International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 10 | Oct - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Literature Review on the Digicred:Decentralized Identity and Credential System for D-Apps

Anirudh A *Department of Computer Science and Engineering(Cyber Security) Vimal Jyothi Engineering College*
Chemperi, Kannur
Email: anirudhrajan5@gmail.com

Aksh Jolly *Department of Computer Science and Engineering(Cyber Security) Vimal Jyothi Engineering College*
Chemperi, Kannur Email: akshcoc9@gmail.com

Abhiram P V *Department of Computer Science and Engineering(Cyber Security) Vimal Jyothi Engineering College*
Chemperi, Kannur
Email: anuthomas7781@gmail.com

Jinshith Jayaraj
Department of Computer Science
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:jinshithjayaraj3@gmail.com

Mr.Arun Pushpan
Assistant Professor
Department of Computer Science
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:arunpushpan@vjec.ac.in

***Abstract*—The paradigm of digital identity is rapidly shifting from centralized monopolistic control toward decentralized user-centric frameworks to meet the demands of Web3, immersive computing and trustless interactions. Traditional identity systems expose users to privacy breaches, vendor lock-in and cross-platform incompatibilities, creating barriers for seamless adoption. To overcome these challenges DIGICRED introduces a decentralized identity and credential system built on Self-Sovereign Identity (SSI) principles leveraging Decentralized Identifiers (DIDs) and blockchain-based cryptographic proofs as the foundation for trust. A verifiable credential layer enables selective disclosure of tamper-proof claims ranging from academic certifications to government-issued IDs preserving privacy while ensuring interoperability. Complementing this a multi-dimensional reputation system fosters trust in anonymous environments, mitigates Sybil attacks and incentivizes meaningful participation across decentralized applications. By integrating privacy-preserving technologies, compliance-aware architectures and scalable trust mechanisms DIGICRED redefines identity management for Web3. This shift marks the emergence of secure portable and user-controlled digital identities laying the groundwork for the future of decentralized applications and cross-platform digital ecosystems.**

***Index Terms*—Self-Sovereign Identity (SSI), Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), Blockchain, Web3, Digital Identity, Privacy Preservation, Reputation Systems, Trust Management, Cross-Platform Interoperability. .**

I. Introduction

In the modern digital landscape, the reliance on centralized identity management systems has increasingly revealed critical limitations such as vulnerability to large-scale data breaches, lack of user sovereignty over personal credentials, interoperability gaps across platforms and difficulties in meeting evolving regulatory and compliance requirements. As digital ecosystems expand into domains like finance, healthcare, education and government services, the need for secure, trustworthy and user-centric identity solutions has become more urgent than ever. DIGICRED addresses this challenge by introducing a decentralized identity and credential management framework that leverages blockchain technology, decentralized identifiers (DIDs) and verifiable credentials to create a transparent, tamper-resistant and scalable identity infrastructure. The system is built on the principles of self-sovereign identity, enabling individuals to own, control and selectively disclose their credentials without dependency on centralized authorities. By incorporating zero-trust security models, cryptographic assurances and interoperability mechanisms, DIGICRED not only enhances privacy and security but also facilitates seamless credential exchange across diverse ecosystems. Furthermore, it provides a sustainable pathway for building trust in digital interactions while ensuring compliance with privacy regulations and supporting adaptability for future technological growth.

II. Literature Survey

Ferdous et al. [1] introduce SSI4Web, a Self-Sovereign Identity (SSI) framework aimed at replacing traditional password-based authentication in web services. Recognizing that usernames and passwords remain a major source of security breaches and user inconvenience, the authors propose a blockchain-enabled solution built upon Hyperledger Indy and Hyperledger Aries. The framework leverages decentralized identifiers (DIDs) and verifiable credentials (VCs) to facilitate passwordless, privacy-preserving authentication where users retain full control of their identity data. The paper details the system architecture, implementation, and a proof-of-concept validated through threat modeling and requirement analysis. Reported advantages include reduced reliance on password management, cross-device usability, and enhanced

TABLE I
COMPARISON TABLE

Reference	Name	Advantages	Disadvantages
[1]	SSI4Web: A Self-sovereign Identity (SSI) Framework for the Web	• Clear taxonomy of threats and countermeasures • Provides future research directions	• Very broad scope, less technical depth • Risk of becoming outdated quickly
[2]	C4 model in a Software Engineering subject to ease the comprehension of UML and the software	• Standards-oriented, useful for industry adoption • Shows practical application example	• Narrower focus, lacks broader perspectives • Limited technical depth or performance evaluation
[3]	Decentralized and Self-Sovereign Identity: Systematic Mapping Study	• Provides a clear framework and layered architecture for intelligent agents • Highlights multiple practical applications	• Raises privacy, ethical, and scalability challenges without concrete solutions • Highly futuristic, so implementation feasibility remains uncertain
[4]	Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective	• Offers a broad interdisciplinary perspective • Identifies key challenges and barriers to adoption clearly	• Lacks technical depth on underlying technologies • No empirical validation or case studies,mostly theoretical
[5]	Decentralized Identity: Where Did It Come From and Where Is It Going?	• Unifies OS and software-defined principles • Highly scalable for any system	• Generic model creates design trade-offs • Significant security and privacy risks
[6]	SSI Strong Authentication using a Mobile-phone based Identity Wallet Reaching a High Level of Assurance	• Unified architecture for crowdsourcing platforms • Improves development with core frameworks	• Complex kernel is difficult to maintain • Requires developers to add algorithms
[7]	What is a (Digital) Identity Wallet? A Systematic Literature Review	• PC-like abstraction simplifies home management • Supports incremental and organic growth	• Diagnosing wireless connectivity is difficult • Functionality limited by device vendors
[8]	Design Aspects of Decentralized Identifiers and Self-Sovereign Identity Systems	• Simplifies campus app development with APIs • Open ecosystem for community contributions	• Testing community features is challenging • Migrating existing campus apps is hard
[9]	Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology	• Owners control media quality access by user trust • Uses smart encryption and servers for smooth performance	• Relies on one authority, which can fail or slow things down • Hard to manage many changing access rules
[10]	SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone	• The paper reveals a new way to spy on touchscreens using reflections • They built a system that can detect touches and recover inputs from videos automatically	• Attack works only with good lighting, angles, and steady recording • Better at stealing short codes like PINs than long texts

TABLE II
COMPARISON TABLE

Reference	Name	Advantages	Disadvantages
[11]	Comparative Analysis of Decentralized Identity Approaches	• Protects user privacy by keeping data on-device • Cuts communication costs with efficient updates	• Performance drops with non-IID data • Relies on device availability and stable connectivity
[12]	Twin3: Pluralistic Personal Digital Twins via Blockchain	• Performs many tasks without supervision • Performance scales well with model size	• Practical performance can be rudimentary • Training data overlaps with test sets
[13]	Web3-Powered Service Provisioning in Cellular Networks using NFT and Self-Sovereign Identity	• First foundation model for forecasting • Simplifies forecasting to one step	• Simpler models better for small data • Many open questions and limitations remain
[14]	A Systematisation of Knowledge: Connecting European Digital Identities with Web3	• Proactively aligns features before training • Improves convergence speed and accuracy	• Sensitive to hyper-parameter choices
[15]	Privacy in Digital Identity Systems	• Enables large models on clients • Resolves task gradient conflicts effectively	• Split learning increases communication costs

user privacy. Nevertheless, the study identifies limitations such as the absence of wallet backup mechanisms, user learning curves, and susceptibility to denial-of-service attacks. Overall, SSI4Web highlights a novel approach to integrating SSI into mainstream web authentication and outlines future research directions toward federated identity models, secure wallet backup, and large-scale adoption

Andrea Va´zquez-Ingelmo et al. [2] in their study "C4 model in a Software Engineering subject to ease the comprehension of UML and the software development process" (2020) address the persistent challenges faced by students in understanding UML within software engineering education. Despite prior adoption of active learning methodologies such as project-based learning, UML remains difficult due to its extensive syntax and the "model-code gap" that separates abstract models from executable code. To mitigate this, the authors propose incorporating the C4 model—a framework consisting of four levels of abstraction (context, containers, components, and code)—as a complement to UML. Their approach emphasizes the use of the first two C4 levels during the requirements elicitation phase, enabling students to conceptualize system architecture without excessive technical detail. This integration supports better system documentation, strengthens abstraction skills, and bridges the gap between high-level models and real-world applications. The study concludes that combining the C4 model with UML can enhance comprehension, improve project outcomes, and increase student motivation in software engineering subjects.

Andrea Va´zquez-Ingelmo et al. [3] in their study "C4 model in a Software Engineering subject to ease the comprehension of UML and the software development process" address the persistent challenges faced by students in understanding UML within software engineering education. Despite prior adoption of active learning methodologies such as project-based learning, UML remains difficult due to its extensive syntax and the "model-code gap" that separates abstract models from executable code. To mitigate this, the authors propose incorporating the C4 model—a framework consisting of four levels of abstraction (context, containers, components, and code)—as a complement to UML. Their approach emphasizes the use of the first two C4 levels during the requirements elicitation phase, enabling students to conceptualize system architecture without excessive technical detail. This integration supports better system documentation, strengthens abstraction skills, and bridges the gap between high-level models and real-world applications. The study concludes that combining the C4 model with UML can enhance comprehension, improve project outcomes, and increase student motivation in software engineering subjects.

Rui Oliveira et al. [4] in their paper "Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective" examine the urgent need to secure critical infrastructures (CIs) against emerging threats posed by quantum computing. As quantum capabilities evolve, traditional public-key cryptographic schemes such as RSA and ECC are increasingly vulnerable, endangering essential services including energy, transport, healthcare, and communications. The authors analyze post-quantum cryptography (PQC) algorithms

proposed by NIST, discussing their applicability to CIs in terms of performance, scalability, and resilience. They argue that transitioning to PQC is particularly challenging in critical infrastructure environments due to long system lifecycles, interoperability demands, and stringent real-time constraints. The paper also explores hybrid cryptographic solutions and phased migration strategies as practical approaches for deployment. Ultimately, the study concludes that proactive integration of PQC into CI cybersecurity frameworks is vital to ensure future resilience, highlighting the necessity of early adoption, cross-sector collaboration, and standardization efforts.

Alan Bachmann et al. [5] provide an overview of Decentralized Identity (DI) also referred to as Self-Sovereign Identity (SSI) tracing its evolution from earlier models such as centralized, federated and user-centric identity. The paper highlights how blockchain and distributed ledger technology (DLT) have enabled the emergence of decentralized identifiers (DIDs) and verifiable credentials which allow individuals to control their own digital identities without reliance on centralized providers. The work emphasizes the open and interoperable standards being developed at W3C and other communities while also showcasing early proof-of-concept implementations like ID2020, uPort, Sovrin and CULedger. One of its notable contributions is positioning decentralized identity as a user-centric model that enhances privacy, portability and trust in digital interactions. However the research identifies key challenges such as interoperability, regulatory compliance (e.g. GDPR's "right to be forgotten"), usability of privacy controls and the need for robust governance frameworks. Future directions include strengthening security and privacy mechanisms, developing sustainable trust networks and integrating DI with existing identity infrastructures to create a scalable global identity ecosystem .

Andreas Abraham et al. [6] propose a framework for achieving strong authentication in Self-Sovereign Identity (SSI) systems using a mobile phone-based identity wallet designed to reach the highest Level of Assurance (LoA High). While traditional SSI wallets provide user control over identity data they fall short of meeting stringent assurance requirements for sensitive services such as eGovernment or public administration. To address this gap the authors define system requirements based on standards like ISO 29115 and eIDAS and design a generic wallet architecture that combines a mobile secure element with an external FIDO2 hardware token. Their proof-of-concept implementation on iOS demonstrates feasibility by leveraging secure enclaves, biometric authentication, cryptographic accumulators for privacy-preserving revocation and multi-factor authentication. The evaluation shows that their approach can meet LoA High and enable SSI systems for sensitive use cases. The work identifies remaining challenges such as usability issues of hardware tokens, lack of key backup and reliance on trusted identity providers. Future research should explore improving usability without compromising assurance and extending interoperability across diverse SSI ecosystems .

G.G. Dagher et al. [7] introduce Blockcerts, an open standard for creating, issuing and verifying blockchain-based certificates that enable individuals to have tamper-evident, portable and independently verifiable digital credentials. Unlike traditional digital certificates that rely on centralized authorities Blockcerts leverages Bitcoin's blockchain to ensure persistence and trust without dependence on a single entity. The system architecture consists of an issuer component, a recipient wallet and a verification portal allowing certificates to be anchored on the blockchain while sensitive data remains off-chain. One of the significant contributions is that Blockcerts supports lifelong credential ownership giving users sovereignty over their academic, professional and personal certificates. However challenges remain in terms of blockchain scalability, certificate revocation and integration with existing institutional systems. The authors suggest future work should address broader interoperability with emerging standards such as DIDs and Verifiable Credentials and explore adoption across different sectors to establish a global ecosystem of blockchain-based credentials .

Divya Singh et al. [8] present a comprehensive study on the design aspects of Decentralized Identifiers (DID) and Self-Sovereign Identity (SSI) systems by analyzing their architectural foundations, technical requirements and governance dimensions. The paper explains how DID and SSI aim to shift digital identity management from centralized models to user-centric ecosystems where individuals gain autonomy, privacy and portability of their credentials. The authors discuss critical components such as lifecycle management of identities, issuance and verification of verifiable credentials, interoperability across heterogeneous platforms and establishment of trust through cryptographic protocols and governance frameworks. A detailed evaluation of blockchain and distributed ledger technologies highlights their role as enabling infrastructures for decentralization while also surfacing issues like transaction throughput, scalability limitations, privacy preservation and compliance with global data protection regulations. The paper further emphasizes the socio-technical challenges of adoption including usability of wallets, lack of universally accepted standards, cross-border legal alignment and ensuring inclusivity in identity provisioning. By mapping current gaps, the authors argue that sustainable SSI ecosystems require not only technical robustness but also transparent governance models, interoperability frameworks and human-centric design principles that can balance innovation with accountability. They conclude that future research should prioritize privacy-by-design approaches, regulatory harmonization and community-driven trust models to establish SSI as a widely accepted and secure paradigm for next-generation digital identity infrastructures.

Nitin Naik et al. [9] explore the pressing challenges of digital identity management and sovereignty in their work on Self-Sovereign Identity (SSI) specifications. The paper critiques traditional centralized and federated identity management models for their inability to provide individuals with full ownership, control and privacy over their digital identities. To address these limitations the authors propose a comprehensive framework of specifications to evaluate SSI

solutions, emphasizing principles such as sovereignty, user-controlled storage, longevity of credentials, verifiability of claims, privacy preservation, interoperability across systems and scalability for large-scale adoption. Applying these specifications, the paper presents a comparative analysis of two leading SSI platforms: uPort, which operates on the Ethereum blockchain, and Sovrin, developed on Hyperledger Indy. Their evaluation reveals that while both systems adhere to core SSI requirements such as sovereignty and verifiability they struggle with challenges related to scalability, interoperability and continuous operational availability. Sovrin demonstrates stronger privacy and security features through mechanisms like zero-knowledge proofs and governance-oriented trust frameworks, whereas uPort is recognized for its simplicity, ease of use and developer accessibility. The study underscores that although these platforms represent major advances in the SSI paradigm, true global adoption will depend on the creation of standardized protocols, development of cross-platform interoperability frameworks and optimization for scalability and reliability. The authors conclude that SSI has strong potential to redefine digital identity management by enabling secure, privacy-preserving and user-centric ecosystems but sustained progress requires overcoming significant technical and governance hurdles.

Zhengan Huang et al. [10] present SBLWT: A Secure Blockchain Lightweight Wallet Based on TrustZone, a novel approach to improving the security and efficiency of blockchain wallets. The authors highlight that traditional blockchain wallets face critical issues such as private key leakage, susceptibility to malware attacks and high computational costs, all of which undermine the reliability of blockchain-based identity and transaction systems. To address these challenges the paper leverages ARM TrustZone technology to design a secure lightweight wallet architecture that isolates sensitive operations in a trusted execution environment (TEE). This ensures that private keys, cryptographic computations and wallet-related operations remain protected even if the main operating system is compromised. The authors evaluate SBLWT across parameters such as resilience against attacks, computational efficiency, scalability and usability. Their findings demonstrate that SBLWT not only enhances protection from key theft and malware intrusion but also reduces resource consumption compared to conventional wallet designs, thereby maintaining lightweight performance. One of the notable contributions of this work is its ability to integrate hardware-based security mechanisms with blockchain systems, providing a practical balance between strong security guarantees and operational efficiency. The study concludes that SBLWT offers a promising pathway for secure identity management, trusted transactions and privacy-preserving operations in decentralized ecosystems, while also suggesting that future research should focus on improving cross-platform adaptability and extending TEE-based security models for broader blockchain applications.

Harikrishnan Rajendran et al. [11] propose a blockchain-based digital identity management framework designed to enhance privacy, trust and security in decentralized ecosystems. The paper critiques existing centralized and federated identity models for issues such as single points of failure, lack of user control and vulnerability to data breaches. To overcome these limitations the authors design an identity system that leverages blockchain's immutability and transparency to provide verifiable, tamper-resistant credentials under a self-sovereign identity (SSI) model. Their framework introduces mechanisms for secure key management, selective disclosure of credentials and decentralized verification processes that minimize dependence on third-party authorities. The evaluation demonstrates that the system strengthens resistance to identity theft, enhances interoperability across platforms and ensures higher assurance in identity validation compared to traditional models. However the study also identifies challenges such as blockchain scalability, latency and compliance with evolving privacy regulations. The authors suggest that future research should focus on optimizing blockchain performance, improving usability of identity wallets and establishing standardized governance models to facilitate large-scale adoption of decentralized identity solutions.

Lukas Reisch et al. [12] present Twin3: Pluralistic Personal Digital Twins via Blockchain, a framework that addresses the limitations of existing personal digital twin (PDT) solutions in terms of trust, sovereignty and interoperability. The paper defines PDTs as digital counterparts of individuals that enable data-driven personalization, decision-making and automation across multiple domains but notes that current implementations often depend on centralized infrastructures that undermine user autonomy and restrict cross-domain adoption. To overcome these shortcomings the authors design Twin3, a blockchain-based framework that integrates decentralized identifiers (DIDs) and verifiable credentials (VCs) to ensure transparency, accountability and tamper resistance while granting individuals self-sovereign control of their identities and associated data. The architecture supports pluralism by enabling multiple coexisting PDTs that can interact seamlessly across heterogeneous domains without compromising privacy or autonomy. Through conceptual modeling and architectural design, the study demonstrates how Twin3 facilitates scalable, trustworthy and privacy-preserving orchestration of services that enhance interoperability and user empowerment. The authors conclude that pluralistic PDTs can form the foundation of next-generation decentralized ecosystems by enabling secure identity management, seamless cross-platform integration and personalized service delivery, while also highlighting the need for future research on usability, governance and real-world deployment.

Nischal et al. [13] propose a Web3-driven framework for cellular service provisioning that integrates Self-Sovereign Identity (SSI) and Non-Fungible Tokens (NFTs) to overcome the limitations of traditional mobile networks. Conventional provisioning methods rely on centralized operators, SIM-based authentication and rigid subscription models that constrain user autonomy, create security vulnerabilities and hinder interoperability across service providers. To address these short-

comings the authors design a decentralized architecture where SSI enables privacy-preserving authentication and portability of user identities across operators, while NFTs function as verifiable and transferable service entitlements. The framework leverages blockchain infrastructure to ensure transparency, traceability and trust without dependence on centralized authorities. Through conceptual modeling and prototype discussion the paper demonstrates how tokenized entitlements and decentralized identity management can streamline onboarding, simplify roaming procedures and enable the creation of flexible service bundles in 5G and beyond. The authors conclude that Web3-powered service provisioning represents a significant step toward user-sovereign, secure and interoperable mobile ecosystems, while emphasizing open challenges in scalability, regulatory compliance and integration with next-generation telecom infrastructures.

F. Ulbricht et al. [14] present A Systematisation of Knowledge: Connecting European Digital Identities with Web3, a comprehensive study that examines the convergence of European regulatory frameworks with emerging decentralized identity technologies. The paper traces the evolution of digital identity models from centralized and federated approaches to blockchain-based solutions, emphasizing the distinction between self-sovereign identity (SSI) and decentralized identity within the context of the European Union's eIDAS 2.0 regulation. By analyzing developments from 2005 to 2024, the authors highlight the tensions between traditional OpenID Connect (OIDC)-based infrastructures and Web3-enabled identity frameworks that leverage decentralized identifiers (DIDs) and verifiable credentials (VCs). The study identifies key challenges including interoperability across heterogeneous systems, privacy preservation, regulatory compliance and the usability of identity wallets. At the same time, it underscores the necessity of digital identity bridges that can seamlessly integrate European Digital Identity Wallets (EUDIW) with Web3 applications to ensure cross-domain trust and adoption. The authors conclude that decentralized identity in Europe is positioned at a critical intersection of regulation, innovation and societal trust, and future research must focus on aligning technical plurality with robust governance, user sovereignty and secure large-scale deployment.

Artem Khatchatourov [15] in his paper Privacy in Digital Identity analyzes the role of privacy as a central challenge in the design and deployment of digital identity systems. The study highlights how conventional identity management approaches often expose users to risks such as surveillance, profiling and misuse of personal data due to their reliance on centralized authorities and weak privacy controls. To address these issues the paper investigates how privacy principles can be systematically integrated into digital identity infrastructures by examining regulatory, organizational and technological perspectives. It emphasizes the importance of embedding privacy-by-design methodologies, implementing minimal disclosure techniques and ensuring user-centric control over personal data. The analysis also considers the broader sociotechnical implications noting that privacy in digital identity is not only a technical requirement but also a foundation for trust, autonomy and democratic participation in digital societies. The author concludes that sustainable digital identity ecosystems must reconcile functionality and usability with strong privacy protections and future research should focus on aligning technical standards with evolving legal frameworks and user expectations.

III. Conclusion

This study of DIGICRED illustrates a clear technological progression towards decentralized and self-sovereign digital identity, enabled by the convergence of blockchain, decentralized identifiers (DIDs) and verifiable credentials (VCs). These innovations move beyond the fragility of traditional username and password systems by offering tamper-resistant identity proofs, privacy-preserving verification and seamless interoperability across platforms. DIGICRED provides essential guarantees of user sovereignty, enabling individuals to own and manage their credentials without reliance on centralized authorities, while also supporting advanced features such as cross-chain identity, credential verification and decentralized reputation building. Yet despite this potential, significant challenges remain. Interoperability across heterogeneous ecosystems requires stronger standardization, scalability issues in blockchain networks must be addressed to support widespread adoption and regulatory frameworks must evolve to balance compliance with user autonomy. As decentralized applications expand and Web3 ecosystems mature, solutions like DIGICRED point toward one possible direction for secure, user-controlled and privacy-preserving identity infrastructures, provided the community can overcome these persistent hurdles in scalability, governance and usability.

References

[1] M. S. Ferdous, A. Ionita, and W. Prinz, "Ssi4web: A self-sovereign identity (ssi) framework for the web," in *International Congress on Blockchain and Applications*. Springer, 2022, pp. 366–379.

[2] A. Va´zquez-Ingelmo, A. Garc´ıa-Holgado, and F. J. Garc´ıa-Pen˜alvo, "C4 model in a software engineering subject to ease the comprehension of uml and the software," in *2020 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2020, pp. 919–924.

[3] S˘. C˘ uc˘ko and M. Turkanovic´, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE access*, vol. 9, pp. 139 009–139 027, 2021.

[4] J. O. del Moral, A. deMarti iOlius, G. Vidal, P. M. Crespo, and J. E. Martinez, "Cybersecurity in critical infrastructures: A post-quantum cryptography perspective," *IEEE Internet of Things Journal*, vol. 11, no. 18, pp. 30 217–30 244, 2024.

[5] O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, E. Maler, D. Reed, and M. Sporny, "Decentralized identity: Where did it come from and where is it going?" *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 10–13, 2019.

[6] A. Abraham, C. Schinnerl, and S. More, "Ssi strong authentication using a mobile-phone based identity wallet reaching a high level of assurance." in *SECRYPT*, 2021, pp. 137–148.

[7] B. Podgorelec, L. Alber, and T. Zefferer, "What is a (digital) identity wallet? a systematic literature review," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2022, pp. 809–818.

[8] C. N. Butincu and A. Alexandrescu, "Design aspects of decentralized identifiers and self-sovereign identity systems," *IEEE Access*, vol. 12, pp. 60 928–60 942, 2024.

[9] N. Naik and P. Jenkins, "Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology," in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. IEEE, 2020, pp. 90–95.
[10] W. Dai, J. Deng, Q. Wang, C. Cui, D. Zou, and H. Jin, "Sblwt: A secure blockchain lightweight wallet based on trustzone," *IEEE access*, vol. 6, pp. 40 638–40 648, 2018.
[11] M. Alizadeh, K. Andersson, and O. Schele´n, "Comparative analysis of decentralized identity approaches," *IEEE Access*, vol. 10, pp. 92 273– 92 283, 2022.
[12] M. H. Wen and J. C.-W. Lin, "Twin3: pluralistic personal digital twins via blockchain," *IEEE Access*, 2024.
[13] N. Aryal, F. Ghaffari, E. Bertin, and N. Crespi, "Web3-powered service provisioning in cellular networks using nft and self-sovereign identity," in *2024 6th Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*, 2024, pp. 1–8.
[14] B. Biedermann, M. Scerri, V. Kozlova, and J. Ellul, "A systematisation of knowledge: Connecting european digital identities with web3," in *2024 IEEE International Conference on Blockchain (Blockchain)*, 2024, pp. 605–610.
[15] A. Khatchatourov, M. Laurent, and C. Levallois-Barth, "Privacy in digital identity systems: models, assessment, and user adoption," in *International Conference on Electronic Government*. Springer, 2015, pp. 273–290.