporary electronic pass. Instead of revealing full personal details each time, it allows a user to prove only the specific attributes needed for access (for example, over 19 years old') while hiding other sensitive data. This token mechanism automatically controls who can access which resources, ensuring both security and privacy.

From a market perspective, architecture encourages horizontal expansion of DID services beyond basic digital identity verification, positioning them as a foundation for a broad range of credential and affiliation verification models. These include both macro-level ecosystems (e.g., passports, driver's licenses, academic certificates) and micro-level ecosystems (e.g., community membership credentials and loyalty programs). To ensure sustainability, a subscription-based business model targeting credential issuers and verifiers is proposed. A decentralized governance structure for trust registries should be implemented to support not only government-led initiatives but also sector-specific, cross-sector, and public-private trust registries. For instance, in the music industry, a trust registry could be jointly managed by creators, producers, and distributors. The development of "killer services" and continuous UI/UX enhancements will be vital to driving adoption, while the architecture must also support the operational efficiency and scalability required for real-world deployment.

From a policy perspective, the study recommends establishing a self-regulatory framework to accelerate the institutionalization of the DID ecosystem, supported by proactive government involvement. In addition to general regulatory flexibility, targeted policy tools should be introduced: 1. tax incentives for organizations adopting DID-based solutions, 2. certification programs to verify compliance with privacy and interoperability standards, and 3. public procurement requirements that include DID-enabled solutions. Policies aligned with ESG(Environmental, Social, and Governance) principles could further encourage voluntary private sector participation. A continuous feedback loop should be established so that user needs, behaviors, and usage patterns directly inform technology development and policy-making, creating alignment between technological advancement and social acceptance. Standardization of DID and VC specifications through bodies such as W3C, along with global compatibility in data structures, communication protocols, and software interfaces, will require strong policy support and multi-sector collaboration, including public-private partnerships.

As DID technology is still transitioning toward mature standardization and interoperability, both enterprises and governments must adopt proactive roles—contributing to global standards alignment, cross-sector governance models, and pilot deployments.

6 Conclusion

This study defines DID Services as a social technology that protects data privacy in the digital age. It aims to ensure these services evolve and sustainably develop within the digital identity ecosystem by interacting with societal members and environmental changes. Despite being the technology-based driver of this innovative paradigm shift, decentralized identity verification services exhibit lower adoption rates than initially predicted growth forecasts. DID technology hold significant potential for privacy protection, yet its adoption remains limited due to technical implementation challenges, the absence of comprehensive standards and policy frameworks, and the complex, often conflicting interests among stakeholders.

We aimed to present architecture from technological, societal (market), and policy perspectives for DID to achieve its original useful technological purpose while evolving through interaction with society's members as a sustainable implementation. Consequently, this study highlighted the need to develop a framework enabling DID to evolve through iterative interaction with societal members' requirements. A review of existing global frameworks and design principles for distributed identity verification services revealed that they primarily exist at a conceptual and theoretical level. Due to the absence of standards or unbalanced development based on technical elements, they fail to adequately address the complexities and practical challenges that may arise during actual implementation.

To address these issues, the study introduced a comprehensive framework designed to support both the horizontal diffusion and vertical integration of DID services. The core objective of the derived framework is to maximize the overall efficiency and effectiveness of the system through the complementary interaction of social and technical components. The social components identified are user-centricity, mutual trust, operational effectiveness, regulatory compliance and governance, and sustainability. The technical components identified are eliminated central authority dependency, privacy preservation, multifunctionality, interoperability, and security. The distinctiveness of this research framework lies in adding 'operational effectiveness' as a social component and 'multifunctionality' as a technical component, which were not extensively addressed in existing frameworks. These were incorporated based on enterprise requirements and expert interviews. This framework incorporates enterprise-specific requirements—such as operational efficiency and multifunctionality—that have often been overlooked in previous research and models. Refined and validated through expert consultation, the framework strengthens both theoretical rigor and practical applicability. Building on this foundation, the study proposes a Refined DID Service Architecture that embeds privacy-preserving mechanisms directly into the technical infrastructure. The core aim is to enable users to achieve socially acceptable levels of data privacy automatically, without requiring additional configuration or intervention.

Achieving this in practice will require meeting several key conditions across technical, policy and social domains. Ultimately, the practical adoption of DID services will only be possible when technical design, policy support, and social acceptance are seamlessly integrated.

This research makes both academic and practical contributions. Academically, it offers a comprehensive overview of the current state of digital IDs in Korea and abroad, examines DID services from technological, market and policy perspectives through the lens of STS theory and proposes a structured framework for expanding the decentralized identity ecosystem. Practically, it provides actionable guidelines—derived from the framework's components and evaluation questions—for designing, building, and operating DID services. It also identifies key technical considerations for policies formulations, advocating for market-driven regulation to foster adoption and move beyond uniform, conventional inspection methods.

However, the several limitations should be acknowledged. Identity and credential systems vary substantially across nations, regions, and cultural contexts. While the proposed framework aspires toward global standardization, it may not fully capture the socio-cultural and institutional particularities embedded within local infrastructures. Future studies could therefore explore ways of adapting the architecture to diverse regulatory environments and contextual realities, seeking an appropriate balance between universality and local relevance.

In addition, although the framework rests on strong theoretical foundations, its broader applicability has not yet been sufficiently examined across diverse real-world deployments. Extending the comparative case study approach to multi-contextual and cross-industry settings would allow future research to more rigorously evaluate the framework's relevance and effectiveness under heterogeneous conditions.

Finally, further opportunities lie in advancing the integration of AI agents with DID services. Beyond conceptual exploration, subsequent work may design and test experimental models—through simulations, pilot implementations, and usability assessments—to better understand the operational feasibility of agent-augmented DID systems. At the same time, sustainable adoption of decentralized identity also requires clear economic and social value propositions for users. Accordingly, examining compensation and incentive mechanisms for personal data within Web3 ecosystems, and developing incentive-compatible models for data exchange and credential use, will be crucial for fostering both fairness and trust in decentralized environments.

Looking ahead, the proposed framework establishes a foundation for the next-generation of decentralized identity solutions. By combining privacy-preserving technologies, token-based credential control, and decentralized trust mechanisms, it outlines a roadmap for governments, enterprises, and international bodies to collaboratively build interoperable, user-centric digital identity ecosystems. If realized, this approach could move DID from limited pilot projects into mainstream infrastructures, transforming how personal data and trust are managed in the Web3 era and beyond.

Finally, the development of a globally interoperable ecosystem for decentralized identity services remains at an early stage. Achieving this vision requires overcoming technical, institutional, and social challenges, including protocol standardization, governance alignment, and continuous stakeholder collaboration.

Importantly, DID services should not be regarded as a panacea for all privacy and identity concerns. Technical design alone risks limited adoption; instead, decentralized identity must continue to evolve within a socio-technical framework, ensuring that future ecosystems are sustainable, inclusive, and equitable.

Data availability statement

No datasets were generated or analyzed for this study. The work draws entirely on publicly available standards, reports, and academic literature. Non-identifiable excerpts from expert consultation materials may be provided by the corresponding author upon reasonable request.

Ethics statement

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. The participants provided their written informed consent to participate in this study.

Author contributions

HH: Data curation, Writing – original draft. MP: Writing – review and editing. HO: Writing – review and editing, Validation, Methodology. SC: Validation, Conceptualization, Supervision, Writing – review and editing.

Funding

The authors declare that financial support was received for the research and/or publication of this article. Socio-Technological Solutions for Bridging the AI Divide : A Blockchain and Federated Learning-Based AI Training Data Platform (NRF-2024S1A5C3A0204365312).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that no Generative AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fbloc.2025.1696955/full#supplementary-material

References

Althlhi, A., AL-Saedi, M., Alsuwat, H., and Alswat, E. (2021). Privacy-preserving in the context of data mining and deep learning. *Int. J. Comput. Sci. and Netw. Secur.* 21 (6), 137–142. https://doi.org/10.22937/ijcsns.2021.21.6.18

Avellaneda, O., Bachmann, A., Barbir, A., Brenan, J., Dingle, P., Duffy, K. H., et al. (2019). Decentralized identity: where did it come from and where is it going? *IEEE Commun. Stand. Mag.* 3 (4), 10–13. doi:10.1109/mcomstd.2019.9031542

Bai, C. A., Sarkis, J., and Xue, W. (2024). Improving operational efficiency and effectiveness through blockchain technology. *Int. J. Prod. Res.* 35, 857–865. doi:10.1080/09537287.2024.2329182

Bauer, I., Ziolkowski, R., Hacker, J., and Schwabe, G. (2023). Why blockchain: a socio-technical perspective on the motives of business consortia members to engage with blockchain technology. *ACM Digit. Libr.* 2 (2), 1–27. doi:10.1145/3573893

Baxter, G., and Sommerville, I. (2011). *Socio-technical systems: from design methods to systems engineering*. London: Elsevier.

Beck, R., and Kranz, J. (2020). Blockchain governance—A new way of organizing collaborations. *Organ. Sci.* doi:10.1287/orsc.2020.1379

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: data privacy and human rights considerations. *Camb. Journals* 3, e15. doi:10.1017/dap.2021.15

Bochnia, R., Dirk, R., and Jens, A. (2024). Self-sovereign identity for organizations: requirements for enterprise software. *IEEE Access*12 7637–7660. doi:10.1109/access.2023.3349095

Bulgakov, V., Litvinov, Y., Panchenko, A. N., and Zaychenko, M. (2024). Scalability and security in blockchain networks: evaluation of sharding algorithms. *Mathematics* 12 (23), 3860. doi:10.3390/math12233860

Chai, S., and Kim, M. (2012). A socio-technical approach to knowledge contribution behavior: an empirical investigation of social networking sites users. *Int. J. Inf. Manag.* 32 (2), 118–126. doi:10.1016/j.ijinfomgt.2011.07.004

Chen, Z., Dai, H.-N., Zheng, Z., and Zhang, Y. (2024). A comprehensive survey of blockchain scalability. *arXiv Prepr.* doi:10.48550/arXiv.2409.02968

Chu, W. (2022). "A Decentralized Approach towards Responsible AI in Social Ecosystems," in Proceedings of the Sixteenth International AAAI Conference on Web and Social Media (ICWSM 2022). Available online at: https://ojs.aaai.org/index.php/ICWSM/article/view/19274

Cooper, H. M. (1982). Scientific guildelines for conducting integrative research review.

Culot, G., Podrecca, M., and Nassimbeni, G. (2024). Blockchain adoption and operational performance: a secondary data analysis on effects and contingencies. *Int. J. Operations and Prod. Manag.* doi:10.1108/IJOPM-12-2022-0877

Davenport, T. H., and Prusak, L. (1998). *Working knowledge: how organizations manage what they know*. Boston, MA, United States: Harvard Business School Press.

Dib, O., and Toumi, K. (2020). Decentralized identity systems: architecture, challenges, solutions and future directions. *Ann. Emerg. Technol. Comput.* 5. doi:10.33166/AETiC.2020.05.002

Difrancesco, Rita, M., Meena, P., and Gopal, K. (2023). How blockchain technology improves sustainable supply chain processes: a practical guide. *Operations Manag. Res.* 16, 620–641. doi:10.1007/s12063-022-00343-y

Dixon, P. (2019). Digital identity ecosystems world privacy forum.

Dong, C., Wang, Z., Chen, S., and Xiang, Y. (2020). "BBM: a blockchain-based model for open banking *via* self-sovereign identity," in *Blockchain – ICBC 2020*. Editors Z. Chen, L. Cui, B. Palanisamy, and L.-J. Zhang (Cham: Springer), 12404, 61–75. doi:10.1007/978-3-030-59638-5_5

Dong, C., Jiang, F., Li, X., Yao, A., Li, G., and Liu, X. (2021). "A blockchain-aided self-sovereign identity framework for edge-based UAV delivery system," in *2021 IEEE/ACM 21st international symposium on cluster, cloud and internet computing (CCGrid)* (IEEE), 622–624. doi:10.1109/CCGrid51090.2021.00074

Dong, C., Yao, A., Xu, Z., Lu, M., Jiang, F., Chen, S., et al. (2024). "A blockchain-based self-sovereign identity system for KYC processes," in *Proceedings of the 6th ACM international symposium on blockchain and secure critical infrastructure (BSCI '24)* (ACM), 1–11. doi:10.1145/3659463.3660026

Dong, C., Pal, S., Chen, S., Jiang, F., and Liu, X. (2025). A privacy-aware task distribution architecture for UAV communications system using blockchain. *IEEE Internet Things J.* 12 (9), 11233–11243. doi:10.1109/JIOT.2025.3529808

Ertresvag, D. S. (2024). *Exploring decentralized digital identity an ecosystem perspective*. Master, Department of Informatics, Oslo, Norway: University of OSLO.

EUDI (2024a). EUDI wallet.

EUDI (2024b). European digital identity wallet architecture and reference framework.

Farmer, C., Sander, P., and hill, A. (2021). Decentralized identifiers for peer-to-peer service discovery. *Text. Io.*, 1–6. doi:10.23919/ifipnetworking52078.2021.9472201

Forum, W. E. (2021). Digital identity ecosystem: unlocking new value. Available online at: www.weforum.org.

Fröhlich, M., Waltenberger, F., Trotter, L., Alt, F., and Schmidt, A. (2022). Blockchain and cryptocurrency in human computer interaction: a systematic literature review and research agenda. *arXiv Prepr.*, 155–177. doi:10.1145/3532106.3533478

Gartner (2024). *Hype Cycle for Digital identity, 2024*. Stamford, CT, United States: Gartner, Inc.

Glöckler, J., Sedlmeir, J., Frank, M., and Fridgen, G. (2023). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Bus. and Inf. Syst. Eng.* doi:10.1007/s12599-023-00830-x

Goodell, G., and Aste, T. (2019). A decentralized digital identity Architecture. *Identity Priv. Gov.* 2. 17. doi:10.3389/fbloc.2019.00017

Graham, G. (2023). Why the world needs an open source digital wallet right now.

Group, Safe Wallet Special Interest (2024). Wallet safety guid.

Guzmán-Castillo, A. F., Suntaxi, G., Flores-Sarango, B. N., and Flores, D. A. (2024). Towards desiging a privacy-oriented Architecture for managing personal idenfiable information. *J. Internet Serv. Inf. Secur. (JISIS)* (1), 64–84. doi:10.58346/JISIS.2024.I1.005

Hochul, K. (2024). Announcing New York Mobile ID operations.

Keaney, S., and Berthon, P. (2025). The blockchain trust paradox: engineered trust vs. experienced trust in decentralized systems. *User Percept.* 16 (9), 801. doi:10.3390/info16090801

Kemppainen, L., Kemppainen, T., Kouvonen, A., Shin, Y.-K., Lilja, E., Vehko, T., et al. (2023). Electronic identification (e-ID) as a socio-technical system moderating migrants' access to essential public services – the case of Finland. *ELSEVIER Gov. Inf. Q.* 40, 101839. doi:10.1016/j.giq.2023.101839

Khayretdinova, A., Kubach, M., Sellung, R., RoEero Lilja, H., Vehko, T., and Kuusio, H. (2023). Electronic identification (e-ID) as a socioSelbstbestimmung, Privatheit und Datenschutz: gestaltungsoptionen für einen europäischen Weg. *Springer Fachmedien Wiesb. Wiesb.*, 389–406. doi:10.1007/978-3-658-33306-5_19

Kim, E.-J, Ha, S.-J., Lee, J.-E., and Lee, N.-Y. (2020). A Study on Mobile driver's license based on international standards (ISO/IEC 18013-5). *Korean J. Inf. Secur.* 31 (2), 45–67.

Kim, J., Kim, P., Choi, D., and Lee, Y. (2023). A Study on the interoperability technology of digital identification based on WACI protocol with multiparty distributed signature. *Sensors* 23 (8), 4061. doi:10.3390/s23084061

Korhonen, J. (2004). Industrial ecology in the strategic sustainable development model: strategic applications of industrial ecology. *J. Clean. Prod.* 12 (8-10), 809–823. doi:10.1016/j.jclepro.2004.02.026

Kuperberg, M. (2020). Blockchain-Based Identity Management: a Survey from the enterprise and ecosystem perspective. *IEEE Trans. Eng. Manag.* 67, 1008–1027. doi:10.1109/tem.2019.2926471

Lim, S. Y., Musa, O. B., Ali, B., Al-Rimy, S., and Almasri, A. (2022). "Trust models for blockchain-based self-sovereign identity management: a survey and research directions," in *Advances in blockchain technology for cyber physical systems*, 277–302.

Lumineau, F., Wang, W., and Schilke, O. (2021). Blockchain governance—a new way of organizing collaborations? *Organization Science*32 (02), 500–21. doi:10.1287/orsc.2020.1379

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *arXiv Prepr.* doi:10.1016/j.cosrev.2018.10.002

Muhtasim, D. A., Tan, S. Y., Hassan, M. A., Pavel, M. I., and Susmit, S. (2022). Customer satisfaction with digital wallet services: an analysis of security factors. *(IJACSA) Int. J. Adv. Comput. Sci. Appl.* 13. doi:10.14569/ijacsa.2022.0130124

Mulligan, C., Morsfield, S., and Cheikosman, E. (2024). Blockchain for sustainability: a systematic literature review. *Telecommun. Policy*. doi:10.1016/j.telpol.2023.102725

NETZPOLITIK.org (2024). EUDI wallet A wallet full of loopholes. Available online at: https://netzpolitik.org/2024/eudi-wallet-a-wallet-full-of-loopholes/#netzpolitik-pw.

Nicolae, C., and Alexandrescu, A. (2024). Design aspects of decentralized identifiers and self-sovereign identity systems. *IEEE Access* 12, 60928–60942. doi:10.1109/access.2024.3394537

Norman, D. (2016). *What are socio-technical systems?* Interaction New York, NY, United States: Design Foundation - IxDF.

Open Mobile Terminals Platform (2009). "Advanced trusted environment: OMTP TR1 v1.1," in *Open Mobile terminals platform*.

Policy Briefing (2024). Mobile ID surpasses 4 million users electronic signature function to be added next year. Available online at: https://www2.korea.kr/news/policyNewsView.do?newsId=148937622&pWise=sub&pWiseSub=C1.

Pop, C., Neagu, B. C., Boiangiu, S. C., and Pop, F. (2020). Blockchain based decentralized applications: Technology review and development guidelines. *arXiv Prepr.* doi:10.3390/fi13030062

Preukschat, A., and Reed, D. (2022). *Self-sovereign identity*. Shelter Island, NY, United States: Manning Publications.

Robels-Carrillo, M. (2024). Digital identity: an approach to its nature, concept, and functionalities. *Int. J. Law Inf. Technol.* 32 (1), eaae019. doi:10.1093/ijlit/eaae019

Satybaldy, A., Ferdous, M. S., and Nowostawski, M. (2024). A taxonomy of challenges for self-sovereign identity systems. *IEEE Access* 12, 16151–16177. doi:10.1109/access.2024.3357940

Schletz, M., and Fischinger, K. (2021). Defining blockchain governance principles: a comprehensive framework. *arXiv Prepr.* doi:10.1016/j.is.2022.102090

Shahaab, A., Khan, I. A., Maude, R., Hewage, C., and Wang, Y. (2022). Blockchain for public service operational efficiency: a case study. *Gov. Inf. Q.* 40 (1), 101759. doi:10.1016/j.giq.2022.101759

Shrestha, A. K., and Vassileva, J. (2019). User acceptance of usable blockchain-based research data sharing system: an extended TAM based study. *arXiv Prepr.* doi:10.1109/TPS-ISA48467.2019.00033

Sovrin Foundation (2020). Principles of SSI, Version 3. Available online at: https://sovrin.org/principles-of-ssi/.Accessed March 15, 2025

Thanasi-Boçe, M., and Hoxha, J. (2025). Blockchain for sustainable development: a systematic review. *Sustainability* 17 (11), 4848. doi:10.3390/su17114848

W3C (2022). Decentralized identifiers (DIDs) v1.0. Available online at: https://www.w3.org/TR/did-core/.

WorldBank (2024). ID4D. Available online at: https://id4d.worldbank.org/.

Xiong, F., Yang, Y., and Li, X. (2023). The impact of blockchain-enabled smart contracts on operational efficiency. *J. Operations Manag.* 71 (1), 100700. doi:10.1002/joom.70006

Yildiz, H., Küpper, A., Thatmann, D., Göndör, S., and Herbke, P. (2023). IDs v1.0and Mariusz Nowlf-Sovereign identities. *IEEE Access* 11, 114080–114116. doi:10.1109/ACCESS.2023.3322605