IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Comparative Analysis Of Self-Sovereign Identity (SSI) Solutions

[1]Swapnil Gaidhani, [2]Dr. Gopal Krishna Sharma

[1]Research Scholar, [2]Assistant Professor and Head

[1]Department of Computer Science,

[1]Dev Sanskriti Vishwavidyalaya, Haridwar, India

Abstract: The management of digital identity is undergoing a significant transformation, moving away from centralized and federated models towards the user-centric paradigm of Self-Sovereign Identity (SSI). SSI aims to empower individuals with greater control, privacy, and security over their personal data. This paper presents a comparative analysis of prominent SSI solutions and related platforms, including Privado ID, Hyperledger Indy, Sovrin, the uPort ecosystem (Serto and Veramo), Jolocom, Sora ID, ShoCard (as integrated by Ping Identity), Wipro Dice ID, and Curity Identity Server. The analysis employs a framework evaluating key criteria such as underlying architecture, governance models, adherence to standards (W3C DIDs and VCs), core features, security and privacy mechanisms, interoperability potential, scalability considerations, and ecosystem maturity. The research outcomes indicate a notable heterogeneity in technological methodologies, encompassing dedicated distributed ledger technology (DLT)-based networks as well as integrated functionalities within pre-existing identity and access management (IAM) platforms. The dynamics of the market, including the anticipated cessation of the Sovrin MainNet, the progressive development of uPort, and strategic acquisitions such as the procurement of ShoCard by Ping Identity, play a pivotal role in shaping the ecosystem. Notwithstanding advancements in standardization, obstacles pertaining to interoperability, user-friendliness, key management, governance, and regulatory compliance continue to endure. This manuscript provides a comprehensive analysis of the contemporary landscape of self-sovereign identity (SSI) solutions, elucidating their distinguishing characteristics and the challenges that hinder their extensive adoption.

Index Terms - Digital Identity, Centralized Credentials, Federated Identity, Decentralized Identity, Self-Sovereign Identity, Literature Review, Historical Analysis, Comparative Analysis, Thematic Coding.

I. INTRODUCTION

A. The Evolving Landscape of Digital Identity

For numerous decades, the field of digital identity management has been predominantly characterized by both centralized and federated frameworks. Centralized systems, in which a singular authority is responsible for the issuance and management of identities, are plagued by intrinsic vulnerabilities, including the establishment of single points of failure, heightened susceptibility to extensive data breaches, and a fundamental deficiency of user autonomy concerning personal data. Users frequently find themselves bound by the policies and potential shortcomings of the central authority, with their identities at risk of vanishing should the organization encounter failure.[1] Federated models, while distributing trust across multiple identity providers (IdPs), still present challenges, including potential privacy violations through user tracking across services and the persistence of identity silos.[2] Both models often lead to the over-sharing of personal information, increase the risk of identity theft through fraudulent replication, and can result in administrative inefficiencies and inconsistent data across platforms.[3] These limitations have fueled concerns about data misuse, lack of transparency, and the overall security of personal information online.[4]

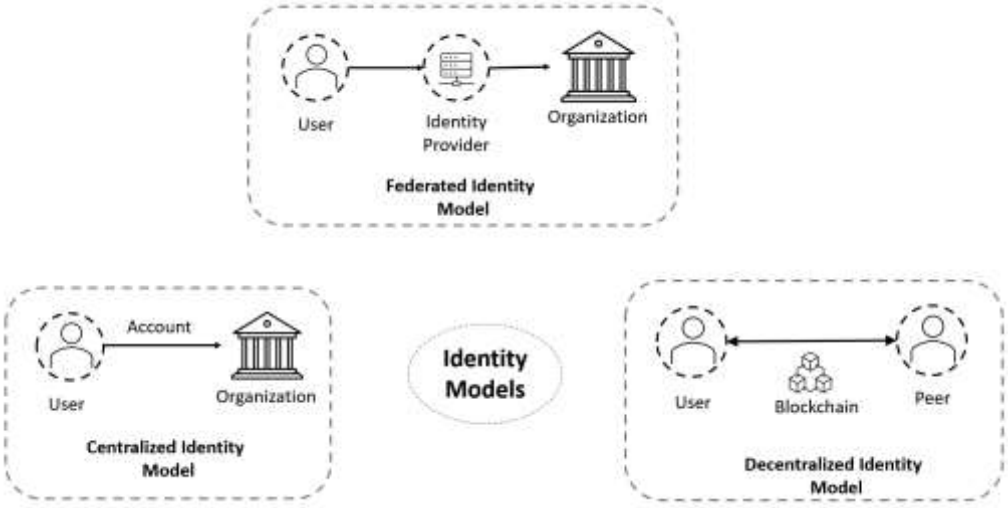

Figure 1 Identity Models

B. Rationale for Comparative Analysis of SSI Solutions

The increasing scholarly attention towards SSI has catalyzed the emergence of various platforms and solutions endeavoring to operationalize its foundational principles.[5] These solutions exhibit significant diversity in their underlying architectures, technological choices (e.g., specific DLTs or non-DLT approaches), governance models, and feature sets.[6] This heterogeneity necessitates a structured comparative analysis to understand the strengths, weaknesses, trade-offs, and suitability of different solutions for various applications. Furthermore, the SSI landscape is dynamic and evolving rapidly. Significant market events, such as the anticipated shutdown of the Sovrin MainNet [7], the strategic split of the pioneering uPort project into Serto and Veramo [8], and the acquisition of SSI startups like ShoCard by established IAM vendors like Ping Identity [9], underscore the volatility and maturation challenges within the ecosystem. These developments highlight that while core W3C standards like DIDs and VCs provide a common foundation [1], the paths to implementation, sustainable operation, and market adoption are fragmenting and consolidating simultaneously. This suggests a critical phase where technical merit must be balanced with viable governance and economic models, making a current, comparative assessment essential for researchers, developers, and potential adopters.

C. Research Objectives and Paper Structure

The primary objective of this research paper is to conduct a comprehensive comparative analysis of prominent SSI solutions: Privado ID, Hyperledger Indy, Sovrin, the uPort ecosystem (Serto/Veramo), Jolocom, Sora ID, ShoCard/Ping Identity, Wipro Dice ID, and Curity Identity Server. This paper is predicated on a delineated framework that includes architecture, governance, adherence to standards, functionalities, security measures, interoperability, scalability, and levels of maturity. Secondary objectives include elucidating the foundational concepts of SSI, identifying key differentiating factors among the solutions, discussing persistent challenges hindering widespread adoption, and providing insights into the potential future trajectory of the SSI landscape.

The paper is organized in the following manner: Section II elucidates the foundational concepts and principles of Self-Sovereign Identity (SSI), encompassing the roles, essential technologies (Decentralized Identifiers, Verifiable Credentials, Distributed Ledger Technology/Cryptography), and the fundamental objectives. Section III delineates the framework for comparative analysis, as well as the evaluation criteria employed therein. Section IV offers a comprehensive analysis of each selected SSI solution in relation to these established criteria. Section V integrates the findings through a comparative discourse, emphasizing critical divergences, convergences, and the repercussions of recent advancements within industry. Section VI addresses the principal obstacles encountered in the adoption of SSI and investigates emerging trends alongside prospective trajectories. Section VII furnishes concluding observations, encapsulating the principal findings and providing a definitive viewpoint on the current landscape of SSI solutions.

II. Foundational Concepts of Self Sovereign Identity

A. Core Principles and Goals of SSI

SSI is guided by a set of core principles, often attributed to Christopher Allen, designed to ensure user control and data protection.[3] These principles articulate the fundamental requirements for a truly self-sovereign system [10]:

Table 1 Self-Sovereign System Principles

Principle	Description
Existence	Independent existence in the digital realm, not dependent on administrators or central authorities
Control	Users must be the ultimate authority over their identities and data usage
Access	Users must have access to their own data without barriers
Transparency	Systems and algorithms must be open, understandable, and publicly verifiable
Persistence	Identities should be long-lasting and not subject to external organization failures
Portability	Users must be able to transport identity data and credentials across services
Interoperability	Identities should be usable across different systems and contexts
Consent	Users must explicitly consent to the use and sharing of their data
Minimization	Disclosure of personal data should be limited to what is necessary
Protections	User rights, particularly privacy, must be protected through safeguards

These principles collectively aim to achieve several key goals: enhancing user privacy and security by minimizing data exposure and central points of attack; empowering users with direct control over their digital representations [3]; reducing identity fraud and tampering through cryptographic verification [7]; eliminating data silos and enabling seamless, trusted interactions across diverse platforms [2];and improving efficiency by streamlining verification processes.[3]

B. The SSI Trust Triangle: Issuers, Holders, and Verifiers

The operational model of SSI is often conceptualized as a "Trust Triangle," involving three primary roles [10]:

- **Issuer:** Authorized entity that issues Verifiable Credentials containing claims about a subject.
- **Holder:** An individual or organization designated with the responsibility of securely preserving and regulating access to Verifiable Credentials.
- **Verifier:** An entity tasked with the duty of authenticating the genuineness and integrity of credentials through the application of cryptographic techniques.

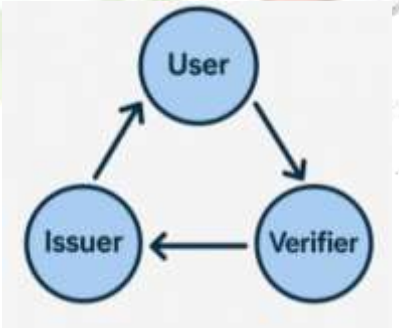

Figure 2 Self-Sovereign Identity Trust Triangle

The flow typically involves the Issuer creating and signing a VC, delivering it to the Holder. The Holder stores it and later, upon request from a Verifier, creates a Verifiable Presentation (potentially containing claims from multiple VCs and selectively disclosing information) and presents it to the Verifier. The Verifier checks the cryptographic proof associated with the presentation and the underlying VC(s) to establish trust.[10] While this model clearly defines the roles and interactions, it simplifies the complex nature of trust establishment. Trust in the Issuer's authority to make claims and trust in the Verifier's responsible handling of received data remain critical considerations that often require additional mechanisms like governance frameworks, reputation systems, or advanced privacy techniques like Zero-Knowledge Proofs (ZKPs) to fully address.[11]

C.Key Enabling Technologies

SSI relies on a combination of emerging and established technologies, standardized primarily by the W3C, to enable its core functionalities.

Decentralized Identifiers (DIDs)

DIDs are a novel type of globally unique identifier designed specifically for verifiable, decentralized digital identity. Unlike traditional identifiers (email addresses, usernames, domain names) that are typically issued and controlled by centralized authorities, DIDs are designed to be generated and controlled by the identity subject themselves. They are URIs with a specific syntax: did:method:method-specific-identifier. [1]

- **did::** The URI scheme identifier.
- **method::** Specifies the DID Method, which defines the technical mechanism for how DIDs of this type are created, resolved, updated, and deactivated (CRUD operations). Examples include did:key, did:web, did:ethr, did:sov,did:indy.[6]
- **method-specific-identifier::** A unique identifier within the namespace of the specified DID method.

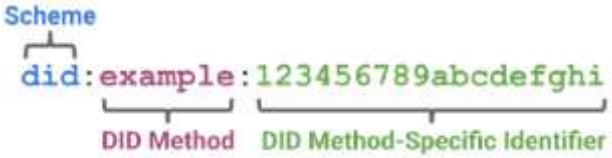

Figure 3 Decentralized Identifier Syntax [1]

- **Verification Methods:** Public keys or other cryptographic material used to authenticate or authorize interactions with the DID subject (e.g., verifying digital signatures).[1]
- **Service Endpoints:** Network addresses or service descriptions defining how to interact with the DID subject (e.g., an agent endpoint for secure messaging). [1]

The process of retrieving the DID Document associated with a DID is called DID Resolution. This typically involves interacting with a Verifiable Data Registry (VDR) defined by the specific DID Method, such as a distributed ledger, a web server, or even being self-contained within the DID string itself (did:key). The diversity of DID Methods allows for flexibility but also presents interoperability challenges.[6]

Verifiable Credentials

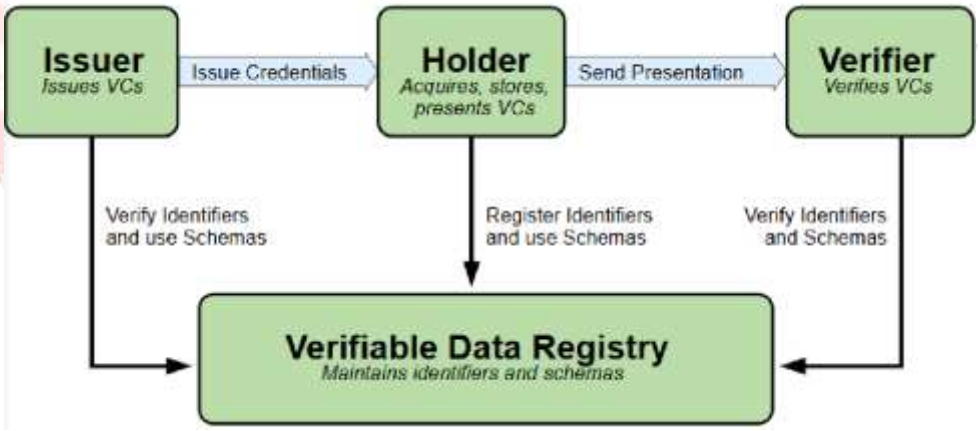

Figure 4 Verifiable Credentials Specification

VCs provide a standard way to represent claims made by an Issuer about a subject in a tamper-evident and cryptographically verifiable format.[3] They are the digital equivalent of physical credentials like passports, driver's licenses, or diplomas, but with enhanced security and privacy features.[12] The W3C Verifiable Credentials Data Model defines the core structure, typically represented in JSON-LD or as a JWT [6]:

- **Metadata:** Information about the credential itself, such as its type, the Issuer's DID (issuer), issuance date (issuanceDate), expiration date (expirationDate), and status (e.g., regarding revocation).[13]
- **Credential Subject:** Contains the claims (statements) the Issuer is making about the subject, identified by the subject's DID (id). Claims are represented as property-value pairs (e.g.,"alumniOf": "Example University").[13]
- **Proof:** Cryptographic proof (e.g., a digital signature) generated by the Issuer.[14] This allows anyone to verify that the credential was issued by the claimed Issuer and that its contents have not been altered since issuance. [13]

Holders can create Verifiable Presentations from one or more VCs to present to Verifiers. Presentations allow for selective disclosure, meaning the Holder can choose to reveal only specific claims required for an interaction, enhancing privacy. [13] Presentations also include proof generated by the Holder, demonstrating control over the presented credentials.

The Role of Distributed Ledger Technology (DLT) and Cryptography

While not strictly mandated by the core DID and VC specifications [1], Distributed Ledger Technologies (DLTs), particularly blockchains, play a significant role in many SSI implementations. DLTs often serve as the Verifiable Data Registry (VDR) for:

- Anchoring DIDs: Storing DID Documents or pointers to them, ensuring they are publicly resolvable and tamper-resistant.
- Publishing Public Keys: Making the verification keys associated with DIDs discoverable.
- Storing Schemas and Credential Definitions: Providing a common reference point for the structure and semantics of VCs.
- Managing Revocation Status: Publishing information about revoked credentials in a verifiable and often privacy-preserving manner (e.g., using revocation registries or status lists). [15]

The immutability and transparency characteristics of DLTs make them well-suited for these functions, providing a high degree of trust in the integrity of the registered information. However, it is crucial to note that for privacy reasons, the Verifiable Credentials themselves, which contain personal data, are typically stored off-ledger (e.g., in the Holder's digital wallet) and exchanged via peer-to-peer communication channels.[13] The association of SSI solely with blockchain is a common misconception; the actual requirement is for a verifiable registry for public information, which DLT fulfills effectively but is not the only option, as demonstrated by methods like did:web (relying on web servers) and did:key (self-contained).[1]

Cryptography is the fundamental underpinning of SSI security and trust. Key cryptographic techniques include:

- **Asymmetric Cryptography (Public/Private Keys):** Used for generating DIDs, creating digital signatures for VCs and presentations, and enabling secure authentication. The Holder maintains control of their private key, proving ownership of their DID and credentials. [1]
- **Digital Signatures:** Ensure the authenticity (proof of origin) and integrity (tamper-evidence) of VCs and DID Documents. [13]
- **Hashing:** Used to create unique fingerprints of data, often employed in Merkle Trees for efficient verification within DLTs.[16]
- **Zero-Knowledge Proofs (ZKPs):** Advanced cryptographic techniques allowing a Holder to prove the truth of a statement (e.g., "I am over 18") based on their VCs without revealing the underlying data (e.g., their actual date of birth). This significantly enhances privacy and data minimization.[17]

III. Comparative Analysis Framework

A.Methodology Overview

This study employs a qualitative comparative analysis methodology to evaluate the selected SSI solutions. The analysis is based on information gathered from publicly available resources, including official documentation, technical specifications, whitepapers, academic publications [18], industry reports, and project repositories, primarily utilizing the provided research snippets. Each solution is systematically assessed against a predefined set of evaluation criteria detailed below. The objective is to furnish a systematic analysis that emphasizes the principal similarities, disparities, advantages, and disadvantages.

It is important to acknowledge the limitations inherent in this approach. The study is contingent upon the precision and thoroughness of the existing documentation, which may differ among various solutions. Moreover, the field of SSI is distinguished by its swift innovation and developmental trajectory, signifying that certain information may rapidly become obsolete. Applying a consistent set of criteria across technologically diverse solutions—ranging from DLT-centric platforms to integrated IAM features—requires careful interpretation of each solution's specific context and positioning, presenting a methodological consideration in ensuring fair comparison.

B.Evaluation Criteria Definition

To facilitate a structured and comprehensive comparison, the following evaluation criteria have been defined, drawing upon key aspects discussed in the reviewed literature and technical documentation:

- **Architecture:** Examines the fundamental design and technology stack. This includes the underlying platform (e.g., specific DLT, cloud service, standalone library), consensus mechanism (if applicable), core software components (e.g., ledger nodes, agents, SDKs), supported DID methods, preferred VC formats, and overall system modularity.[2]
- **Governance:** Assesses the control structure and decision-making processes governing the solution. This includes the type of governing body (e.g., non-profit foundation, corporate entity, open-source community project, consortium), transparency of operations, mechanisms for updates and changes, and the model for financial sustainability, including any associated costs or fees for usage.[14]
- **Standards Compliance:** Evaluates adherence to key industry standards critical for interoperability. This primarily focuses on compliance with W3C DID Core v1.0 [1], W3C VC Data Modelv1.1/2.0 [12], support for specific, standardized DID methods[19], compatibility with common VC formats (JWT, JSON-LD)[6], support for interoperable communication protocols like DIDComm [3], and alignment with relevant DIF specifications or profiles.[14]
- **Features & Functionality:** Details of the specific capabilities offered by the solution. This includes mechanisms for key generation and management, credential issuance, verification, and revocation processes, support for advanced privacy features like selective disclosure and ZKP integration [20], the nature and capabilities of associated agents or wallets, availability and quality of developer tools (SDKs, APIs), and support for specific use cases (e.g., KYC, authentication, authorization).[10]
- **Security & Privacy:** Assesses the measures taken to protect user data and ensure system integrity. This covers the cryptographic algorithms employed, implementation of privacy-enhancing techniques (e.g., use of pairwise DIDs, off-ledger VC storage [15], ZKPs [20], data minimization practices [10]),considerations for known threats based on available threat models [18], and the auditability of identity-related events.[21]
- **Interoperability & Portability:** Gauges the solution's ability to interact with other SSI ecosystems and allow users to manage their identity across platforms. Key indicators include support for standard communication protocols (DIDComm, OpenID4VC/VP), use of standardized DID methods and VC formats, and the ease with which users can migrate their identities and credentials away from the specific solution.[2]
- **Scalability:** Considers the solution's capacity to handle a large volume of users, DIDs, credentials, and transactions efficiently. This involves evaluating potential bottlenecks related to the underlying architecture, consensus mechanisms, or registry performance. [2]
- **Maturity & Ecosystem:** Evaluates the solution's stage of development and the surrounding community. Factors include the project's age, the size and activity level of its developer and user community, the number and scope of documented deployments or pilot projects, the quality and availability of documentation and support resources, significant partnerships, and recent impactful developments (e.g., major updates, acquisitions, splits, shutdowns).[14]

These criteria provide a multi-faceted lens for evaluation, acknowledging that the success and suitability of an SSI solution depend not only on its technical capabilities but also on its governance, standardization, ecosystem support, and practical viability.

Table 2 Summary of Evaluation Criteria

Criterion	Definition / Scope
Architecture	Underlying technology stack (DLT, cloud, library),consensus, core components (DID methods, VC formats, wallet), modularity.
Governance	Control model (foundation, company, community),decision-making, transparency, sustainability, cost/fee structure.
Standards Compliance	Adherence to W3C DID Core, W3C VC Data Model, specific DID methods, VC formats (JWT/JSON-LD),DIDComm, DIF specs, OpenID4VC/VP.
Features & Functionalities	Key management, VC lifecycle (issue/verify/revoke), privacy features (selective disclosure, ZKP), agent/wallet capabilities, developer tools.
Security & Privacy	Cryptographic methods, privacy techniques (pairwise DIDs, ZKP, off-chain storage), threat model considerations, data minimization, auditability.
Interoperability & Portability	Interaction with other ecosystems, support for standard protocols (DIDComm, OpenID4VC/VP), ease of identity/credential migration.
Scalability	Capacity to handle large numbers of users, transactions, and credentials; performance characteristics.
Maturity & Ecosystem	Project age, community size/activity, deployments/pilots, documentation/support, partnerships, recent developments (shutdowns, acquisitions).

IV. Analysis of Prominent SSI Solutions

This section provides an individual analysis of each selected SSI solution based on the evaluation criteria defined in Section III.

A. Privado ID

Privado ID positions itself as middleware infrastructure and tooling for applications implementing privacy-preserving digital identity, strongly emphasizing user data ownership and Zero-Knowledge Proofs (ZKPs). It is an open-source project under MIT/Apache licenses, built upon the technology stack formerly known as Polygon ID. Its focus use cases include Know Your Customer(KYC) processes and establishing Sybil resistance.[20]

Analysis against Criteria:

- **Architecture:** Functions as middleware, leveraging ZKPs extensively. It operates on EVM-compatible blockchains, with current deployments on Polygon Testnet (Amoy) and PolygonPoS Mainnet. It utilizes DIDs and VCs, storing VCs off-chain in user wallets (including a web wallet accessible via authenticator). ZKPs are used for credential verification and selective disclosure, generated client-side. [20]
- **Governance:** Governed by its open-source nature (MIT/Apache licenses) and likely influenced by its origins within the Polygon ecosystem. [20] A formal external governance body is not explicitly mentioned in the provided materials.
- **Standards Compliance:** Explicitly states adherence to SSI principles and implementation of W3C (DIDs, VCs) and DIF standards. Leverages ZKPs, a key technology in advanced SSI implementations. [20]
- **Features & Functionality:** Offers reusable credentials, instant identity verification flows, a web wallet, ZKP-based verification, selective disclosure, tools like Schema and Query Builders for developers, and aims for ecosystem interoperability. Supports KYC and identity verification use cases. [20]
- **Security & Privacy:** Core focus on privacy ("Privacy First, Security Always") through ZKPs, user control over data, and minimizing data liability for verifiers. User data is encrypted and decrypted client-side.
- **Interoperability & Portability:** Promotes an ecosystem approach, allowing interaction with multiple credential providers. Adherence to W3C/DIF standards facilitates interoperability. Portability depends on wallet implementations and standard compliance.
- **Scalability:** Relies on the scalability of the underlying EVM blockchain (Polygon) and the efficiency of ZKP generation/verification.

- **Maturity & Ecosystem:** Evolved from Polygon ID, indicating significant development effort.[22] Provides developer resources and promotes an ecosystem model. [20] Being open-source fosters community potential.

Strengths & Weaknesses:

- **Strengths:** Strong focus on privacy through ZKPs, open-source, adherence to standards, developer tools, leverages performant blockchain (Polygon).
- **Weaknesses:** Maturity as an independent entity post-Polygon ID branding might be developing, reliance on ZKP technology adds complexity.

B.Hyperledger Indy

A prominent project under the Linux Foundation's Hyperledger umbrella, Indy provides tools, libraries, and reusable components specifically designed for building decentralized identity solutions rooted on distributed ledgers.[23] It is not an end-user application itself but a foundational technology stack used to build identity networks, most notably the Sovrin network.[15] Its core components include indy-node (the server/ledger software), indy-plenum (the consensus protocol implementation), and client SDKs (though the original indy-sdk is being deprecated in favor of libraries within the Hyperledger Aries project).[24]

Analysis against Criteria:

- **Architecture:** Employs a purpose-built, permissioned DLT.[25] Consensus is achieved using Indy Plenum, an implementation of Redundant Byzantine Fault Tolerance (RBFT).[26] RBFT involves parallel instances of a 3-phase commit protocol operating on batches of transactions, combined with transaction validation. State is stored using a Merkle Patricia Trie. Key components are the node software, the Plenum consensus engine, and client interaction tools (historically SDK, now Aries components). [25] Primarily uses the did:indy DID method and the AnonCreds Verifiable Credential format, which natively supports ZKPs.[23]
- **Governance:** Governed under the Hyperledger project structure within The Linux Foundation, following open-source principles and community-driven development. Specific Indy networks built upon it (like Sovrin) have their own governance frameworks.[27]
- **Standards Compliance:** Defines its own DID method (did:indy). While pioneering many SSI concepts, its native AnonCreds format predates and differs from the W3C VC Data Model standard, although mapping is possible. Supports DIDComm for agent communication. ZKP implementation is core via AnonCreds.[17]
- **Features & Functionality:** Natively supports correlation-resistant pairwise DIDs.[15] Provides ZKP capabilities through AnonCreds for selective disclosure and privacy. Defines specific roles within its networks (Steward, Trustee, Trust Anchor, Endorser) with distinct permissions for writing different transaction types (NYM, SCHEMA, CRED_DEF,REVOC_REG_DEF, etc.) to the ledger.[23]
- **Security & Privacy:** Designed with privacy as a core goal, utilizing pairwise DIDs and ZKPs to minimize data correlation and disclosure. Security relies on the BFT nature of the consensus protocol and cryptographic primitives.
- **Interoperability & Portability:** Strong interoperability within the Indy/Aries ecosystem. Interoperability with non-Indy systems can be challenging due to the prevalence of AnonCreds versusW3C standard VCs, though efforts exist to bridge this gap.
- **Scalability:** RBFT consensus performance depends on the number of participating nodes (Stewards). Designed for permissioned networks, scalability characteristics differ from public permissionless blockchains.[26]
- **Maturity & Ecosystem:** An established and mature project within the Hyperledger portfolio, forming the basis for several production and pilot networks. Has an active developer community, although the shift from indy-sdk to Aries components represents an evolution in the client tooling strategy. [25]

Strengths & Weaknesses:

- **Strengths:** Purpose-built for SSI, mature DLT foundation, strong privacy features (pairwise DIDs, ZKPs via AnonCreds), established governance under Linux Foundation, active community within Hyperledger Aries.
- **Weaknesses:** Reliance on AnonCreds format creates interoperability friction with W3C VC standard, permissioned model requires network bootstrapping and governance, SDK transition to Aries adds complexity for developers.

C.Sovrin

Sovrin aimed to be a global public utility for self-sovereign identity, built upon the Hyperledger Indy codebase.[27] It was governed by the non-profit Sovrin Foundation and operated as a public, permissioned network where approved organizations (Stewards) ran the validator nodes.[17] Sovrin was a pioneer in the SSI space, launching its network in 2017.[28] However, in late 2024, the Sovrin Foundation announced the likely shutdown of its MainNet ledger by March 31, 2025, or sooner, citing sustainability challenges.[7]

Analysis against Criteria:

- **Architecture:** Directly based on Hyperledger Indy's DLT, consensus (RBFT), and state management.[15] Conceptualized with three layers: Credential Exchange (off-ledger P2P), Agent-to-Agent (communication), and Sovrin Ledger (on-ledger registry for DIDs, schemas, etc.). Operated as a public permissioned network. [29]
- **Governance:** Governed by the Sovrin Foundation through the Sovrin Governance Framework (SGF). [27] Stewards (trusted organizations) operated nodes under agreement with the Foundation. A Board of Trustees oversaw business/legal aspects. The announced shutdown cited significant governance challenges, including limited Steward involvement in governance and financial burdens ($2M debt).[7]
- **Standards Compliance:** Utilized the did:sov method (based on Indy) and primarily the AnonCreds VC format. Contributed significantly to early SSI concepts but faced challenges aligning with evolving W3C standards.
- **Features & Functionality:** Supported public DIDs, schemas, credential definitions, and revocation registries on the ledger. VCs were exchanged and stored off-ledger via agents.[17] Defined roles like Issuer, Holder, Verifier, Agent, and Steward. Utilized ZKPs inherited from Indy/AnonCreds.
- **Security & Privacy:** Emphasized Privacy by Design principles, leveraging Indy's features like pairwise DIDs and ZKPs.
- **Interoperability & Portability:** Primarily interoperable within the Sovrin/Indy/Aries ecosystem. Challenges existed in broader interoperability due to AnonCreds usage.
- **Scalability:** Inherited scalability characteristics and limitations of the underlying Hyperledger Indy RBFT consensus mechanism.
- **Maturity & Ecosystem:** A pioneering network launched in2017.[28] However, declining MainNet usage, lack of new Transaction Endorser adoption in 2024, regulatory uncertainty, technical resource strains, and governance issues led to the likely shutdown decision. [7] This highlights the difficulty in sustaining such a public utility model.

Strengths & Weaknesses:

- **Strengths:** Pioneering role in SSI, established a global network based on Indy, strong focus on governance frameworks(initially), utilized robust privacy features.
- **Weaknesses:** Facing likely shutdown due to sustainability issues (usage, funding, governance), reliance on AnonCreds impacted broader W3C interoperability, governance model proved challenging to maintain effectively.

D. uPort Ecosystem: Serto and Veramo

The original uPort project, an early SSI initiative built on the public, permissionless Ethereum blockchain [29], underwent a strategic evolution, splitting into two distinct projects: Serto and Veramo. Both projects aim to carry forward uPort's mission of decentralizing the internet and empowering users with data control. Serto appears focused on enterprise solutions and usability, while Veramo provides a modular JavaScript framework for developers building verifiable data applications. [8]

Analysis against Criteria (Serto):

- **Architecture:** Focuses on enabling enterprises to use DIDs and VCs, positioning itself as a low-code platform for decentralized identity and connected data solutions. It utilizes a "Serto Agent" and supports DID methods like did:web. It builds on the legacy and tooling of uPort, aiming for usability and enterprise implementation.[30] Specific underlying DLT or infrastructure details beyond did:web usage are less clear from the provided snippets.
- **Governance:** Appears to be a commercially driven entity, potentially linked to ConsenSys Mesh. It is listed as a company offering solutions on AWS Marketplace and has competitors in the enterprise identity space. Founded in 2020.
- **Standards Compliance:** Emphasizes W3C standards for DIDs and VCs. Used W3C compliant schemas in examples. [30]

- **Features & Functionality:** Provides tools for creating/issuing DIDs and VCs. [30] Focuses on making data portable, private, and valuable. Enables identity linking across different platforms (website, social, NFTs).
- **Security & Privacy:** Inherits the goals of SSI regarding privacy and user control, aiming to make data more private. Specific mechanisms depend on implementation details not fully covered.
- **Interoperability & Portability:** Aims to make data portable. Adherence to W3C standards should aid interoperability. [30]
- **Scalability:** Dependent on the chosen underlying technologies(e.g., did:web relies on web server scalability).
- **Maturity & Ecosystem:** Evolved from the uPort project around 2021. Targets enterprise adoption. Listed as an unfunded startup with active competitors.

Analysis against Criteria (Vermo):

- **Architecture:** A modular JavaScript framework built around a core agent concept with pluggable functionality. Designed to run through Node.js, browsers, and React Native. Provides APIs for managing DIDs, VCs, keys, and communication protocols.[31]
- **Governance:** Open-source project under the Apache 2.0 license. Housed under the Decentralized Identity Foundation (DIF).[32] Encourages community contributions and plugin development.
- **Standards Compliance:** Strongly aligns with W3C standards for DIDs and VCs, and DIF specifications. [32] Supports DIDComm messaging.[33] Natively supports core DID methods: did:ethr, did:web, did:key. Extensible architecture allows adding support for other methods via plugins (e.g., did:cheqd plugin exists). [34] Supports both JWT and JSON-LD VC formats.[35]
- **Features & Functionality:** Provides comprehensive tooling for developers: key management, DID creation/resolution/management, VC issuance/verification/storage, selective disclosure presentation, secure messaging (DIDComm), event system, CLI tool. [34] Designed to handle complexity and interoperability challenges across different standards. [32]
- **Security & Privacy:** Enables building applications adhering to SSI principles. Security depends on the chosen plugins and underlying key management.
- **Interoperability & Portability:** High focus on interoperability through standards compliance and modular plugin architecture. Aims to avoid vendor lock-in. [30]
- **Scalability:** As a framework, scalability depends on the application built with it and the underlying infrastructure used (e.g., DID method choice, storage solutions).
- **Maturity & Ecosystem:** Evolved from uPort, benefits from that experience. Active open-source project with community engagement (Discord, GitHub Discussions). [31] Used as a foundation by other projects like Cheqd and Identify Snap. Provides template repositories for plugin development. [32]

Strengths & Weaknesses (Serto):

- **Strengths:** Enterprise focus builds on uPort legacy, supportsW3C standards, aims for usability (low-code).
- **Weaknesses:** Less technical details available in provided snippets compared to Veramo, commercial nature might limit openness, ecosystem seems less defined than Veramo's.

Strengths & Weaknesses (Veramo):

- **Strengths:** Highly modular and extensible, strong standards compliance supports multiple platforms, open source under DIF, active community, addresses interoperability challenges.
- **Weaknesses:** Primarily a developer framework requires building applications on top, complexity inherent in its flexibility.

E.Jolocom

Jolocom provides a protocol and SDK aimed at being a universal, lightweight, open-source solution for decentralized digital identity and access rights management.[36] The Jolocom SDK serves as a toolkit for managing SSI Agents and their interactions.[37]

Analysis against Criteria:

- **Architecture:** Built as a protocol aggregating existing SSI specifications. The SDK (written in TypeScript) acts as an" Agent Factory," managing storage and DID method resolution for the agents it creates. Relies on underlying DID methods for anchoring and resolution. [36] Requires polyfills for browser/React Native environments. [37]

- **Governance:** Open-source project with code available on GitHub under Apache 2.0 license.
- **Standards Compliance:** Explicitly builds upon W3C DID and VC specifications.
- **Features & Functionality:** Enables creation of self-sovereign identities (human, org, agent), association of VCs with identities, and interaction flows for sharing/receiving verifiable information. Supports creating/verifying signed credentials, managing public profiles, and credential request/issuance flows. SDK provides interfaces for Agent management and Interactions.
- **Security & Privacy:** Relies on the security mechanisms of the chosen DID Method for message security. Enables standard SSI privacy patterns through VCs.
- **Interoperability & Portability:** Achieved through adherence toW3C standards.
- **Scalability:** Depends on the scalability of the underlying DID methods and infrastructure used.
- **Maturity & Ecosystem:** Provides documentation and an SDK. GitHub repository shows activity. Appears less prominent in recent discourse compared to some other solutions analyzed. [37]

Strengths & Weaknesses:

- **Strengths:** Open source, lightweight protocol approach, adheres to W3C standards, provides SDK and documentation.
- **Weaknesses:** Seems less actively discussed or adopted compared to platforms like Indy or frameworks like Veramo based on available snippets, requires developers to integrate and build upon the SDK.

*F. **Sora ID***

Sora ID focuses on providing fast and secure identity verification by linking verified user identities to "secure, portable cryptographic credentials". It aims to streamline KYC, improve passthrough rates, lower costs, reduce fraud, and offer passwordless login capabilities.[38]

Analysis against Criteria:

- **Architecture:** Employs a network model where verified credentials contribute to the network's trust. Integrates with multiple data sources for verification and uses device/environmental signals for fraud detection. Provides a dashboard for configuring KYC flows. Stores Personally Identifiable Information (PII) centrally ("PII is stored by SoraID").[39] Uses "cryptographic credentials" and offers biometric device-based login.[40]
- **Governance:** Appears to be a commercial service offering, governance likely internal to the company providing Sora ID.
- **Standards Compliance:** Mentions using "secure, portable cryptographic credentials" and adherence to "open-source standards". However, explicit confirmation of using W3CDID/VC standards is not present in the specific snippets about Sora ID. General snippets on VCs/DIDs [3] discuss the standards but don't confirm Sora ID's implementation details.
- **Features & Functionality:** Core focus on identity verification (IDV) and KYC. Offers customizable decisioning flows, passwordless login using the Sora ID credential, biometric authentication, ongoing fraud checks (OFAC, PEP), and audit trails. Provides an API aimed at developers. [40]
- **Security & Privacy:** Claims user control over data and uses biometrics for security. However, the statement that "PII is stored by Sora ID" contrasts with typical SSI principles aiming to minimize centralized PII storage. States "No data selling".
- **Interoperability & Portability:** Interoperability depends heavily on whether standard DIDs/VCs are used. The network model seems focused internally. Portability of credentials outside the Sora ID ecosystem is unclear from the data.
- **Scalability:** As a likely cloud-based service, scalability depends on Sora ID's infrastructure.
- **Maturity & Ecosystem:** Positioned as a solution for the identity verification market, focusing on improving existing processes like KYC.

Strengths & Weaknesses:

- **Strengths:** Clear focus on IDV/KYC market needs, offers passwordless login, includes fraud detection features, provides customization dashboard.
- **Weaknesses:** Centralized PII storage model deviates from core SSI privacy principles, lack of explicit confirmation on W3CDID/VC standards usage in provided snippets raises interoperability questions, governance is commercial/closed.

F. ShoCard (Acquired by Ping Identity)

ShoCard was a personal identity startup focused on user control and privacy, leveraging blockchain technology and mobile devices as identity vaults. It was acquired by Ping Identity, a major IAM vendor, in April 2020 (announced October 2020).[9] ShoCard's technology has since been integrated into the Ping Intelligent Identity Platform and forms the basis for offerings like PingOne Neo.[41] It was notably used for Ping's "Project COVID Freedom" vaccine passport initiative.[42]

Analysis against Criteria:

- **Architecture:** Utilized a mobile application as a personal identity vault, secured with biometrics (facial/fingerprint). Employed blockchain technology for aspects of its security model. Now integrated within the broader Ping Identity platform architecture. [9]
- **Governance:** Originally a startup, now governed entirely by PingIdentity as part of its product portfolio.
- **Standards Compliance:** Focused on concepts of "personal identity" and "sovereign identity". Used the concept of validated claims, akin to Verifiable Credentials, which could be shared via various channels. Post-acquisition integration likely aligns with Ping's broader standards strategy.
- **Features & Functionality:** Allowed users to collect validated claims (proof of employment, ID, etc.) in their mobile wallet. Enabled selective disclosure and user control over sharing. Provided real-time verification capabilities for businesses. Facilitated streamlined onboarding and interactions.
- **Security & Privacy:** Marketed as a privacy-first approach, putting users in control and allowing businesses to avoid storing sensitive user data. Leveraged mobile biometrics and blockchain security.
- **Interoperability & Portability:** As part of the Ping platform, interoperability is likely focused within Ping's ecosystem and supported standards (e.g., SAML, OIDC). Portability outside Ping may be limited.
- **Scalability:** Scalability is now tied to the Ping Intelligent Identity Platform's capabilities.
- **Maturity & Ecosystem:** ShoCard technology was in beta/pilot stages at acquisition. It has since been integrated and productized by Ping Identity, a mature IAM vendor, lending it enterprise credibility and distribution.[29]

Strengths & Weaknesses:

- Strengths: Innovative mobile-centric approach, focus on user control and privacy, integration into a leading IAM platform provides enterprise reach and support.
- Weaknesses: Technology is now proprietary to Ping Identity, potential for vendor lock-in, original blockchain/decentralization aspects might be less prominent post-integration.

G. Wipro Dice ID

Wipro's Decentralized Identity platform (referred to as Dice ID in app stores) utilizes blockchain technology to enable individuals, organizations, and devices to manage their identities securely via a digital wallet.[4] A mobile application, "Wipro DICEID," is available on app stores.

Analysis against Criteria:

- **Architecture:** Explicitly blockchain-powered. Follows the Issuer-Subject-Verifier model. Utilizes Verifiable Credentials stored in a user-controlled wallet (mobile app). Verification can be initiated via QR codes. [4]
- **Governance:** Developed and offered by Wipro Limited, suggesting a commercial product governance model.
- **Standards Compliance:** Uses the term "Verifiable Credentials" consistent with W3C terminology. Specific details on DID method or VC format compliance are not provided in the snippets.
- **Features & Functionality:** Enables users to control data sharing, potentially selectively disclosing attributes. Aims to eliminate traditional passwords. Allows issuers to issue digital credentials and verifiers to check validity without contacting the issuer directly (leveraging blockchain). Mobile app provides a wallet interface.

- **Security & Privacy:** Claims "Privacy, by design". Leverage blockchain for tamper resistance and verification. [4] User control over data sharing is emphasized. App privacy policy indicates collection of identifiers not linked to user identity.
- **Interoperability & Portability:** Interoperability depends on the specific standards implemented by Wipro. Portability relies on the ability to export credentials/keys from the wallet. Claims the technology is "easily portable".
- **Scalability:** Dependent on the underlying blockchain technology chosen by Wipro.
- **Maturity & Ecosystem:** Presented as a Wipro platform offering a live mobile application that has user ratings. Part of Wipro's broader blockchain services. [4]

Strengths & Weaknesses:

- **Strengths:** Backed by a major technology services company (Wipro), utilizes blockchain and VCs, provides a mobile wallet app, focuses on user control.
- **Weaknesses:** Specifics on standards compliance (DID method, VC format) unclear from snippets, likely a commercial/proprietary ecosystem, governance is corporate.

H. Curity Identity Server

The Curity Identity Server is a comprehensive Identity and Access Management (IAM) platform, not exclusively an SSI solution, but one that has integrated features for decentralized identity, specifically Verifiable Credential issuance.[43] It supports OpenID for Verifiable Credential Issuance (OpenID4VCI) and enables presentation via OpenID4VP flows.[44]

Analysis against Criteria:

- **Architecture:** A modular IAM server with distinct services for Authentication, Tokens, and User Management. [44] Designed for deployment flexibility (on-premise, cloud, containers).[45] Integrates VC issuance as a capability within its Token Service profile.[46]
- **Governance:** A commercial product developed and supported by Curity IO AB. Governance is internal to the company.
- **Standards Compliance:** Strong adherence to core IAM standards like OAuth 2.0, OpenID Connect, SAML, SCIM.[47] Explicitly supports OpenID4VCI. Issues VCs in JWT format.[46] Binds issued VCs to user DIDs, supporting various DID methods for the subject. DID management features appear focused on binding VCs rather than full DID lifecycle management.
- **Features & Functionality:** Offers a rich set of traditional IAM features: advanced authentication (MFA, adaptive), SSO, API security (token issuance/validation), user management federation.[43] Provides configuration UI/CLI/API for setting up VC issuance (defining credential types, templates, issuers, endpoints). Offers a demo wallet to illustrate OpenID4VCflows.[44]
- **Security & Privacy:** Leverages robust security from underlying IAM standards (OAuth, OIDC). Privacy characteristics of issued VCs depend on the credential design and usage patterns. Supports standard cryptographic algorithms.
- **Interoperability & Portability:** High interoperability within standard IAM ecosystems due to strong standards support. Support for OpenID4VCI enhances interoperability with compliant SSI wallets.[46]
- **Scalability:** Designed for enterprise scale with clustering capabilities and multi-faceted configuration management for automation.[43]
- **Maturity & Ecosystem:** A mature and established IAM platform.[43] SSI/VC issuance features are more recent additions, integrating decentralized concepts into a traditional IAM framework.

Strengths & Weaknesses:

- **Strengths:** Mature IAM platform foundation, strong standards compliance (OAuth, OIDC, SAML, OpenID4VCI), enables integration of VCs into existing enterprise systems, comprehensive configuration and deployment options.
- **Weaknesses:** Not a pure-play SSI solution (focus remains IAM), DID management capabilities seem limited compared to dedicated SSI platforms, commercial product with associated licensing costs.

V. Comparative Synthesis And Discussion

The individual analysis reveals a diverse and dynamic landscape for SSI solutions. Although unified by the shared objective of enhancing user autonomy, the methodologies employed exhibit considerable divergence. This section synthesizes the findings, comparing the solutions across key dimensions and discussing the implications of recent market shifts.

A.Key Architectural and Technological Differences

A vital distinction among SSI solutions lies in their choice of underlying architecture and Verifiable Data Registry (VDR). Hyperledger Indy and Sovrin utilize a permissioned DLT approach with the RBFT consensus mechanism, ensuring controlled environments under trusted node networks (Stewards). While offering immutability, this requires ongoing consortium governance. In contrast, uPort originally leveraged Ethereum's public blockchain, prioritizing openness but facing higher transaction costs and regulatory concerns.

Ledger-agnostic systems like Veramo support flexible DID methods, including did:web and did:key, alongside ledger-bound methods like did:ethr. Jolocom's protocol similarly adapts to diverse infrastructures. Platforms like Curity and Ping Identity integrate SSI features into IAM frameworks, combining VC issuance or blockchain-enhanced services with enterprise systems. DLT-based systems provide strong immutability but contend with scalability challenges. Non-DLT DID methods simplify deployment but rely on DNS and TLS trust. Credential formats also vary: Indy/Sovrin favor AnonCreds for ZKP privacy, while others like Veramo and Curity adopt W3C VC standards, bridging interoperability gaps.

B.Governance Models: A Spectrum of Approaches

Governance is a cornerstone of SSI, showcasing diverse approaches across solutions. Hyperledger Indy is congruent with the open-source paradigm established by the Linux Foundation, promoting collaborative efforts while remaining reliant on communal assets. The governance framework established by the Sovrin Foundation now faces jeopardy due to fiscal challenges, thereby raising concerns regarding the sustainability of public identity services. Corporate offerings like Curity and Ping Identity provide clear management but risk vendor lock-in. Jolocom operates with an open protocol, leaving network governance undefined. These discrepancies elucidate the inherent conflict between the principles of decentralization and the exigencies of sustainable practices. The obstacles faced by Sovrin underscore the necessity for substantial financial support, active engagement, and viable operational frameworks, thereby demonstrating that governance is equally as crucial as technological advancements for the efficacy of Self-Sovereign Identity ecosystems.

C.Standards Adherence and Interoperability Landscape

Solutions like Veramo explicitly tackle interoperability through modularity and broad standards support. Integrated platforms like Curity leverage OpenID4VCI for interoperability with compliant wallets. However, achieving seamless credential exchange across the entire fragmented ecosystem remains an ongoing effort requiring further standardization of profiles and protocols.

Achieving interoperability is essential for realizing SSI's promise. While many solutions align with W3C standards for DIDs and VCs, practical integration faces challenges. Diverse DID methods require wallets and verifiers to support multiple mechanisms, addressed by tools like DIF Universal Resolver. VC formats vary between JWT and JSON-LD profiles, demanding tailored application handling. Communication protocols like DIDComm are still maturing, whileOpenID4VC/VP leverages OAuth infrastructure but alters interaction models. Platforms such as Veramo emphasize modularity and broad standards compliance, while Curity uses OpenID4VCI for interoperability. Standardizing profiles and protocols remain critical to unify the fragmented SSI ecosystem.

D. Impact of Recent Industry Developments

Recent developments indicate significant shifts within SSI ecosystems. Sovrin's likely shutdown underscores the challenges faced by foundation-governed identity utilities in achieving financial sustainability and robust community participation. Meanwhile, uPort's split into Serto and Veramo highlights the trend toward focused solutions—Serto targets enterprises, while Veramo offers developer frameworks. Ping's acquisition of ShoCard exemplifies growing interest from IAM vendors in SSI,

integrating user-controlled wallets and VCs into enterprise platforms for faster adoption. However, this risks vendor-specific implementations, compromising decentralization. These events suggest industry consolidation, with decentralized models facing sustainability hurdles while commercial integrations gain traction. This period of re-evaluation emphasizes balancing innovation with mass adoption to ensure SSI's growth and relevance.

VI. Conclusion

Self-Sovereign Identity (SSI) holds the potential to fundamentally transform digital engagements by granting individuals dominion over their personal data, thereby enhancing privacy and facilitating the establishment of trust. Notwithstanding progress in essential technologies such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), several challenges remain. These challenges encompass issues of interoperability, user-friendliness, secure key management, sustainability of governance, and alignment with regulatory frameworks. Platforms like Hyperledger Indy, Veramo, and Privado ID push SSI innovation, while IAM vendors like Ping Identity integrate SSI features, accelerating enterprise adoption but raising questions about decentralization. Key trends shaping SSI include improved privacy through Zero-Knowledge Proofs (ZKPs), standardized protocols like DIDComm v2, and hybrid models blending SSI with enterprise systems. Regulatoryinitiatives, such as the EU Digital Identity Wallet, further drive adoption but necessitate compliance. The ecosystem is fragmented, with no single solution dominating. Each shows compromises among decentralization, privacy, usability, and governance. The failure of Sovrin underscores the complexities associated with maintaining models of public utility. The prospective advancement of Self-Sovereign Identity (SSI) is contingent upon the resolution of systemic obstacles through cooperative efforts among developers, enterprises, and policymakers to establish a functional, interoperable, and reliable digital identity framework, thereby influencing the pathway towards accessible and scalable identity solutions.

References

[1] Manu Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, *Decentralized Identifiers (DIDs) v1.0*. 2022. [Online]. Available: https://www.w3.org/TR/2022/REC-did-core-20220719/

[2] R. Błaszczyk, "Exploring Self-Sovereign Identity (SSI) on Blockchain." [Online]. Available: https://billongroup.com/blog/Exploring-Self-Sovereign-Identity-on-Blockchain

[3] L. Dock, "Decentralized Identity: The Ultimate Guide 2025." [Online]. Available: https://www.dock.io/post/decentralized-identity

[4] "Blockchain for Supply Chain platform." wipro. [Online]. Available: https://www.wipro.com/applications/services/blockchain/wipro-decentralized-identity-platform/

[5] F. Schardong and R. Custódio, "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy," *Sensors*, vol. 22, no. 15, p. 5641, Jul. 2022, doi: 10.3390/s22155641.

[6] I. Bolychevsky, "Verifiable Credentials and Decentralised Identifiers: Technical Landscape." GS1, Feb. 03, 2025. [Online]. Available: https://ref.gs1.org/docs/2025/VCs-and-DIDs-tech-landscape

[7] Sovrin Foundation Board of Trustees, "Sovrin Foundation MainNet Ledger Shutdown Likely on or before March 31, 2025." sovrin, Feb. 08, 2025. [Online]. Available: https://sovrin.org/sovrin-foundation-mainnet-ledger-shutdown-likely-on-or-before-march-31-2025/

[8] "uPort has evolved." uport. [Online]. Available: https://uport.me/

[9] Denver, "Ping Identity Acquires Personal Identity Leader ShoCard to Revolutionize Privacy, Streamline Customer Interactions and Put Users in Control of their Identity." pingidentity, Oct. 07, 2020. [Online]. Available: https://press.pingidentity.com/2020-10-07-Ping-Identity-Acquires-Personal-Identity-Leader-ShoCard-to-Revolutionize-Privacy,-Streamline-Customer-Interactions-and-Put-Users-in-Control-of-their-Identity

[10] "Self-Sovereign Identity: The Ultimate Guide 2025." dock labs, Apr. 29, 2025. [Online]. Available: https://www.dock.io/post/self-sovereign-identity

[11] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Comput. Secur.*, vol. 99, p. 102050, Dec. 2020, doi: 10.1016/j.cose.2020.102050.

[12] M. Sporny, D. Longley, D. Chadwick, and I. Herman, *Verifiable Credentials Data Model v2.0*, Mar. 20, 2025. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/

[13] G. Bernstein, D. Burnett, and D. Chadwick, *Verifiable Credentials Overview*. 2025. [Online]. Available: https://www.w3.org/TR/vc-overview/

[14] "Decentralized Identity Foundation (DIF)." Learn & Work Ecosystem Library, Apr. 28, 2025. [Online]. Available: https://learnworkecosystemlibrary.com/organizations/decentralized-identity-foundation/
[15] A. Tobin, "Sovrin: What Goes on the Ledger?" sovrin, Apr. 2017. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/10/What-Goes-On-The-Ledger.pdf
[16] L. Hendrickson, "Your Guide to Self-Sovereign Identity (SSI)." identity, Apr. 23, 2025. [Online]. Available: https://www.identity.com/self-sovereign-identity/
[17] THE SOVRIN FOUNDATION, "Innovation Meets Compliance." Sovrin Foundation, Jan. 2020. [Online]. Available: https://sovrin.org/wp-content/uploads/GDPR-Paper_V1.pdf
[18] E. Krul, H. Paik, S. Ruj, and S. S. Kanhere, "SoK: Trusting Self-Sovereign Identity," *Proc. Priv. Enhancing Technol.*, vol. 2024, no. 3, pp. 297–313, Jul. 2024, doi: 10.56553/popets-2024-0079.
[19] J. Ebersbach, "DID Traits 0.9.0 Editor's Draft." Identity Foundation. Accessed: May 03, 2025. [Online]. Available: https://identity.foundation/did-traits/
[20] P. Mittal, "Introduction to Privado ID." privado. [Online]. Available: https://docs.privado.id/docs/introduction
[21] L. Marques Da Fonseca, H. Barzegar, and C. Pahl, "Decentralized Identification and Information Exchange in Distributed, Blockchain-Based Internet Architectures: A Technology Review:," in *Proceedings of the 19th International Conference on Web Information Systems and Technologies*, Rome, Italy: SCITEPRESS - Science and Technology Publications, 2023, pp. 535–544. doi: 10.5220/0012254900003584.
[22] D. Schumm, K. O. E. Müller, and B. Stiller, "Are We There Yet? A Study of Decentralized Identity Applications," Mar. 20, 2025, *arXiv*: arXiv:2503.15964. doi: 10.48550/arXiv.2503.15964.
[23] "Hyperledger Indy." Linux Foundation. [Online]. Available: https://www.lfdecentralizedtrust.org/projects/hyperledger-indy
[24] "Indy, Verifiable Credentials and Decentralized Identity Basics." aca-py. [Online]. Available: https://aca-py.org/latest/gettingStarted/IndyBasics/
[25] "Indy Walkthrough." github. [Online]. Available: https://github.com/hyperledger-indy/indy-sdk/blob/main/docs/getting-started/indy-walkthrough.md
[26] "Hyperledger Architecture, Volume 1." [Online]. Available: https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/Hyperledger/Offers/Hyperledger_Arch_WG_Paper_1_Consensus.pdf
[27] "Sovrin Governance Framework V2 Master Document." Sovrin Foundation, Oct. 31, 2018. [Online]. Available: https://www.gleif.org/media/pages/lei-solutions/regulatory-use-of-the-lei/consultation-responses/b4fa9a45c0-1747294888/sovrin-governance-framework-v2-master-document.pdf
[28] "'The Community Moved On': Sovrin Announces MainNet's 'Likely Shutdown.'" idtechwire, Oct. 21, 2024. Accessed: Mar. 31, 2025. [Online]. Available: https://idtechwire.com/the-community-moved-on-sovrin-announces-mainnets-likely-shutdown/
[29] R. Verhelst, "Implementing SSI: Comparing Uport, Sovrin and IRMA," Implementing SSI: Comparing Uport, Sovrin and IRMA. [Online]. Available: https://info.suresync.nl/blog/different-approaches-ssi
[30] "uPort: Veramo and Serto." Decentralized Identity. Accessed: May 03, 2025. [Online]. Available: https://decentralized-id.com/web-3/ethereum/uport-veramo-serto/
[31] mirceanis and Revert "chore(ci): fix jest call on GH workflow," "decentralized-identity / veramo." Accessed: May 05, 2025. [Online]. Available: https://github.com/decentralized-identity/veramo
[32] "Veramo Basics." Accessed: May 03, 2025. [Online]. Available: https://docs.tuum.tech/identify/basics/veramo
[33] "Why Veramo?" veramo. Accessed: May 04, 2025. [Online]. Available: https://veramo.io/docs/basics/introduction/
[34] "DID Methods." veramo. [Online]. Available: https://veramo.io/docs/veramo_agent/did_methods/
[35] "Veramo SDK." cheqd. Accessed: May 04, 2025. [Online]. Available: https://docs.cheqd.io/product/sdk/veramo
[36] "The Jolocom Protocol - Own Your Digital Self." jolocom. Accessed: May 04, 2025. [Online]. Available: https://jolocom-lib.readthedocs.io/en/latest/
[37] jolocom, "jolocom-sdk: A tool kit for integration with SSI." github. Accessed: May 04, 2025. [Online]. Available: https://github.com/jolocom/jolocom-sdk
[38] "Fast and secure identity verification." Sora ID. Accessed: May 04, 2025. [Online]. Available: https://www.soraid.com/solutions/product/

[39] "Security and Standards." Accessed: May 05, 2025. [Online]. Available: https://www.soraid.com/product/security-and-standards/
[40] M. Takemiya and B. Vanieiev, "Sora Identity: Secure, Digital Identity on the Blockchain," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Tokyo, Japan: IEEE, Jul. 2018, pp. 582–587. doi: 10.1109/COMPSAC.2018.10299.
[41] S. Cucko and M. Turkanovic, "Decentralized and Self-Sovereign Identity: Systematic Mapping Study," *IEEE Access*, vol. 9, pp. 139009–139027, 2021, doi: 10.1109/ACCESS.2021.3117588.
[42] K. Miller, "Ping Identity's 'Project COVID Freedom' Aims to Make Vaccination Verification Simple," *Busniess Wire*, Feb. 17, 2021. Accessed: May 05, 2025. [Online]. Available: https://www.businesswire.com/news/home/20210217005166/en/Ping-Identitys-Project-COVID-Freedom-Aims-to-Make-Vaccination-Verification-Simple
[43] "Curity Identity Server." curity. Accessed: May 05, 2025. [Online]. Available: https://curity.io/product/
[44] "Run Verifiable Credentials Demo Wallet." Accessed: May 05, 2025. [Online]. Available: https://curity.io/resources/learn/use-verifiable-credentials/
[45] "Curity Identity Server Datasheet." Accessed: May 05, 2025. [Online]. Available: https://assets.ctfassets.net/tldhjvq55hjd/3KVQhs3K5rC7U7FeZQpMzy/f257e2cae3c92c74f0b0c3068887c58e/Curity-DataSheet18-online.pdf
[46] "Issue a Verifiable Credential." Accessed: May 05, 2025. [Online]. Available: https://curity.io/resources/learn/configure-verifiable-credential-issuance/
[47] "Curity Identity Server | SSO Provider." ssojet. Accessed: May 05, 2025. [Online]. Available: https://ssojet.com/protocol/curity-identity-server/