Self-Sovereign Identity in Decentralized Federated Identity Management: A Framework for Secure and Scalable Access Control

Muhammad Ahmad[*], Muhammad Adnan[†], Muhammad Asif Nauman[‡]

Abstract

Centralized identity systems are still facing challenges of single points of failure, weak interoperability between platforms, and lack of control for users on their personal data. This paper suggests a Self-Sovereign Identity (SSI) architecture for Decentralized Federated Identity Management (DFIM) to use the blockchain as a trust anchor between Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs) and a governance layer that holds the issuers, verifiers and identity owners to account. The architecture is built around seven functional components: Identity Owners, Issuers, Verifiers, Decentralized Identity Ledger, Identity Hubs, Decentralized Identity Protocols and a Governance Framework, with each having a specific role in the credential issuance, verification and revocation processes. The framework was validated using five scenario-based use cases developed with the input from 20 software industry practitioners, ranging from cross-border healthcare access, age verification on the Internet, validation of university credentials, multi-service authentication in smart cities, to revocation of suspicious credentials. The three use cases were evaluated using three criteria – privacy, scalability, and security – with a comparative rating system. Results indicate that security and privacy are always the most challenging concerns on all use cases, with security being very high in three out of five cases and privacy being a concern that could be traded for scalability in the smart-city use case. The scores for security and privacy were the biggest drivers with zero-knowledge proofs, end-to-end encryption, and federated authentication being the most important. Zero-knowledge proofs and end-to-end encryption were the most important for security and privacy, while federated authentication was the biggest contributor to scalability. The results suggest that, in practice, the potential for meaningful user control over disclosure without compromising multi-domain usability is sufficient to suggest that a well-governed identity layer on a blockchain is likely to accelerate adoption, and that governance and revocation-handling are likely to drive cross-domain adoption most.

Keywords: Centralized, Decentralized, Federated Identity, Digital Identity, Blockchain, Verifiable Credentials, Decentralized Identifiers

Introduction

As a result of the mass dependence of the internet, individuals, and organizations are relying increasingly more upon web services to do

[*]Riphah School of Computing & Innovation, Riphah International University, Lahore 54660, Pakistan, muhammad.ahmad@riphah.edu.pk

[†]Corresponding Author: Riphah School of Computing & Innovation, Riphah International University, Lahore 54660, Pakistan, muhammad.adnan@riphah.edu.pk

[‡]Riphah School of Computing & Innovation, Riphah International University, Lahore 54660, Pakistan, asif.nauman@riphah.edu.pk

various assignments, from social networking systems to banking. Yet, this availability has additionally brought about serious security issues, particularly with respect to distinguishing proof. Although they work adequately, they still have limitations against security breaches, single point of failure, and privacy issues (Raghav & Chaudhary, 2023). One potential remedy for these issues is Decentralized Federated Identity Management (DFIM). With the use of blockchain technology, DFIM seeks to offer a user-centered, safe, and private method of managing digital identities (Badirova et al., 2024; Zargar et al., 2024; Sibahee et al., 2024).

Many corporations are centralized, as the user identities are managed by a single authority. These systems are frequently vulnerable to data breaches, privacy abuses, and cyberattacks. Furthermore, they can be ineffective and difficult to use, particularly when working with numerous organizations (Goel & Rahulamathavan, 2024). Decentralized identity, on the other hand, gives anyone the ability to manage their own digital identity. Users can safely share their identify attributes with several service providers without depending on a central authority (Raipurkar et al., 2023). It provides more control to the user over their personal data. User have complete control to whom he wants to share his identity. User can also control up-to what level of access provide to the organization or other individuals Butincu & Alexandrescu, 2024; Zeydan et al., 2024).

The urgency behind this shift comes from how quickly cybersecurity threats are escalating. A single breach at a centralized provider can expose millions of identity records at once, and the concentration of data in one place makes that provider an attractive target rather than a safeguard (Ding et al., 2024; Liu et al., 2024; Deng et al., 2024). This concentration risk, rather than any single technical defect, is the core problem that decentralized alternatives are trying to address.

A second, more practical problem is interoperability. Ordinary users routinely interact with dozens of platforms, each issuing its own credentials, so managing separate logins and identity proofs across services becomes a genuine burden rather than a minor inconvenience. Federated approaches try to let a single, portable identity carry across platforms without forcing users through repeated authentication procedures for every new service (Sidhu et al., 2022).

Privacy preservation is a third pressing challenge, and arguably the hardest to solve without weakening usability. Verifying a claim, someone's age, residency, or qualification, has traditionally meant handing over far more personal data than the claim itself requires, which is precisely what raises the risk of unauthorized data sharing and identity theft in the first place (Luong & Park, 2023). Finally, regulatory pressure adds a compliance dimension to all of the above. Frameworks such as the

GDPR require data minimization and demonstrable user consent, and centralized identity providers, which by design aggregate more data than any single transaction needs, are structurally at odds with that requirement (Butincu & Alexandrescu, 2024).

Taken together, these four problems, single points of failure, poor interoperability, weak privacy guarantees, and regulatory misalignment, define the gap this work sets out to close. The remainder of this paper reviews how prior SSI and DFIM proposals have approached these problems individually, then presents a blockchain-anchored architecture that addresses them jointly through a defined set of components, a governance layer, and credential lifecycle workflows, and evaluates that architecture against five practitioner-informed use cases.

Literature Review

The study by Razieh et al. (2021) addresses Self-Sovereign Identity (SSI) systems, in particular with the integration of blockchain technologies, a field that is rapidly becoming a focus of study. The authors point out the importance of identity in the digital transformation and how there is no single, universal identity layer on the internet. They point to the possibilities of blockchain technology to provide decentralized, tamper-proof and secure identity management solutions. The paper outlines 22 non-functional requirements (NFRs) of the system such as provability, scalability and usability and analyzes 31 existing SSI solutions against them. The authors also describe 20 use cases for SSI solutions and 7 sets of functional requirements, giving a general idea on the possibilities of their application. The study highlights the gaps in the academic literature by analyzing the commercial and academic solutions and highlights the need to further research for improving SSI frameworks.

As the world is undeniably digitalized, Kheng et al. (2023) paper addresses the concepts of computerized and information power, urging people to take control of their information. It includes the shift in concentrated information administration models to decentralized ones such as SSI. Key challenges identified are key management, interoperability and scalability of SSI systems. The research paper links the policy framework and the technical implementation giving an overall understanding of the notion of digital sovereignty.

Vaios et al. (2022) discuss the drawbacks of the conventional solutions and the introduction of a new model which is composed of three technologies: Self-Sovereign Character (SSC), Electronic Identification, Authentication, and Trust Services (eIDAS) and Fast Identity Online (FIDO). The framework integrates Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to offer a strong verification and ensure

information security. Some of the points discussed here are useful ones which are threats to security, data confidentiality and trust among various entities. This framework could be especially beneficial to European Blockchain Services Infrastructure (EBSI), which enables users to securely handle identities.

In this paper, authors from Jana et al. (2023) give an extensive overview of Identity and Access Management (IAM) and describe its basic components, and propose a secure password-less SSI decentralized approach. It breaks IAM needs down into four categories: security and compliance, operability, technology and user aspects. The study shows the potential of SSI to overcome these challenges, especially in improving usability and manageability, and in conformance with concepts such as "least privilege. But SSI is not a "one size fits all" solution and faces integration issues with the enterprise systems.

Junli et al. (2024) tackle the privacy and revocation issues in the conventional IAM system using an SSI-based approach. Signatures can be generated sequentially and aggregated, and dynamic accumulators can be used for privacy preserving credential issuance and revocation. The proposed framework also balances protection, responsibility, ensuring the rigorousness of identity verification, yet keeping the data open through the use of zero-knowledge proof and particular disclosure techniques. It maintains a decentralized Industrial Internet environment, and provides better scalability and security.

Mirza et al. (2024) utilized blockchain innovation to create a decentralized identification framework. The objective of their work is to utilize blockchain innovation to decentralize the identity provider to enhance the security against centralized identity federations. The objective of decentralizing the identity provider is to diminish weak links and upgrade framework security overall. Blockchain can likewise make it more straightforward for different identity providers to communicate effectively and securely.

Various investigations have analyzed the conceivable outcomes of DID frameworks in light of blockchain innovation. Atharva et al. (2022) looks at how blockchain innovation can be utilized to safely and decentrally handle computerized IDs. The traditional organizations that massively depends upon centralized systems are vulnerable against information misuse and leakage. The proposed arrangement utilizes the circulated record of blockchain innovation to further develop protection, bring down the risk of data fraud, and give people more noteworthy command over their own data. The architecture is depicted, alongside potential purposes in enterprises including medical services and banking.

Hardjanto et al. (2021) recommended a identity management framework that is based on blockchain, while ensuring the safely handling and preservation of personal identity and data. As indicated by their research, blockchain innovation is fundamental for safeguarding protection and information honesty. The appropriated record innovation of blockchain can be utilized by the framework to offer a transparent and immutable record of personal information.

Biagio et al. (2024) characterizes a system for enhanced privacy federated learning and decentralized identity management in automotive system. Their review shows how much identity management is critical that safeguards security in automotive sector. They desire to work on the security and protection of auto frameworks while working with helpful learning among vehicles by facilitating DID with federated leaning. Secure information sharing and correspondence among vehicles and the central system can be extraordinarily helped by blockchain innovation.

The traditional centralized identity systems suffer from such drawbacks as security breaches and privacy intrusions, as well as inefficiencies, as explored by Nigang et al. (2023). It presents DFIM as a game-changing solution, which uses blockchain technology to establish a secure and user-centric framework for digital identities. By giving individuals full control of their identity attributes, DFIM can be used to selectively share and revoke attributes, while also providing resilience and tamper-proof management. DFIM resolves these interoperability issues, enabling seamless communication between different platforms. It enhances the privacy using different cryptographic techniques like zero-knowledge proof. DFIM places a strong emphasis on the principles of data minimization and user consent, offering a robust, scalable and privacy-focused solution that aligns with the needs of the present times.

Yirui et al. (2022) studies the evolution of digital identity systems from centralized to decentralized models. The study emphasis the role of SSI in achieving secure, user-centric, and privacy-preserving identity management. Because of vulnerabilities, including data breaches, single points of failure, and limited user control over personal data, traditional systems are critiqued. SSI enables users to independently manage their identities by leveraging blockchain. It also facilitates to securely share attributes, and revoke access when needed. The study has also mentioned some challenges like regulatory, adaption, and privacy concerns in adoption.

Engin et al. (2024) outlines the transformation from traditional centralized identity systems to a DFIM. It encourages the adoption of DFIM through addressing the security vulnerabilities, single points of failure, and privacy concerns inherent in centralized systems. It provides

users the way to manage their digital identities, enabling secure, selective sharing of identity attributes across platforms. DFIM reduced interoperability challenges by facilitating seamless identity usage across services. This enhances interoperability among different platforms.

Together, these studies will make two enduring contributions to the field. The first is conceptual - studies like Razieh et al. (2021) and Kheng et al. (2023) laid the groundwork for later designs through the creation of the non-functional requirements, use-case taxonomies and policy-technology bridges that provided a common vocabulary to work with. The second technical one was succeeded by further studies, which translated the vocabulary into practical mechanisms such as dynamic accumulators and signatures for revocation (Junli et al., 2024), hybrid SSI-eIDAS-FIDO integration (Vaios et al., 2022), and federated-learning-aware identity handling in the automotive and industrial context (Biagio et al., 2024). Together, their impact is that they demonstrate in healthcare, education, IoT and smart cities that decentralization can be achieved in practice, and not just in theory.

The one thing that they're missing, though, is a single architecture that integrates governance with credential lifecycle management and cross-domain federation into one seamless system instead of disparate add-ons. The overwhelming majority of the surveyed proposals focus on one of the three properties—strategies for optimization, strategies for revocation, or strategies for meeting standards—but they never check the new design against realistic multi-stakeholder use cases. This paper is part of this space: it proposes a seven-component architecture, which includes an explicit governance structure, and unlike most of the literature analyzed herein, tests it against five use cases derived from practitioners' experience and evaluates them for privacy, scalability and security (not just architectural description).

Methodology

The proposed approach is based on the seven components. These components with their role in a system are explained as follows:

Identity Owners

The identity owners are individuals or organizations that will own the digital identities completely. The VCs and DIDs are kept in secure digital wallets, with the ability to selectively disclose only the data necessary for a specific transaction or interaction. Built in interoperability means that the same wallet can be used on different platforms, providing a consistent point of control for the user instead of separate logins for each platform. Credential-management features also allow users to revoke or update

credentials they have stored in their wallet, ensuring that their identity records are accurate over time.

Issuers

Issuers are trusted organizations that develop and issue VCs. The role may be undertaken by the government, universities or private institutions. Issuers sign each credential they issue to ensure that it is authentic and its integrity has not been altered—the university might digitally sign a degree certificate and give it to a graduate. Issuers can also modify the schema of credentials on the blockchain as standards change, ensuring that issued credentials are still valid and meet current standards.

Verifiers (Service Providers)

Verifiers verify credentials from the identity owners and accept or refuse access to a service. For instance, a bank may require an individual to pass a background check on their employment history before granting a loan. Verifiers ask blockchain-based registries to verify the authenticity of credentials, eliminating the need for any single authority, and enhancing security and scalability. They also adhere to having a "privacy-by-design", asking only for the attributes necessary for a specific transaction, which results in fewer sensitive data being released in the verification process.

Decentralized Identity Ledger

At the heart of this system is the Decentralized Identity Ledger, which maintains credential schemas, DIDs, and revocation lists in an immutable way, meaning they can't be changed after they're created. A DID registered to the blockchain is secure, private, and has public verification. The ability to process many transactions per second without compromising on responsiveness is made possible by the advanced consensus mechanisms, and this consistency is essential for the global identity management solution to be viable for cross-border use.

Identity Hubs

Since sensitive user data is not appropriate for on-chain storage, Identity Hubs offer encrypted off-chain storage for users to control access to their data and over time. For example, one patient may give a medical record to a certain doctor or clinic and determine the length of time for that doctor or clinic to have access to the medical record. This ensures that it is both secure and compatible with the user's digital wallet.

Decentralized Identity Protocols

By using decentralized identity protocols like DIDComm, it enables secure communication between identity stakeholders, and conforming to

international standards such as VCs and the W3C DID ensures that credentials can be used to verify identity on various platforms without issues. They also include privacy features like zero-knowledge proofs and anonymized data sharing, and provide resilience techniques to ensure identity services remain operational in the event of disruptions in the network.

Governance Framework

The Governance Framework is the set of regulations and standards that defines how identity stakeholders interact with one another. Because issuers, verifiers, and users jointly formulate its policies and protocols, decision-making stays transparent rather than being dictated by a single party. The framework enforces compliance with legal principles such as the GDPR, uses blockchain as a trust anchor to discourage fraud and reinforce accountability, and provides dispute-resolution mechanisms for resolving conflicts both on-chain and off-chain. Table I defines concisely the function of each proposed component. You can refer Table I to get quick insights of individual components.

Table 1: Key components and functions

Components	Functions
Identity Owners	Manage personal identities using DIDs and credentials.
Issuers	Issue VCs to users.
Verifiers	Validate credentials for service access.
Decentralized Identity Ledger	Store metadata like DIDs and revocation statuses.
Identity Hubs	Securely store sensitive user data off-chain.
Decentralized Identity Protocols	Facilitate secure communication among entities.
Governance Framework	Define rules and ensure regulatory compliance.

Workflow of Proposed Architecture

Whereas the seven components above describe the static building blocks of the architecture, the six phases below describe how those blocks interact over the lifetime of a single identity, from creation through eventual revocation:

Phase 1 (Identity Creation)

The process of creating an identity starts when the user opens their digital wallet to create a unique digital identity DID that is meant to be globally unique and serve as their digital identity. The wallet provides complete management of that identity, the private keys to which it is bound, remaining securely on the user's device. The DID resides on the blockchain after creation, with associated public key and base document service endpoints, which ensures the immutability and verifiability of the DID in the future.

The framework is very easy to use as it provides interactive onboarding interfaces for creating and managing a DID, along with guidance and troubleshooting tools to allow non-technical users to complete this process without external help. This enables users to claim and control their own identities by themselves.

Phase 2 (Credential Issuance)

The process for creating credentials starts with obtaining a request for a Verifiable Credential from the user to an approved credential issuer, like a government entity or a university. The provider verifies the user and signs the credential with its private key and securely sends the credential to the user's wallet.

The credential is then stored in the digital wallet from where it can be used, and the issuer keeps their schema in the blockchain, which will be updated as the need for that credential arises, keeping it in line and current with the standards. The properties of security and interoperability enter into this close relationship between blockchain and credential issuance.

Phase 3 (Authentication and Verification)

Architectural elements include authentication and verification. It begins with the user authenticating some credentials on their digital wallet, and requesting access to some service. The wallet provides cryptographic proofs like zero-knowledge proofs that enable it to confirm the user's claims without revealing the private information.

The direct interaction with the blockchain allows verifiers the ability to verify authenticity and revocation of a credential without the need of a central authority, further improving trust and scalability. If access is successfully verified, the user will have access to the requested service and the resulting blockchain log will create an unchangeable record of transactions, ensuring trust, security and transparency.

Phase 4 (Federated Authentication)

A way to use a single identity to gain access to a number of services in a federation. The concept is to log into one of the services in the blockchain federation and then the blockchain becomes the trust anchor for subsequent communication among the services of the federation without relying on a central authority. In the governance structure there are rules and the members of the Federation adhere to these rules to ensure uniformity of trusts and interoperability across the Federation. In general, the consolidated validation improves the user experience and simplifies the identity management procedure.

Phase 5 (Credential Revocation)

Credential revocation makes sure that if a credential is compromised or expired, they will be unable to be used. Compromised accounts, expired accounts or change of circumstances can lead to revocation, which can be issued by the user or the issuer, and is reflected on the blockchain in real-time and can be viewed by verifiers. Identity hubs are important to alert the users and the relevant stakeholders to credentials being revoked, as well as for verifiers to request further proof to verify credentials after being revoked. The system will have a robust revocation system in place that will help guarantee the integrity of the system and trust of all the stakeholders.

Phase 6 (Data Privacy and Security)

All aspects of the architecture are designed with security and privacy in mind. All communication between the identity parties is encrypted end-to-end to ensure that no one can access the data, and Zero-knowledge proofs allow users to prove a claim without sharing the private data they are claiming.

The privacy-preserving capabilities of the framework are also in compliance with the GDPR and other regulations, which restrict exposure of the data, and multi-factor verification, with the need for multiple levels of proof in key operations, provides an additional layer of security. When combined, these measures provide each stakeholder with a secure and reliable ecosystem focused on privacy and security as first principles of design. Figure 1 illustrates the workflow of proposed approach. It is depicting the components along with their feature, protocol or functions required to communicate them.

Results and Discussion

Experimental Use Cases

We have consulted almost twenty experienced professionals of the relevant domain from the software industry in order to validate our approach. They helped us to design and refine the use cases as per their user requirements. The best five use cases that fits in our domain are discussed in this section with their proper mechanism of validation. We have considered three parameters to evaluate the performance of the proposed approach. These parameters are security, scalability and privacy.

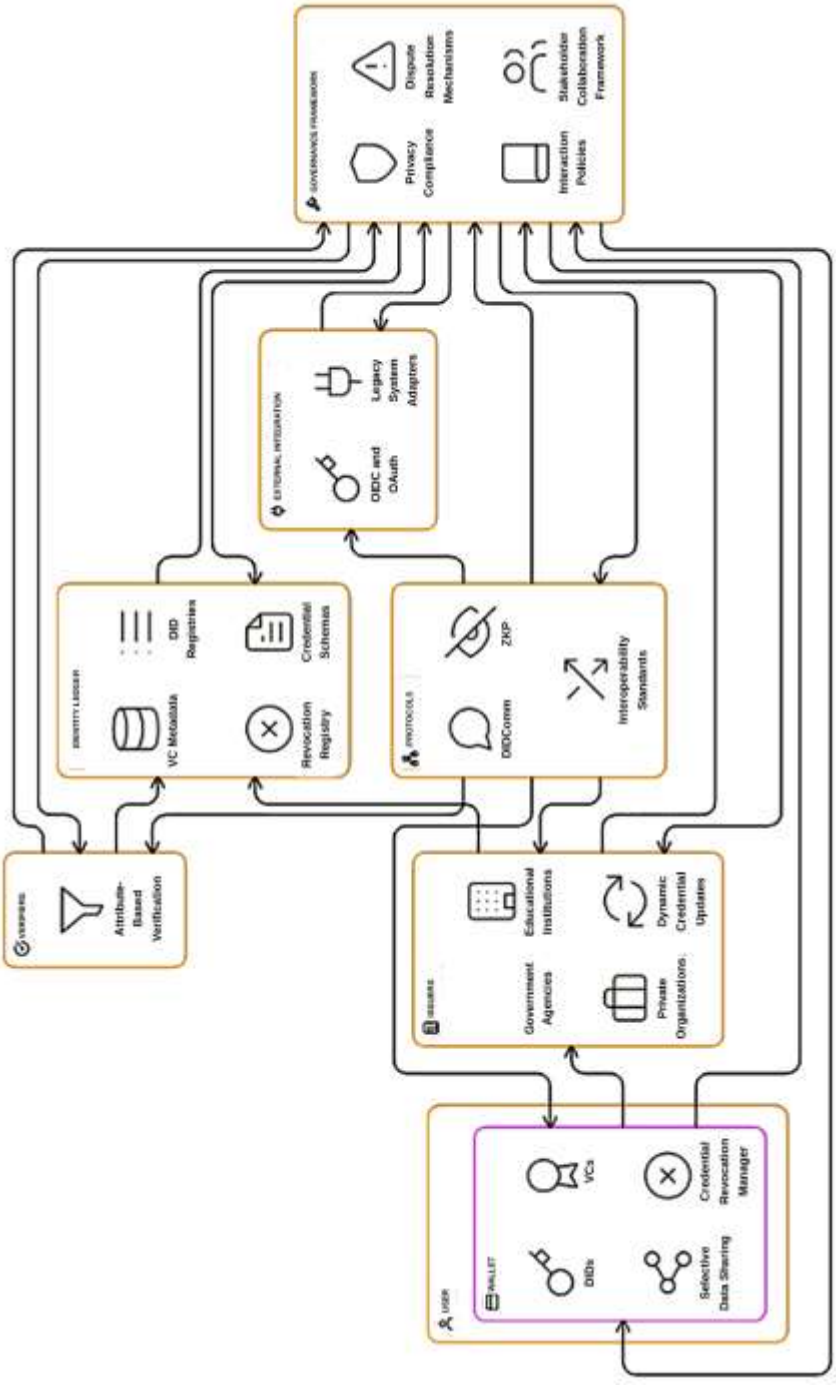


Figure 1: The detailed architecture and workflow of proposed approach

Use Case 1 (Cross-Border Healthcare Access)

Scenario: A user needs to share their medical records when visiting a healthcare provider abroad, in a way that protects both the provider's and the user's privacy, security, and ease of access. The validation steps are shown below:

1. The user opens their digital wallet and selects the relevant medical records stored in an identity hub.
2. The wallet produces a temporary, encrypted access token for the medical services office.
3. The healthcare office checks the token and confirms it against the blockchain to guarantee its authenticity.
4. Access is granted only to the essential records, and only for as long as necessary.
5. The access token automatically expires after a predefined period, revoking access.

From Figure 2, we can see that use case1 is best fit with respect to security parameter. While ensuring equal scalability and privacy.

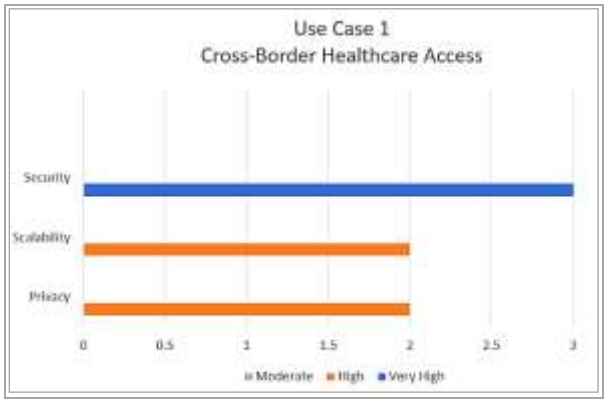


Figure 2: Parameters validation of use case 1

Use Case 2 (Age Verification for Online Services)

Scenario: A user must confirm they meet a minimum age requirement to access an online service, without disclosing their exact date of birth or any other unnecessary personal detail. The validation steps are as follows:

1. Through digital wallet, user initiate request for their age verification.
2. The wallet verifies its age through zero-knowledge proof without revealing his personal data like birth-date.
3. The online service provider verifies the proof using the blockchain.
4. Access is granted upon successful validation, with no additional user data stored.

Figure 3 illustrates that the use case2 is best to maintain user privacy.

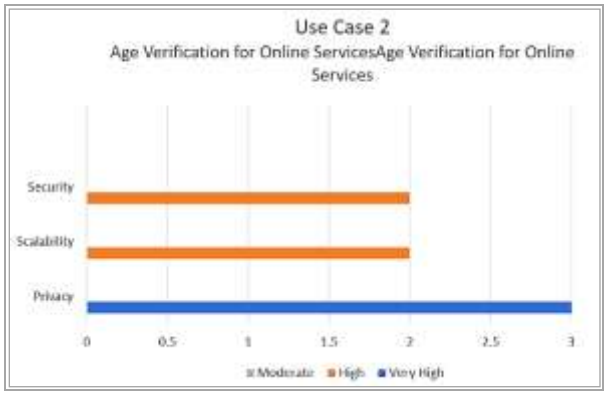


Figure 3: Parameters validation of use case 2

Use Case 3 (University Credential Validation)

Scenario: A business needs to swiftly and safely confirm a candidate's academic background. The validation steps are given below:

1. The user shares a digitally signed degree credential from their wallet with the employer.
2. The employer queries the blockchain to check the credential's authenticity and revocation status.
3. The blockchain confirms the credential's validity and trusted issuer.
4. The employer gains assurance of the applicant's academic qualifications without needing physical copies.

Figure 4 illustrates use case 3 is best suitable to validate credentials, ensuring high level of security.

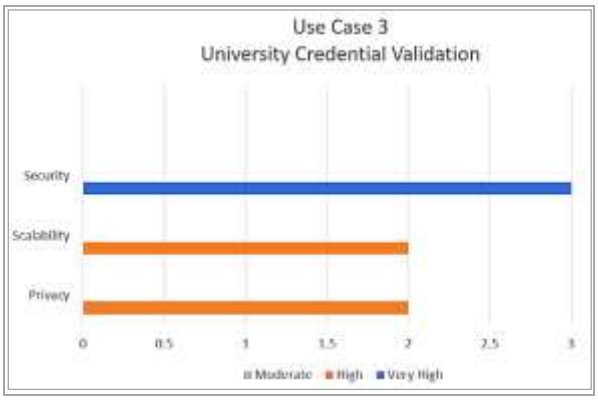


Figure 4: Parameters validation of use case 3

Use Case 4: Multi-Service Authentication in Smart Cities

Scenario: A user uses a single federated identity to access a variety of city services, including events, libraries, and public transportation. The validation steps are as follows:

1. The user authenticates with one city service (e.g., public transport) using their digital wallet.
2. The service verifies the credentials via the blockchain.
3. Federated authentication shares the verified credentials with other city services.
4. The user accesses multiple services seamlessly without separate logins.

From Figure 5, we can see that use case 4 provides great level of scalability while ensuring security. But it lags in terms of user privacy.

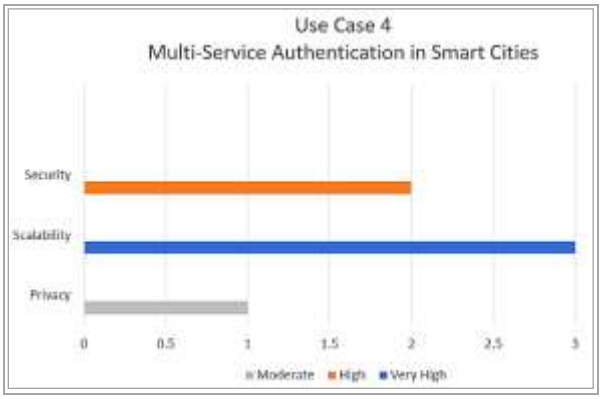


Figure 5: Parameters validation of use case 4

Use Case 5 (Credential Revocation of Suspicious Credentials)

Scenario: To safeguard the ecosystem, an issuer revokes a credential when it discovers fraudulent conduct. The validation steps are shown below:

1. The issuer updates the credential's status as revoked on the blockchain.
2. All verifiers are automatically notified of the revocation.
3. Before accepting the credential, the Verifiers query the blockchain and detect its revoked status.
4. To ensure trust and regain access, users must revalidate or reissue new credentials.

Figure 6 illustrates that the use case5 is best to provide security while credentials revocation. It also provides appropriate level of privacy.

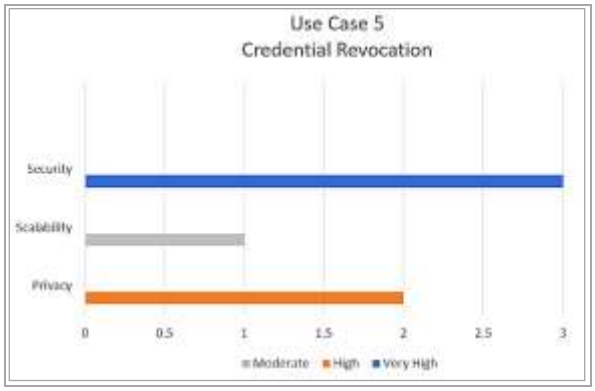


Figure 6: Parameters validation of use case 5

Table 2: Detailed comparison and validation of use cases

Use Cases	Privacy	Scalability	Security
Cross-Border Healthcare Access	High	High	Very High
Age Verification for Online Services	Very High	High	High
University Credential Validation	High	High	Very High
Multi-Service Authentication in Smart Cities	Moderate	Very High	High
Credential Revocation	High	Moderate	Very High



Figure 7: The obtained results and comparison of applied use cases in view of privacy, scalability and Security parameters

The obtained results are presented in Table 2 after validating the use cases by applying performance parameters that are privacy, security and scalability. Furthermore, it is evident from Figure 7 that the said parameters are equally important concerns on the performance scale whereas top concerns identified after the comparative analysis of applied use cases are Security and Privacy respectively. Hence, our proposed approach is user-centric, that provides users the complete control over their digital identities in a very secure way. The credential verification through zero-knowledge proofs ensures privacy and don't reveal sensitive

information of user. This is useful in many scenarios. The best best-fitting scenarios are also discussed above. This provides interoperability among different platforms through VCs and standards like W3C DIDs. Nevertheless, Security is a key consideration. End-to-end encryption of sensitive data and multi-factor authentication make it robust and secure. Identity hubs serve as off-chain mechanism to kept sensitive data while ensuring data accessibility. Allow users to authenticate on multiple platforms through federated authentication. This aspect ensures cross-border scalability. Moreover, System adaptability is a great strength. Issuers do necessary updates in credential schemas to ensure compliance with changing technologies and regulations. Comprehensive governance framework assists in operational as well legal issues. They guaranteeing adoption and transparency according to international standards. The proposed approach has removes centralized authorities and provides decentralized, scalable, and robust identity management solution. Blockchain is used as a trust anchor to make system transparent and immutable.

This study's results do not suggest a generic improvement, but rather a few concrete differences to the studies reviewed earlier. The present framework differs by validating a single design end-to-end against a set of use cases defined by, and tested by, practitioners, and by evaluating 31 SSI solutions against 22 non-functional requirements but not going so far as to create a catalogue comparing their respective merits. Vaios et al. (2022) integrated SSI with eIDAS and FIDO to enhance authentication, where the strong security scores found here for credential validation and credential revocation were used, but focused on the regulatory alignment of SSI with European regulation, not on scalability trade-offs, which we have shown here is a live tension, not a solved one, once multiple services are federated together. Jana et al. (2023) and Junli et al. (2024) both improved specific mechanisms, password-less access and privacy-preserving revocation respectively, and our results corroborate their premise that zero-knowledge proofs and revocation handling are central to security outcomes, since three of the five use cases in this study score security as very high specifically because of those two mechanisms. Where this work diverges from Nigang et al. (2023) and Engin et al. (2024), whose contributions were largely conceptual accounts of the shift from centralized to federated identity, is in offering an empirically ranked account of which properties are hardest to deliver simultaneously; the Multi-Service Authentication in Smart Cities case in particular shows that scalability gains from federated authentication can come at the cost of privacy, a trade-off that the conceptual literature does not surface because it does not test competing properties against one another.

The contribution of this study is not so much to propose a new primitive as to bridge the gap between architectural proposals and operational behaviour. Previous research has been mostly successful in demonstrating the technical viability of decentralized identity, and this research further points to contexts where such systems work well out of the box (credential validation, credential revocation, health/wellbeing access) and where they require intentional design compromises (smart city federation, where privacy must be balanced with scale). If it is a research program that is about real deployment, not proof of concept, then it does matter: it tells implementers which use cases can be adapted to the architecture with very little tuning, and which will require further privacy-preserving mechanisms (such as selective disclosure policies tuned per federation partner) to scale further.

Conclusion and Future Work

SSI in decentralized federated identDFIM is a secure, privacy-conscious and scalable architecture. It decentralizes identity management and provides trust via blockchain technology, provides privacy with zero-knowledge proofs, and provides usability across domains with federated authentication. It has been practically validated in five different scenarios including Healthcare, Education and Smart cities. More work is needed to further develop scalability for high-transaction volumes, and to consider more advanced cryptographic techniques before simulation or pilot deployments to refine performance and usability. As new standards are developed, the framework will gain even more practical and robust features with its enhanced interoperability and as it incorporates AI-driven fraud detection capabilities.

References

Badirova, A., Moghaddam, F. F., & Yahyapour, R. (2024). Integration of self-sovereign identity in centralized identity management: SSI-based authentications, attribute-based authorization. *2024 11th International Conference on Future Internet of Things and Cloud (FiCloud)*, 362–367.

Bai, Y., et al. (2022). Decentralized and self-sovereign identity in the era of blockchain: A survey. *2022 IEEE International Conference on Blockchain (Blockchain),* 500–507.

Boi, B., De Santis, M., & Esposito, C. (2024). Decentralized identity management and privacy-enhanced federated learning for automotive systems: A novel framework. *2024 IEEE 27th International Symposium on Real-Time Distributed Computing (ISORC),* 1–6.

Bolgouras, V., Angelogianni, A., Politis, I., & Xenakis, C. (2022). Trusted

and secure self-sovereign identity framework. *Proceedings of the 17th International Conference on Availability, Reliability and Security.*

Butincu, C. N., & Alexandrescu, A. (2024). Design aspects of decentralized identifiers and self-sovereign identity systems. *IEEE Access, 12, 60928–60942*.

Deng, H., Liang, J., Zhang, C., Liu, X., Zhu, L., & Guo, S. (2024). FutureDID: A fully decentralized identity system with multi-party verification. *IEEE Transactions on Computers, 73*(8), 2051–2065.

Ding, Y., et al. (2024). Data aggregation management with self-sovereign identity in decentralized networks. IEEE Transactions on Network and Service Management, 21(6), 6174–6189.

Fang, J., Feng, T., Guo, X., & Wang, X. (2024). Privacy-enhanced distributed revocable identity management scheme based on self-sovereign identity. *Journal of Cloud Computing: Advances, Systems and Applications, 13*(1).

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2023). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. *Business & Information Systems Engineering.*

Goel, A., & Rahulamathavan, Y. (2024). A comparative survey of centralised and decentralised identity management systems: Analysing scalability, security, and feasibility. *Future Internet, 17*(1), 1.

Liu, Y., Zhao, B., Zhao, Z., Liu, J., Lin, X., Wu, Q., & Susilo, W. (2024). SS-DID: A secure and scalable Web3 decentralized identity utilizing multi-layer sharding blockchain. *IEEE Internet of Things Journal, 11*(15), 25694–25705.

Luong, D. A., & Park, J. H. (2023). Privacy-preserving identity management system on blockchain using ZK-SNARK. *IEEE Access, 11*, 1840–1853.

Mirza, S. M. H., Das, T. K., Sakib, M. N., & Ferdous, M. S. (2024). Decentralised identity federations using blockchain. *International Journal of Information Security.*

Nokhbeh, R., Kai, Z., Chang, C., Huang, T.-C., Liau, D., Song, W., Tyagi, A., Barber, K., Khalil, M., Lamison, M., & Pandey, S. (2021). *Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study.*

Nusantoro, H., et al. (2021). *Blockchain-based authentication for identity management. 2021 9th International Conference on Cyber and IT Service Management (CITSM),* 1–8.

Raipurkar, A. R., et al. (2023). Digital identity system using blockchain-

based self-sovereign identity & zero knowledge proof. *2023 OITS International Conference on Information Technology (OCIT),* 611–616.

Raghav, R., & Chaudhary, A. (2023). Authentication system and authorization system using blockchain technology. *2023 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, 1–6.

Roy, S. K. (n.d.). Decentralized identity and access management (IAM) and self-sovereign identity. *International Journal of Research in Engineering, Science and Management.*

ShareID. (n.d.). Centralized vs. decentralized identity: *Which is right for your company?* https://www.shareid.ai/blog/centralized-vs-decentralized-identity

Sibahee, A., Abduljabbar, Z. A., Ngueilbaye, A., Luo, C., Li, J., Huang, Y., Zhang, J., Khan, N., Nyangaresi, V. O., & Ali, A. H. (2024). Blockchain-based authentication schemes in smart environments: A systematic literature review. *IEEE Internet of Things Journal,* 1–1.

Sidhu, S. S., Nguyen, M. N. H., Ngene, C., & Rouhani, S. (2022). Trust development for blockchain interoperability using self-sovereign identity integration. *In 2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 0033–0040). IEEE.

Sun, N., Zhang, Y., & Liu, Y. (2023). A universal privacy-preserving multi-blockchain aggregated identity scheme. *Applied Sciences,* 13(6), 3806.

Tan, K. J., Chi, C.-H., & Lam, K.-Y. (2023). Survey on digital sovereignty and identity: From digitization to digitalization. *ACM Computing Surveys.*

Thorve, A., et al. (2022). Decentralized identity management using blockchain. *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N),* 1985–1991.

Zargar, G. R., Barati, H., & Barati, A. (2024). An authentication mechanism based on blockchain for IoT environment. *Cluster Computing, 27*(9), 13239–13255.

Zeydan, E., Blanco, L., Mangues-Bafalluy, J., Arslan, S. S., Turk, Y., Kumar Yadav, A., & Liyanage, M. (2024). Blockchain-based self-sovereign identity: Taking control of identity in federated learning. *IEEE Open Journal of the Communications Society, 5,* 5764–5781.