frontiers | Frontiers in Blockchain

TYPE Review
PUBLISHED 30 August 2024
DOI 10.3389/fbloc.2024.1443362

OPEN ACCESS

EDITED BY
Isaac Agudo,
University of Malaga, Spain

REVIEWED BY
Qin Wang,
Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia
Adrian McCullagh,
Griffith University, Australia

*CORRESPONDENCE
Roberto A. Pava-Díaz,
rapavad@udistrital.edu.co

RECEIVED 03 June 2024
ACCEPTED 15 August 2024
PUBLISHED 30 August 2024

CITATION
Pava-Díaz RA, Gil-Ruiz J and López-Sarmiento DA (2024) Self-sovereign identity on the blockchain: contextual analysis and quantification of SSI principles implementation.
Front. Blockchain 7:1443362.
doi: 10.3389/fbloc.2024.1443362

Self-sovereign identity on the blockchain: contextual analysis and quantification of SSI principles implementation

Roberto A. Pava-Díaz[1]*, Jesús Gil-Ruiz[2] and Danilo A. López-Sarmiento[1]

[1]Research and Development Laboratory in Electronics and Networks, Faculty of Engineering, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, [2]Faculty of engineering, Fundación Universitaria Internacional de La Rioja, Logroño, Spain

Self-sovereign identity (SSI) embodies the fundamental human right to own and control a digital identity that grants access to public, social, and financial services. The absence of a dedicated digital identity layer in the development of the Internet has rendered SSI a significant challenge in contemporary society. Blockchain technology emerges as a promising solution by enabling the creation of decentralized and automatically verifiable identities. This study contextualizes SSI and analyzes how blockchain technology facilitates the autonomous management of digital identities. It explores nine prominent frameworks in this field—Sovrin, uPort, Jolocom, ShoCard, Litentry, Civic, KILT, Idena, and ION—highlighting their features, functionalities, and compliance with digital identity principles. The research concludes by identifying the challenges and opportunities in implementing these systems for digital identity management, thus contributing to the advancement of this emerging field.

KEYWORDS

blockchain technology, decentralized identity management, self-sovereign identity, self-sovereign identity frameworks, digital identity

1 Introduction

Digital identity is the representation of an entity in the digital realm, whether an individual, organization, software, or IoT device. For individuals, a digital identity may encompass personally identifiable information (PII), which consists of specific data elements that uniquely identify a person. These attributes can include, but are not limited to, a full legal name, date of birth, telephone number, physical address, and email address. When combined, these identifiers form a comprehensive digital representation of an individual's identity within identity information systems. This representation enables authentication and authorization processes, allowing entities to access services and conduct digital transactions (Naik and Jenkins, 2021a). Digital identity management stands out as one of the most significant challenges facing today's society (Stokkink et al., 2021). The Internet was developed without a dedicated digital identity layer, leaving this responsibility to individual service providers.

Table 1 provides an overview of digital identity, focusing on four key characteristics: (1) the fundamental human right to possess and provide verifiable evidence of a digital identity that facilitates access to public, social, and financial services; (2) the necessity for a universal and interoperable digital identity without geographical limitations, allowing secure

TABLE 1 Digital identity characteristics: exploring the challenges, features, and properties of digital identity.

Human right	Verifiable evidence of identity Access to essential services Social inclusion and participation Control over personal information
Property	Self-governed: autonomously controlled by the individual Privacy-preserving: ensures data confidentiality and user anonymity Portable: transferable across different systems Persistent: maintains longevity and consistency over time Reliable: provides verifiable and trustworthy information Universal: accessible and applicable across diverse contexts
Technological factor	Cybersecurity resilience: mitigating attack vectors and vulnerabilities Cryptographic integrity: implementing robust encryption protocols Decentralized architecture: ensuring distributed control and data storage Verifiability mechanisms: enabling tamper-evident credential validation Interoperability standards: facilitating seamless cross-system functionality
Benefit	Enhanced service accessibility: facilitating equitable access to public and private sector services Strengthened national security: improving identity verification and fraud prevention mechanisms Empowered privacy management: enabling granular control over personal data disclosure Cybersecurity risk mitigation: reducing vulnerability to phishing attacks and identity theft

transactions in trusted environments, ensuring persistence even in the face of political or economic disasters, and facilitating the assignment of permissions or contexts for its use; (3) current technological advancements enable the creation of a decentralized identity that is automatically verifiable under interoperability standards, mitigating the risks of cyber-attacks; and (4) social wellbeing is enhanced by strengthening the management of public services, such as public health, medicine delivery, census, or education. This contributes to more effective government controls against terrorism and greater security in the storage, control, and use of personal data (The ID 2020 Alliance, 2019).

The current state of digital identity is highly fragmented and relies on verification by trusted third parties, limiting the storage of personal information by users. There is also low interoperability between systems, restricting identity migration and posing risks of fraud and impersonation (Li et al., 2019). In addition, there are challenges in correlating digital identities with physical identities. Physical identity is cumulative, self-managed, and multifaceted, allowing a person to have multiple associated digital identities, each with a unique identifier but linked to the main identifier of their identity (Kiva, 2020). These unique identifiers must be decentralized and linked to verifiable credentials containing claims about an entity, which is more fully argued and justified below in this paper.

Moreover, distributed ledger technology (DLT) provides the underlying technological support for deploying a decentralized and self-governed digital identity. This enables the creation of an identity service infrastructure that supports the generation of decentralized unique identifiers (DIDs), the registration and validation of cryptographically verifiable credentials (VCs), the assignment and revocation of permissions and consent for using personal data, and the implementation of a computable law. This law facilitates entities in monetizing their identity and controlling access to their personal information (Kondova and Erbguth, 2020).

Ultimately, the justification for creating a decentralized digital identity lies in the drawbacks of the centralized scheme for identity management, which relies on trusted intermediaries and poses risks associated with centralized repositories and a single point of access. Centralized information control can increase cybersecurity vulnerabilities, as evidenced by the 2007 cyberattack on Estonia, which spurred the country's rapid adoption of blockchain technology to safeguard citizen privacy (Haataja, 2017; Priisalu and Ottis, 2017).

1.1 Self-sovereign identity

Self-sovereign identity (SSI) is an identity management model where individuals maintain control and custody of their identification attributes. They can either generate verifiable credentials or obtain them from an issuer to present them to a verifier. The trust relationship between the issuer and verifier is established through registered cryptographic proofs. Figure 1 illustrates the challenges and context necessary for self-sovereign digital identity management. The issue of managing digital identity is emphasized as it is considered a fundamental and universal human right that should enable the inclusion of individuals without restricting their access to a global market of goods and services in an interconnected world (Wang and De Filippi, 2020; Sicilia and Visvizi, 2019).

The rationale behind establishing a decentralized digital identity arises from several key factors. The centralized approach to identity management relies on trusted intermediaries, which facilitates control actions due to a single point of system access and centralized storage of information. However, this concentration of control presents significant cybersecurity risks, as demonstrated by the 2007 cyber incident in Estonia (Haataja, 2017). This event underscored the vulnerability of centralized systems and prompted Estonia to embrace blockchain technology to safeguard citizen privacy (Priisalu and Ottis, 2017). Additionally, identity theft poses a grave threat to personal, economic, and moral stability. Victims of physical or digital identity theft endure considerable hardship, often requiring substantial time and financial resources to recover (Li et al., 2019). Therefore, transitioning to a decentralized digital identity framework is imperative to mitigate these risks and enhance individual sovereignty over personal data.

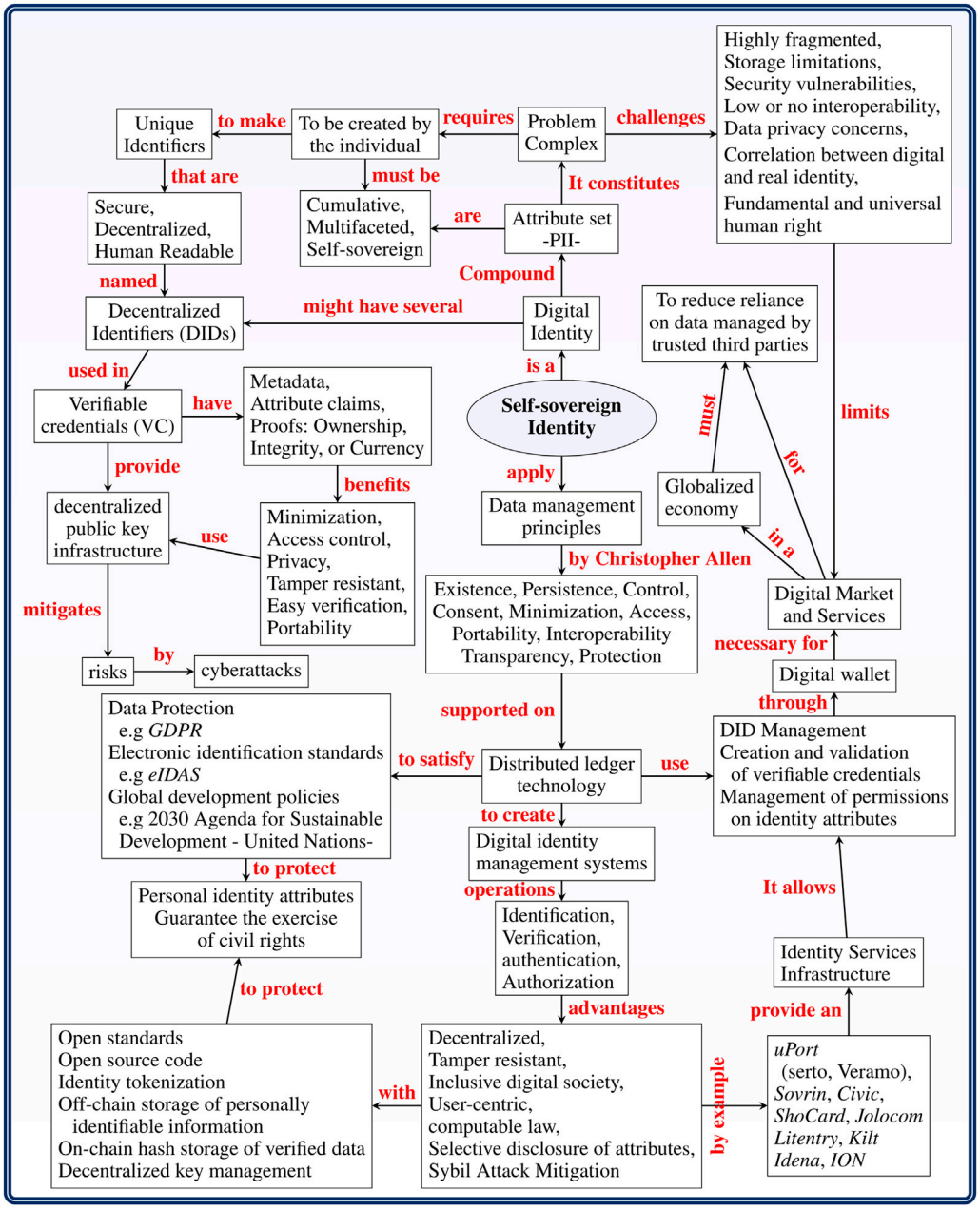


FIGURE 1
Overview of SSI management: challenges and deployment using DLT.

Furthermore, a paradigm shift in information management, driven by DLT, is on the horizon. This transition from an Internet of information to an Internet of value will transform technological management processes within organizations. Consequently, practices for developing corporate technological infrastructures must adapt, including the automation of legal procedures for value transfer. This shift will energize the system of registration and exchange of goods and services under a paradigm of ubiquitous computing with democratic access to information. It also implies a subsequent cultural change that will empower people to control information and institutions, becoming a key factor in transparency and efficiency (Nawari and Ravindran, 2019; Peck, 2017; Heng, 2017).

Finally, while there has been a surge of interest in SSI, the field still lacks a comprehensive evaluation of existing frameworks against a unified set of principles. This study seeks to address this gap by systematically examining popular SSI frameworks through the lens of Allen's SSI principles and describing the architecture designed in each of them. Previous research has explored the landscape of SSI frameworks. Haddouti et al. compared uPort, Sovrin, and ShoCard by utilizing Cameron's seven laws of digital identity. These laws serve as criteria to assess the effectiveness and compliance of each system with essential digital identity features. The specific laws include user control and consent, minimal disclosure for constrained use, justifiable parties, directed identity, design for a

pluralism of operators and technology, human integration, and consistent experience across contexts (Haddouti and Kettani, 2019). Satybaldy et al. proposed an evaluation framework comparing Sovrin, uPort, ShoCard, Civic, and Blockstack by utilizing criteria derived from established models, including Cameron's laws of identity. The framework emphasizes key aspects such as security, data integrity, privacy, and usability, which are essential for assessing the effectiveness of SSI systems. The comparison also highlights the varying levels of decentralization among the systems and their incorporation of blockchain technology to achieve self-sovereignty. It suggests that while no system has fully realized true self-sovereign identity, the discussed systems represent significant attempts to address core challenges in identity management (Satybaldy et al., 2020). Kaneriya et al. compared Sovrin, uPort, everID, lifeID, and Sora based on several key aspects. Their study summarizes important features and functionalities of various blockchain-based SSI implementations, allowing for a comparative analysis. The main points of comparison include open-source status, blockchain type, blockchain implementation, future enhancements, and reputation management. The evaluation provides a structured way to assess the strengths and weaknesses of each SSI system, facilitating a clearer understanding of their capabilities and areas for improvement (Kaneriya and Patel, 2020). Alizadeh et al. analyzed uPort and ShoCard by focusing on several key performance metrics. Specifically, they measured throughput, execution time, and average standard deviation across various models, including serverless, server-based, cloud-based, SSI, blockchain, and DHT-based systems. This structured approach enables a comprehensive evaluation of system performance across various conditions and configurations, providing clearer insights into their strengths and weaknesses within the decentralized identity management landscape (Alizadeh et al., 2022). These papers present diverse approaches to evaluating and comparing SSI systems. The four evaluation frameworks focus on distinct aspects, including performance metrics, key features, Cameron's laws of digital identity, and combined criteria from Allen and Cameron. Each evaluation framework has a unique approach, but all share the goal of providing a structured and comprehensive comparison of SSI systems, facilitating an understanding of their strengths and weaknesses in various contexts and applications. These evaluation frameworks provide systematic tools for comparing and contrasting SSI systems, guiding future innovations in digital identity management.

2 Methodology

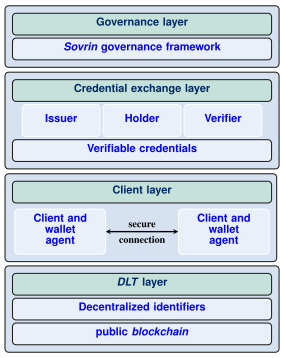
1. Identification of frameworks: a bibliometric study on scientific production related to SSI by Pava-Diaz et al. (2023) provided valuable insights into the main authors and publications in the field (Pava-Diaz et al., 2022). This study allowed us to identify the most relevant SSI frameworks for this article, namely, Sovrin, uPort, Jolocom, ShoCard, Litentry, Civic, KILT, Idena, and ION.
2. Definition of evaluation criteria: typically, the design of an SSI framework incorporates the ten principles of SSI proposed by Allen (2016). These SSI principles are categorized into three groups:
   a. Security (Dib and Toumi, 2020):
      (1) Protection: prioritizing censorship-resistant systems that promote individual rights and freedom in decentralized environments.
      (2) Persistence: ensuring that identities endure for as long as needed by the owner.
      (3) Minimization: allowing users to selectively disclose their identity attributes.
   b. Controllability (Ferdous et al., 2019):
      (1) Existence: prioritizing the existence of a person over the digital representation of their identities, ensuring independence.
      (2) Control: affirming that users have sole control over their information and full authority over their identities.
      (3) Consent: granting users the power to allow or deny access to their data.
   c. Portability (Ferdous et al., 2019):
      (1) Access: ensuring entities always have direct and unrestricted access to their identity attributes and knowledge of any queries made about their identities.
      (2) Transparency: advocating for open-source algorithms and systems for digital identity management that are free from licensing restrictions. This will enable public validation of these systems by software developers.
      (3) Portability: allowing users to move or transport their identity without legal, political, or technological restrictions, ensuring control in unforeseen events or disasters.
      (4) Interoperability: enabling users to use their digital identities across multiple scenarios or systems globally without losing control.
3. Functionality and features: this stage involves a comprehensive examination of the main features of each framework, accompanied by an overview of its underlying architecture.
4. Application of the criteria: the analysis of each framework's compliance with the defined evaluation criteria is conducted and complemented by a discussion of the results.

3 Results

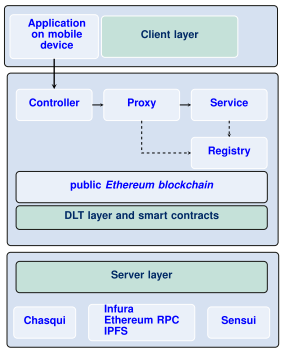
3.1 Frameworks for self-sovereign identity

This section provides an analysis of the selected blockchain frameworks for SSI management, namely, Sovrin, uPort, Jolocom, ShoCard, Litentry, Civic, KILT, Idena, and ION. Each framework is examined in terms of its adherence to the SSI principles, its main features, and its underlying architecture.

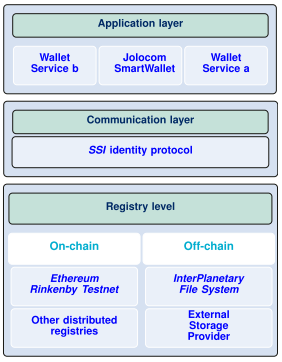
An SSI framework is a digital identity meta-system designed to deploy a decentralized, user-centric digital identity, providing a unified operational interface that facilitates the integration of digital identities (Windley, 2021). The frameworks identified in stage 1 of the methodology are described below. Figure 2 consolidates the architecture designed for each of these frameworks.



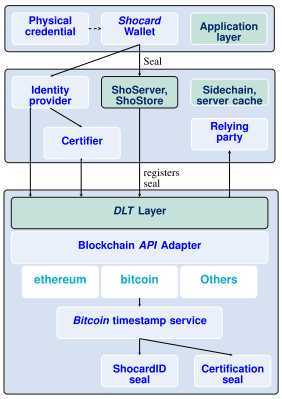
Sovrin: adapted from Naik and Jenkins (2021b)



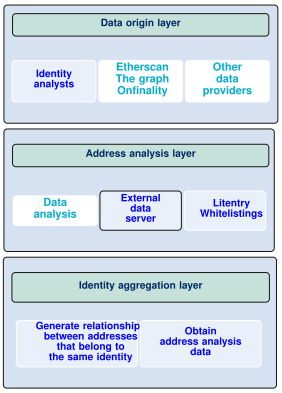
uPort: adapted from Kondova and Erbguth (2020); Naik and Jenkins (2020b)



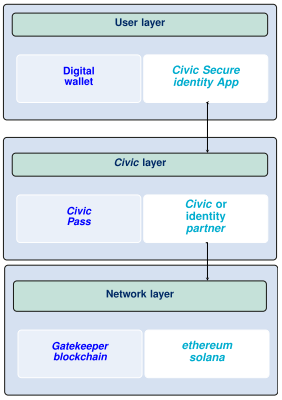
Jolocom: adapted from Jolocom.io (2020)



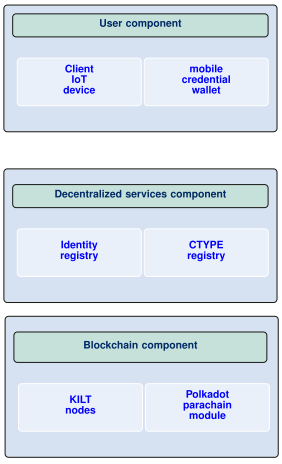
Shocard: adapted from Haddouti and Kettani (2019); ShoCard Inc. (2017)



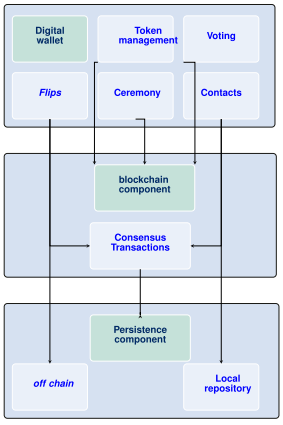
Litentry: adapted from: Litentry (2022); Litentry Technologies (2021)



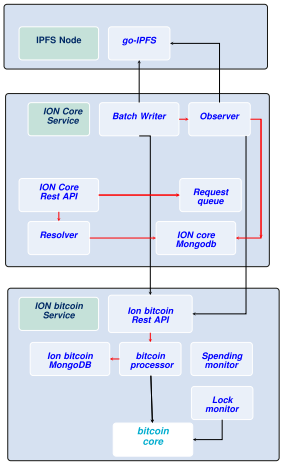
Civic: adapted from Civic Developer Hub (2020)



Kilt: adapted from: BOTLabs GmbH (2020)



Idena: adapted from: Idena network (2018, 2022)



ION: adapted from: Identity Foundation (2022a)

FIGURE 2
Layered architecture diagram of key frameworks for implementing self-sovereign digital identity.

3.1.1 Sovrin

Sovrin deploys an SSI service on a federated blockchain, implementing a unique type of node called stewards. These stewards are trusted organizations responsible for maintaining the network and validating transactions (Sovrin Foundation, 2019). The blockchain is overseen by the Sovrin Foundation, which plays a crucial role in applying the necessary governance framework for decision-making in network operations and guiding its evolution. The original source code was generously contributed by the Sovrin Foundation to the Linux Foundation, resulting in the

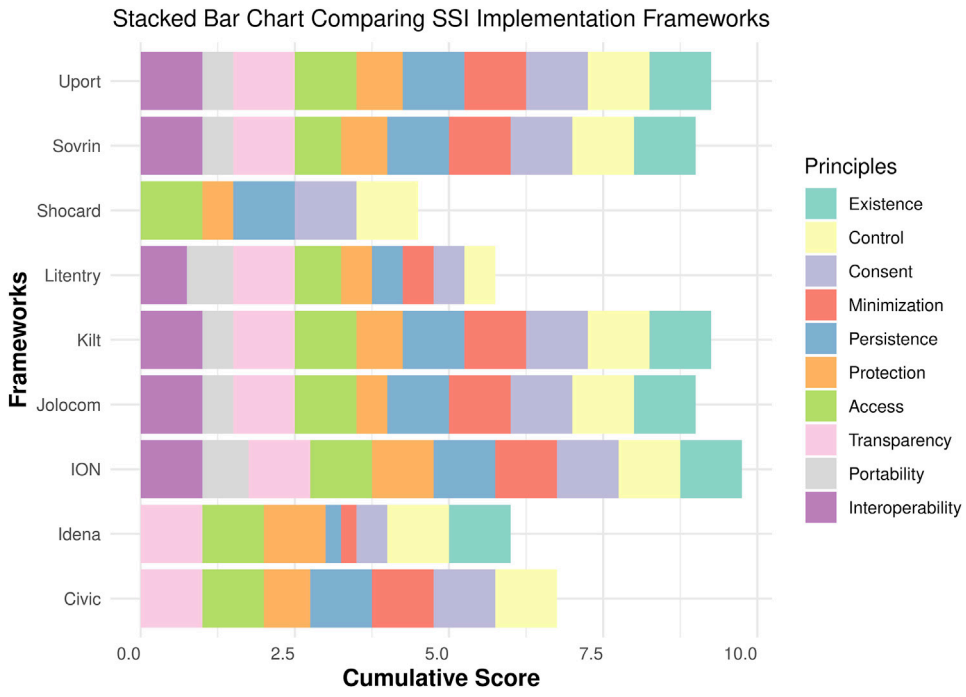


FIGURE 3
Comparative analysis of SSI principle implementation across decentralized identity systems.

creation of the open-source project Hyperledger Indy (Hyperledger Foundation, 2022).

Sovrin's architecture is centered on privacy, providing users with direct and granular control over their personal identity attributes. It minimizes the amount of data shared without the need for a trusted third party and establishes a schema for digital reputation based on the statements comprising verifiable credentials. The Sovrin network is structured into four layers (see Figure 3):

1. Governance layer: this layer is responsible for ensuring the correct application of the governance framework in each jurisdiction where the network operates. This layer also coordinates the network actors.
2. Credential exchange layer: this layer ensures the flow of information through the issuance and presentation of verifiable credentials.
3. Client layer: this layer enables the creation of DIDs to represent an entity in the network and deploys agents that manage peer-to-peer communication between two DIDs. This layer handles digital identity management, acceptance or generation of verifiable credentials, and various identity operations.
4. DLT layer: this layer configures the Hyperledger Indy-type blockchain with steward nodes approved by the governance framework. The DLT notarizes DIDs and verifiable credentials, managing the assignment or revocation of permissions. Additionally, this layer is responsible for achieving consensus using the Byzantine fault tolerance algorithm—RBFT—known as Plenum Indy (Naik and Jenkins, 2021a).

3.1.2 uPort

uPort is an SSI system built on the Ethereum blockchain, enabling the creation, sharing, and management of a decentralized and cryptographically verifiable digital identity. uPort has evolved into two distinct projects: Serto, targeting the deployment of SSI in the business sector, and Veramo, conceived as a JavaScript framework for developing applications requiring DIDs and verifiable credentials. uPort validates verifiable credentials, allowing individuals to possess and control a digital identity. It facilitates authentication and authorization in digital services using a verifiable credential, replacing traditional access credentials like usernames and passwords. The uPort architecture is structured into three layers (see Figure 3):

1. Client layer: this layer comprises a digital wallet storing cryptographic keys and generating a DID known as uPortID. The DID is linked to the private key, facilitating key updates in case of wallet access loss (Haddouti and Kettani, 2019).
2. DLT layer and smart contracts: this layer is based on four smart contracts, namely, a controller responsible for user authentication and digital identity recovery, a proxy contract managing communication between smart contracts, a registration contract linking uPortID to personal identification attributes stored externally, and a contract for interacting with a specific application.
3. Server layer: this layer utilizes four servers, namely, a messaging server (chasqui) for decentralized application communication, a service (sensui) providing tokens to cover gas costs for Ethereum transactions, and two communication interface services—one between uPort and Ethereum services

(Infura Ethereum RPC) and another for decentralized file storage (Infura IPFS).

3.1.3 Jolocom

It operates as a protocol that empowers various entities, including individuals, organizations, IoT devices, and autonomous agents, to establish a primary identity and derive multiple sub-identities. Each identity is associated with a decentralized identifier, and verification is ensured through the use of verifiable credentials encoded as JSON web tokens (JWTs). Jolocom utilizes the Ethereum blockchain to notarize the hash of the generated assertions (Jolocom.io (2020)). The architecture of Jolocom is divided into three layers (see Figure 3):

1. Application layer: this layer is responsible for managing digital identity, generating cryptographic keys, and creating the DID. The associated JSON document is securely stored on an IPFS server.
2. Communication layer: this layer offers an open-source library known as "jolocom-lib," compliant with W3C standards. It facilitates the management of decentralized identifiers and verifiable credentials, supporting all functionalities of the protocol.
3. Registration layer: the DID is registered on the Ethereum blockchain (on-chain), while the verifiable credential schemes, alongside the DID documents, are stored in a decentralized file system (off-chain).

3.1.4 ShoCard

ShoCard is a decentralized identity management system that enables the creation of a digital identity using a trusted physical credential and biometric data captured from a smartphone. It is designed with a permissioned architecture integrated into the upper layer of a blockchain (Haddouti and Kettani, 2019). ShoCard utilizes the Bitcoin blockchain for generating timestamps for identity validation while also allowing integration with other DLTs. Information privacy is ensured through zero-knowledge proof (ZKP) for user registration and validation (Dunphy and Petitcolas, 2018). ShoCard's architecture is structured into three layers (see Figure 3):

1. Application layer: this layer provides a wallet that generates and preserves cryptographic keys, creating the user's DID from a physical credential issued by an official entity. It also manages a list of invited third parties with permission to access personal information (Liu et al., 2020) and stores personally identifiable information.
2. Service layer: this layer deploys a centralized service enabling entities to connect with third parties through a secure communication channel between applications. It associates the ShoCardID with each required service and includes services such as ShoServer, ShoStore, Sidechain, and Server Cache. The latter maintains a copy of the blockchain to enhance network scalability.
3. DLT layer: the system is ledger-agnostic, abstracting the connection with the blockchain through an interface provided by an adapter to each DLT. The hash of verified data is stored in the blockchain ShoCard Inc. (2017) (Identity, 2020).

3.1.5 Litentry

It is an innovative system that assembles a comprehensive digital identity by aggregating DIDs held by an entity across various networks and blockchains. In its current state of development, Litentry has successfully deployed two parachains: the primary Litentry chain on Polkadot (Web3 Foundation (2017)) and Litmus, a fully operational test network, on Kusama (Web3 Foundation (2022)). Kusama serves as a canary network for Polkadot, allowing for real-world testing and optimization of the Litentry protocol. It provides reliable and quantified data through a sophisticated, configurable weighting algorithm, implemented within a robust three-layer architecture, as illustrated in Figure 3 (Litentry, 2022).

1. Data source layer: this foundational layer establishes connections to external data providers, including blockchain explorers (Etherscan, 2022), decentralized protocols for indexing and querying blockchain data (the Graph Foundation (2022)), and information from blockchain-as-a-service (BaaS) platforms (OnFinality, 2022) (Litentry Technologies, 2021). This diverse range of data sources ensures a comprehensive and accurate representation of an entity's digital footprint.
2. Address analysis layer: this intermediate layer comprises an external server dedicated to processing the data obtained from the data source layer. While this system is still under development, it is projected to include a service called Litentry Whitelisting (Litentry Technologies, 2021). This service will play a crucial role in analyzing and validating the addresses associated with each digital identity.
3. Identity aggregation layer: this top-level layer performs the critical function of relating identifiers that belong to the same subject and utilizes the results from the address analysis to compute the identity weighting algorithm. To ensure privacy and security, this layer encrypts all data and protects the calculation process using a trusted execution environment (TEE) implemented with Intel Software Guard Extensions (SGX) (Litentry Technologies, 2021).

3.1.6 Civic

Civic's system utilizes the Ethereum blockchain and incorporates biometrics for robust control over digital identity. It securely encrypts and stores personal identity attributes on the user's smartphone. Additionally, Civic offers an ERC-20 token to facilitate transaction fee payments, incentivize nodes validating identities, and enable the monetization of personal information usage (Kuperberg, 2020). Civic's applications span various domains, including access to financial services, age verification for authorization, and customer identification processes (Know Your Customer — KYC). Civic's architecture comprises three distinct layers (see Figure 3):

1. User layer: users perform a proof of existence through the wallet, utilizing an official identity document like a passport and providing a video of themselves. Upon successful verification, Civic generates a DID called Civic Pass. The data verification process in Civic relies on trusted validators, such as governments or financial institutions, capable of verifying the user's pre-existing identity. The wallet also

records biometric data, such as fingerprints, facilitating application login, and allows users to share their information using a QR code.
2. Civic layer: this layer validates user information or requirements, sends claims to the network layer, and encrypts and transmits identification attributes to the user layer.
3. Network layer: this layer registers verified assertions from the Civic layer in the DLT and facilitates integration with other blockchains, such as Solana and Ethereum.

3.1.7 KILT

KILT is an innovative blockchain protocol designed for managing (creating, claiming, issuing, presenting, and revoking) verifiable credentials. It implements a top–down trust structure where high-reputation entities, such as governments or corporations, attest to other subjects. The protocol aligns with the W3C's data model for verifiable credentials, defining three primary roles for entities: (A) claimer or holder: the entity that holds ownership of a claim requested from a trusted issuer; (B) attester: the entity that provides trust on claims received by subjects and issues verifiable credentials for these claims. Each attester or issuer publishes a set of claim types they can validate, earning rewards in the native token (Coinmarketcap, 2024) and building or maintaining their reputation; and (C) verifier: the entity that facilitates the exchange of verifiable credentials between different subjects, determines which issuers are trustworthy, and validates the holder's identity through a cryptographic challenge. KILT empowers holders to generate self-attestations, which are subsequently validated by an issuer and converted into verifiable credentials. The protocol classifies claims into types, known as Claim types (CTYPEs), with schemas described in JSON documents (BOTLabs GmbH, 2020; BOTLabs GmbH, 2022). The KILT framework architecture, illustrated in Figure 3, comprises several components that communicate via a JavaScript SDK. This SDK encapsulates the necessary cryptographic libraries and implements functions for claim storage, CTYPE registration on the blockchain, and management of identities, claim types, claims, and validations. The key components are

1. User component: this includes a wallet that enables subjects to create their digital identity and incorporate self-attestations. These self-attestations are legitimized through credentials issued by trusted sources. The protocol facilitates the creation and registration of DIDs on the blockchain, with the corresponding DID document stored in an external repository. The DID-KILT method and its integration with the universal resolver are currently under development. Users can create new CTYPEs based on a JSON meta-schema defined in the SDK and register the hash on the DLT. Users can request verification (claiming) of a self-attestation from an issuer. The DID-KILT method continues to develop and integrate with the universal resolver.
2. Decentralized service component: the native token is utilized for governance, enabling payment of fees to issuers, registration of new CTYPEs, writing to the DLT, and credential revocation. This component is invoked by users for claim type management.
3. Blockchain component: this component is developed using the Parity Substrate framework (Parity Technologies, 2020) and the Polkadot blockchain (Web3 Foundation, 2017); this component is based on the modular WebAssembly architecture (W3C Community Group, 2022). Blockchain component, implemented in RUST, offers efficient memory usage and rapid compilation processes (BOTLabs GmbH, 2020). The DLT implements modules for CTYPE creation and the registration, revocation, and querying of attestations.

3.1.8 Idena

Idena presents an innovative blockchain designed for decentralized identity management and Sybil resistance through a consensus algorithm known as 'proof of person.' Its innovative integration of human-centric verification, blockchain technology, and incentive structures provides a promising model for establishing robust and trustworthy digital identity systems on the decentralized web. This algorithm is based on the resolution of a non-Turing test during a synchronous event for all users. The Idena identity, or cryptoidentity, is global, digitally verifiable, access-unrestricted, decentralized without third-party dependency, Sybil-resistant, uncensorable, and anonymous (Idena network (2018), Idena network (2022)). Figure 3 illustrates a high-level architecture diagram of the Idena system.

1. User component: the digital wallet serves as the holder's gateway to the Idena blockchain. The process begins with the generation of a cryptographic key pair, where the public key becomes the cryptoidentity identifier, and the private key must be securely stored as no recovery mechanism exists. A new account requires activation through an invitation from an active network user and validation during three verification ceremonies. The cryptoidentity progresses through the following states: (1) not invited: initial state upon key generation, (2) invited: upon receiving an invitation from an active member, (3) candidate: after passing the first ceremony with at least 75% effectiveness, (4) verified: upon successful completion of three consecutive ceremonies with a minimum 92% success rate, and (5) human: the final identity state. From the candidate level onward, users must contribute three non-Turing proofs, called 'flips.' Each flip comprises four images logically associated with a story based on two keywords, excluding text or numbers. It is presented in two sequences—correct and incorrect—for evaluation in identity verification ceremonies.
2. Blockchain component: the consensus algorithm is founded on synchronous identity validation ceremonies. These are scheduled with a periodicity inverse to the number of users N, with a minimum frequency of 3 days and a maximum of 28. Ceremonies occur at 13:30 UTC on the selected day and are divided into two parts: (1) a short section with six flips to be solved in under 2 minutes and (2) a longer section containing 12 to 20 flips, depending on the number of online users, with a maximum time of 30 min. Failure in a ceremony, either due to absence or more than 25% incorrect answers, modifies the user's state as follows: (a) dead: the identity is removed from the network if it was in the candidate, newbie, or zombie state, (b) suspended: if one ceremony is failed while in the verified

state, and (c) zombie: if two consecutive ceremonies are failed while in the verified or human state. A key constraint of the algorithm is the requirement for all users to be online at a specific, periodic time to prevent the creation of multiple identities. Participation in ceremonies is incentivized by the opportunity to receive invitations as the protocol distributes rewards to users whose invitees successfully complete the ceremony.

3. Storage component: the blockchain maintains the hash of created identifiers, sent invitations, and validation ceremony results. Images included in the flips are stored on a decentralized service such as IPFS.

3.1.9 ION

Identity overlay network—ION is a public, DID-based identity network that implements the Sidetree protocol (Identity Foundation, 2021a) on the Bitcoin blockchain. It deploys a large-scale, global, immutable, decentralized public key infrastructure (DPKI) without a central authority, resistant to censorship and manipulation. ION can manage thousands of DIDs per second (exceeding 10,000 transactions in ION) by encapsulating them into a single Bitcoin transaction (Identity Foundation, 2022a; Identity Foundation, 2021b). ION's architecture does not require a consensus mechanism additional to Bitcoin's, and the Sidetree protocol prevents conflicts in the DPKI by defining a strict set of deterministic rules for state changes in a DID and restricting the transfer of identifier ownership between users. ION represents a significant advancement in decentralized identity management, leveraging the security and immutability of the Bitcoin blockchain while addressing scalability concerns. The architecture, illustrated in Figure 3, comprises the following components:

1. IPFS node: this is a content addressed storage (CAS) service with cryptographic integrity that preserves the transactions encapsulated by the batch-writer.
2. *Core services*:
   - Users initiate transaction requests through a digital wallet via the ION Core REST API. These requests may include state changes to the DID.
   - Requests are queued until a predefined batch size is reached and then processed by the batch-writer service.
   - After encapsulation into a single hash, transactions are sent to the blockchain for processing via the ION Bitcoin REST API.
   - To prevent malicious users from filling the batch size with a single ION transaction, a 'proof of fee' mechanism is implemented. This assigns the cost of each operation to one-thousandth of a Bitcoin transaction value.
   - Node synchronization utilizes the observer service, which queries a local MongoDB registry to identify encapsulated or embedded transaction batches for processing.
3. Bitcoin-associated services:
   - This service connects with the Bitcoin blockchain (Bitcoin Core).
   - The Bitcoin processor service reads block information directly from its local MongoDB copy.
   - The spending monitor service supervises predefined maximum write values to prevent network congestion.
   - The lock monitor service fulfills the temporal requirement of BTC locking, which is proportional to the batch size.

3.2 Adherence to self-sovereign identity principles

The compliance level with the ten principles of self-sovereign digital identity (Allen, 2016) across the Sovrin, uPort, Jolocom, ShoCard, Litentry, Civic, KILT, Idena, and ION frameworks is summarized in Figure 3. The compliance level assessment was conducted using the following scale:

1. Non-compliant 0.0: the *framework* does not comply with a specific SSI principle.
2. Low compliance 0.25: the *framework* partially complies with some characteristics of an SSI principle but has significant deficiencies in its implementation.
3. Moderate compliance 0.5: the *framework* complies with a substantial part of an SSI principle but still has some deficiencies.
4. High compliance 0.75: the *framework* implements essential features that allow compliance with an SSI principle but still presents some minor deficiencies.
5. Full compliance 1.0: the *framework* fully complies with an SSI principle.

Figure 3 presents a comprehensive comparative analysis of compliance levels across nine distinct SSI frameworks, evaluated against Allen's ten guiding principles. The visualization employs a stacked bar chart to illustrate the cumulative scores for each framework across all principles, facilitating rapid assessment of overall compliance levels among the frameworks. These principles encompass critical aspects of SSI systems, including access control mechanisms, user consent protocols, individual control over personal data, existence and validity assurance of digital identities, interoperability between diverse solutions, data minimization practices, persistence and portability of digital identities, robust protection measures, and transparency in identity management processes. The aggregate height of each bar represents the total compliance level for a given framework across all principles. The key observations include

1. High performers: Sovrin, uPort, ION, and KILT consistently achieve high scores (0.75–1.00) across most principles, demonstrating comprehensive adherence to SSI standards.
2. Notable gaps: ShoCard exhibits significant deficiencies, scoring 0 in existence, minimization, transparency, portability, and interoperability. Furthermore, ShoCard's source code is not publicly available, limiting transparency and independent verification.
3. Mixed performance: Civic excels in several areas but falls short in existence, portability, and interoperability. Both Civic and ShoCard demonstrate the lowest overall performance, primarily due to their reliance on external identity

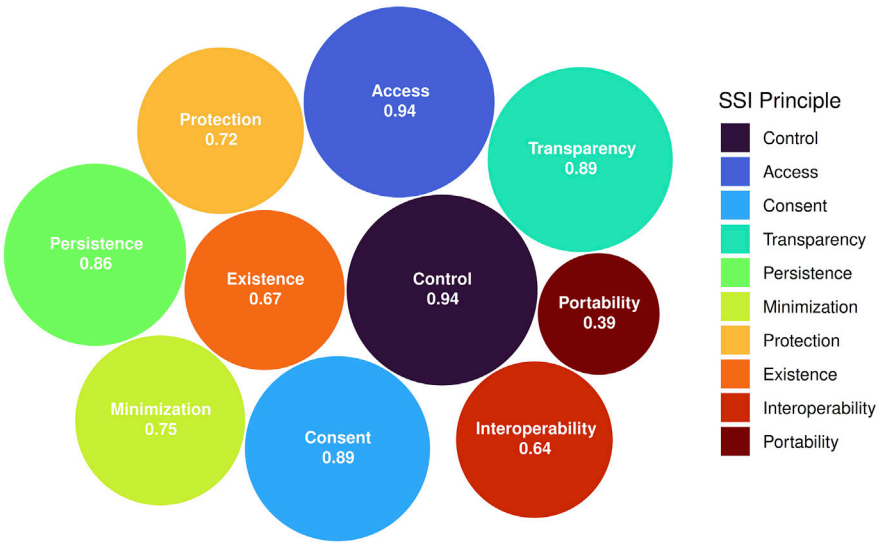


FIGURE 4
Comparative analysis of SSI principles: a bubble hierarchy chart.

validators for identity establishment and their lack of DID method implementation, which impedes interoperability.

4. Moderate compliance: Litentry shows consistent moderate compliance (0.50–0.75) across most principles, indicating a balanced approach to SSI implementation. Partial decentralization: Jolocom exhibits weaknesses in portability and protection, attributed to its partially decentralized network structure that requires a set of trusted nodes for transaction validation.
5. Varied performance: Idena presents a mix of high and low scores, achieving perfect compliance in some areas while completely failing in others, suggesting an uneven implementation of SSI principles.

This analysis provides valuable insights into the strengths and weaknesses of various SSI frameworks, highlighting areas for potential improvement and standardization in the evolving landscape of digital identity management. Section 4 provides a detailed analysis of the degree of compliance with the identity principles in the mentioned frameworks, addressing key aspects and offering a broader perspective on each principle.

4 Discussion

Figure 4 presents a bubble chart hierarchically comparing SSI principles. Each bubble represents an SSI principle, with its size corresponding to the average compliance level across the analyzed frameworks. A detailed analysis of compliance for each principle is provided below.

The principle of existence is effectively implemented in Sovrin, uPort, Jolocom, Idena, and KILT as these frameworks impose no restrictions on the creation of self-sovereign identities. Sovrin enhances this principle by enabling users to generate multiple DIDs (Haddouti and Kettani, 2019). uPort introduces a unique identifier, uPortID, which facilitates cryptographic key rotation without compromising identity integrity (Naik and Jenkins, 2020b). Jolocom empowers users to manage their primary digital identity along with user-defined sub-identities (Jolocom.io (2020)). In contrast, ShoCard (Satybaldy et al., 2020), Civic (Kuperberg, 2020), and Litentry (Litentry Technologies, 2021) deviate from this principle by necessitating pre-existing identities or identity verification for digital identity creation. ShoCard and Civic mandate the presentation of officially established identity documents, such as passports, for identity validation. Litentry, functioning as an identity aggregator, relies on pre-existing identities, potentially introducing vulnerabilities if the source identities lack adequate security or trustworthiness. This dependence on third-party verifiers or existing identities contradicts the fundamental concept of self-sovereignty in digital identity management. ION (Identity Foundation, 2022a), Idena network (2018), and KILT BOTLabs GmbH (2022) further reinforce the existence principle by granting users autonomous control over their cryptographic keys and identity assertions, thus promoting a genuinely self-sovereign approach to digital identity creation and management. uPort distinguishes itself by implementing key update mechanisms that preserve the user's identity integrity throughout the process.

The second principle pertains to the control that users have over their digital identity, ensuring the secure management of their cryptographic keys. The analyzed frameworks excel in providing users with decentralized control over their digital identities, allowing them full ownership and autonomy. Users can decide who accesses their personal information and how it is used. This control is

achieved through blockchain and cryptography technologies, enabling users to manage their digital identities securely without relying on centralized intermediaries. This critical feature empowers users to protect their privacy and maintain control over their online identities. Sovrin, uPort, ION, ShoCard, Jolocom, Civic, Idena, and KILT all provide decentralized control over digital identities, facilitating the management of cryptographic keys and personal information. Sovrin and uPort stand out by offering social key recovery methods and the ability to update identity attributes (Gilani et al., 2020). Additionally, uPort allows modifying cryptographic keys associated with the uPortID upon approval from a previously defined list of delegates (Naik and Jenkins, 2020c). ION provides a recovery key generated during DID creation or key update although it is currently limited to Bitcoin's secp256k1 elliptic curve. Jolocom implements a native key rotation method for compromised private keys (Jolocom.io (2020)). ShoCard and Civic store encrypted information and keys on the user's smartphone but lack key recovery systems (Kuperberg, 2020). Idena network (2022) and KILT BOTLabs GmbH (2022) offer user control over identifiers and DIDs, respectively, without specifying key recovery mechanisms. Litentry, as an identity aggregation layer, partially fulfills this principle, requiring careful application design to ensure user control. These implementations generally allow users to decide who accesses their personal information and how it is used, leveraging blockchain and cryptographic technologies to manage digital identities without centralized intermediaries, thereby enhancing privacy protection and user empowerment in online identity management.

The third principle emphasizes ensuring that users have the authority to grant consent before disclosing their personal information. This principle is implemented in varying degrees across the analyzed SSI frameworks, with most systems prioritizing user control over information disclosure. Sovrin, uPort, ION, Jolocom, Civic, Idena, and KILT demonstrate strong adherence to this principle, allowing users to explicitly authorize access to their PII. Sovrin enables users to determine which DIDs and attributes to disclose (Naik and Jenkins, 2021a), while uPort provides granular permission management for stored personal information (Naik and Jenkins, 2020b). ION gives users full control over their DID state updates and service associations. Jolocom implements mechanisms for granting or revoking access to personal information (Jolocom.io (2020)). Civic allows holders to selectively share data with service providers or authentication authorities (Kuperberg, 2020). Idena and KILT provide user control over identifiers and credentials, respectively. ShoCard allows owner authorization for third-party access to PII, but notably, ShoCard servers may access attributes without explicit consent (Liu et al., 2020). Litentry, as an identity aggregator, requires careful design considerations to ensure proper consent mechanisms. These implementations generally aim to empower users with informed decision-making capabilities regarding their personal information disclosure, aligning with the core tenets of self-sovereign identity management. However, the specific consent mechanisms and their robustness vary across the frameworks, highlighting the need for continued focus on this critical aspect of SSI systems.

The fourth principle centers on the holder's capacity to disclose a minimal amount of information during a transaction. Sovrin, uPort, ION, Jolocom, Civic, and KILT demonstrate full adherence (1.0), implementing robust mechanisms for selective disclosure. Sovrin (Eddine et al., 2021) and KILT utilize ZKP for verifiable credentials, enabling privacy-preserving information sharing. uPort employs smart contracts to minimize identity correlation across dApps and control information disclosure (Gilani et al., 2020). ION focuses on decentralized public key infrastructure deployment, which can be leveraged for PII management use cases. Jolocom incorporates selective disclosure directly into its protocol, offering granular control over verifiable credentials (Jolocom.io (2020)). Civic implements a Merkle tree structure, allowing users to selectively reveal hash fragments of their verified personal information (Satybaldy et al., 2020). Litentry and Idena show partial compliance (0.5 and 0.25, respectively). Litentry's adherence depends on third-party platforms and specific use case designs. Idena, focusing on providing unique identity identifiers, does not store PII directly but can be linked to platforms managing personal attributes. In contrast, ShoCard stands out as non-compliant (0.0), lacking support for selective disclosure (Gilani et al., 2020). This comparative analysis highlights the diverse approaches in implementing the minimization principle across SSI frameworks, with most striving to empower users with granular control over their personal information disclosure.

The fifth principle ensures durable and non-volatile digital identity management. The SSI frameworks exhibit varying approaches to the persistence principle, with most implementing off-ledger storage for PII and prioritizing reliable and enduring solutions for digital identity management. Sovrin, uPort, ION, Civic, and KILT demonstrate full compliance (1.0) with robust off-ledger storage mechanisms. Sovrin utilizes holder-controlled agents over a distributed and decentralized infrastructure, enabling users to uphold their digital identity over time and ensure the security and accessibility of associated personal data, potentially leveraging cloud services for PII storage (Eddine et al., 2021). uPort employs external repositories like IPFS, AWS, or Dropbox, with user profiles in JSON format, which raises potential privacy concerns from metadata analysis (Kaneriya and Patel, 2020; Satybaldy et al., 2020). ION securely stores transactions in IPFS and mongoDB (Identity Foundation, 2022a). Civic encrypts user data in the holder's digital wallet with Google Drive backups, recording data hashes as ERC-20 tokens on the blockchain (Eddine et al., 2021). Litentry shows partial compliance (0.5), linking entity attributes across multiple networks to enable platform-independent identity systems. Idena demonstrates limited compliance (0.25), creating a persistent identifier on its blockchain without storing additional data. ShoCard and Jolocom, despite using off-ledger storage, are rated non-compliant (0.0). ShoCard stores claim hashes on the Bitcoin blockchain and encrypted PII copies on a centralized server (Kuperberg, 2020; Eddine et al., 2021), while Jolocom's architecture allows for adapting external repositories for secure PII storage, enhancing identity longevity and control (Jolocom.io (2020)). In Civic, user data are encrypted within the holder's digital wallet with a backup on Google Drive. The hashes of these data are recorded on the blockchain as an ERC-20 token, revocable by the authentication authority. Trust in identity is contingent upon trust in this actor, exemplified by changes in attribute values (Eddine et al., 2021; Satybaldy et al., 2020). Jolocom's architecture allows for adapting

external repositories for secure PII storage, enhancing identity longevity and control (Jolocom.io (2020); (Gilani et al., 2020)). KILT stores assertions in the holder's wallet, recording hashes of revocable assertions, CTYPE hashes, and payment information using KILT tokens on the DLT. The CTYPE and DID documents are stored in external repositories (BOTLabs GmbH, 2020). This analysis highlights the diverse strategies employed by SSI frameworks to ensure identity persistence, with the most favoring off-ledger storage to enhance security and user control over PII.

The sixth principle, protection, aims to safeguard individual rights by ensuring partial decentralization across all frameworks. Sovrin demonstrates strong adherence (1.0) by implementing a governance framework with trusted nodes (stewards) executing the Plenum consensus protocol based on RBFT (Aublin et al., 2013). It employs pseudonyms for each transaction to mitigate identity correlation risks and supports EU GDPR compliance (Naik and Jenkins, 2021b). uPort, while operating on the Ethereum blockchain, shows partial compliance (0.5) due to potential centralization risks and vulnerabilities in its chasqui messaging service (Gilani et al., 2020; Satybaldy et al., 2020). However, it also supports GDPR compliance (Naik and Jenkins, 2020b). ShoCard exhibits non-compliance (0.0), relying on centralized servers as intermediaries between stakeholders although it ensures KYC and anti-money laundering (AML) regulatory compliance (Kuperberg, 2020). Civic shows partial compliance (0.5) by managing validator nodes through smart contracts, enhancing censorship resistance, but its GDPR compliance remains unclear (Kuperberg, 2020; Eddine et al., 2021). Jolocom, deployed on the Ethereum Rinkeby blockchain with trusted nodes validating transactions, also demonstrates partial compliance (0.5) (Jolocom.io (2020)). ION and KILT both demonstrate full compliance (1.0), with ION focusing on DPKI deployment (Identity Foundation, 2022a) and KILT storing assertions in the holder's wallet while recording hashes on BOTLabs GmbH (2020). Litentry demonstrates moderate adherence (0.5) to the principle by creating a cross-chain identity framework that connects attributes across diverse networks (Litentry Technologies, 2021). Idena shows limited compliance (0.25), focusing on creating persistent identifiers without storing additional data (Idena network, 2018). This analysis highlights the diverse approaches in implementing the protection principle across SSI frameworks, with varying degrees of decentralization and regulatory compliance.

The following principle concerns direct and unrestricted access to digital identity, ensuring secure and controlled access to personal information. SSI frameworks exhibit various strategies for implementing this principle, with most achieving full compliance (1.0) through public blockchain deployments. uPort, ION, ShoCard, Jolocom, Civic, Idena, and KILT all utilize public blockchains to ensure unrestricted access to digital identities. uPort operates on Ethereum, managing transaction costs through its *Sensui* service (Eddine et al., 2021; Naik and Jenkins, 2020b). ION and ShoCard leverage the Bitcoin blockchain, with ShoCard's architecture adaptable to other ledgers (Identity Foundation, 2022a; Gilani et al., 2020). Civic integrates with both Ethereum and Solana, enabling rapid integration of its *Civic Pass* token into dApps Civic (Developer Hub, 2020). Jolocom utilizes the Ethereum *Rinkeby testnet* with a proof-of-authority consensus algorithm (Gilani et al., 2020); Jolocom. io (2020). Sovrin and Litentry exhibit partial compliance (0.75) due to their permissioned blockchain approaches. Sovrin uses *Hyperledger Indy* with writing permissions restricted to trusted nodes although identities remain freely accessible to users (Naik and Jenkins (2021b, 2020a)). Litentry functions as a *Parachain* on *Polkadot*, employing a governance model based on referendum proposals (Litentry Technologies, 2021). ShoCard, initially deployed on the Bitcoin blockchain, has an adaptable architecture that allows integration with other ledgers (Gilani et al., 2020). Civic's integration with Ethereum and Solana facilitates rapid deployment of its Civic Pass token at both the application and blockchain levels (Eddine et al., 2021; Civic Developer Hub, 2020). Jolocom is tested on the Ethereum Rinkeby testnet, utilizing a proof-of-authority consensus algorithm (Jolocom.io (2020)). Idena and KILT adopt unique approaches while maintaining full compliance. Idena deploys its own public blockchain exclusively for managing unique identities, with access secured by user-controlled private keys (Idena network, 2018). KILT uses *Polkadot* with *Parity Substrate*, allowing any entity to create an identity and participate in the network (BOTLabs GmbH, 2020). This analysis underscores the diverse strategies employed by SSI frameworks to ensure accessible yet secure digital identity management, with a notable preference for public blockchain implementations to maximize unrestricted access.

Transparency, the eighth principle, was assessed in terms of licensing, standard usage, and source code availability, allowing users to comprehend how their digital identity is utilized and shared. Notably, Sovrin (Hyperledger Foundation, 2022), uPort (Veramo, 2016), ION (Identity Foundation, 2022a), Civic Technologies Inc., 2020), Jolocom.io (2020), Idena network (2022), Kilt BOTLabs GmbH (2022), and Litentry (2022) all score a perfect 1.0 for transparency, indicating that they are open-source projects that comply with standards established by the W3C. These frameworks provide users with access to their source code, ensuring that the methodologies behind their identity management systems are clear and verifiable. In contrast, ShoCard scores a 0.0 as it employs patented methods and algorithms for identity management, which limits the exposure of its implementation details (Identity, 2020). This lack of transparency may hinder user trust and understanding of how their identities are managed compared to the other frameworks. Overall, the comparative analysis underscores the importance of transparency in fostering user confidence and promoting the adoption of self-sovereign identity solutions.

The ninth principle concerns digital identity portability, which facilitates the convenient and secure transfer of identities across various contexts. Sovrin, despite exhibiting limited portability, distinguishes itself by implementing open standards for verifiable credentials and decentralized identifiers, thereby enhancing interoperability across systems (Naik and Jenkins, 2021b). In contrast, uPort's tight integration with the Ethereum blockchain restricts its portability, limiting its versatility for cross-context applications. Civic faces similar constraints as its system relies on the ERC-20 token CVC for validator nodes to facilitate the sale of verified information to service providers, which further limits its portability (Satybaldy et al., 2020). Jolocom offers a more adaptable

approach with its agnostic protocol, enabling integration with various blockchains such as Bitcoin and BigchainDB although it still encounters some limitations in portability. ShoCard is significantly constrained by its partially centralized management of ShoCardID identifiers, which hinders data export to secondary devices and lacks support for multiple devices, complicating identity migration and deletion processes (Satybaldy et al., 2020; Kuperberg, 2020). Other frameworks, including ION and KILT, show potential for interoperability through the use of open standards, but they do not provide explicit mechanisms for portability, leaving room for improvement in facilitating seamless identity transitions across systems. Overall, the comparative analysis reveals a range of capabilities, with Sovrin demonstrating the highest compliance with the principle of portability, while frameworks such as ShoCard and Civic exhibit substantial limitations.

Finally, the final principle, interoperability, was assessed based on the application of DIDs, the adoption of DID methods, and the formats used for data exchange. The implementation of DID methods facilitates connectivity with the universal resolver, enabling the resolution of decentralized identifiers across various DID methods (Identity Foundation, 2022b). Sovrin, uPort, and Jolocom are aligned with the W3C DID standard. Sovrin uses the did-sov method (version 0.1) and JSON-LD for data formatting, facilitating integration with its public DLT (Identity Foundation, 2022b). uPort employs the did-ethr method (version 2.4.0) and uses JSON files, leveraging a proxy system for communication between smart contracts, which enhances its interoperability across applications (Kaneriya and Patel, 2020). Jolocom adopts the did-jolo method (version 1.0) and employs JSON Web Signature formats, allowing flexible integration with its identity management system, although its interoperability is still confined to systems compatible with universal identifier resolution (Jolocom.io (2020)). In contrast, ShoCard and Civic exhibit notable deficiencies in interoperability. ShoCard lacks a DID connection method and relies on key value-based formats, severely limiting its ability to interact with other systems (Satybaldy et al., 2020). Civic, while adopting the DID standard, does not provide clear documentation on data exchange formats, which impedes its interoperability potential despite its integration with Ethereum (Satybaldy et al., 2020). Overall, Sovrin, uPort, and Jolocom demonstrate robust adherence to interoperability principles through their use of standardized DID methods. In contrast, ShoCard and Civic reveal critical gaps that could hinder their effectiveness within a decentralized identity ecosystem. Idena does not support a DID connection method but is designed to link its identifier to systems requiring a one-to-one user-account relationship, such as social networks (Idena network, 2018).

5 Conclusion

Section 3.2 summarizes the findings from the analysis of SSI frameworks, emphasizing the significance of compatibility with open standards and interoperable protocols. This design approach facilitates seamless integration with diverse systems, ensuring the secure transfer of identity data across different entities and systems—an essential requirement for users interacting with multiple services and organizations that necessitate identity verification. The following technical conclusions can be drawn from our work:

1. Framework performance and compliance: the evaluation of nine prominent SSI frameworks—Sovrin, uPort, ShoCard, Litentry, KILT, Civic, ION, Idena, and Jolocom—against Christopher Allen's ten SSI principles reveals a spectrum of compliance levels. ION, Sovrin, uPort, KILT, and Jolocom emerge as leading frameworks, demonstrating strong alignment with SSI principles. However, no single framework achieves full compliance across all criteria, highlighting the complexity of balancing security, user-centricity, and interoperability in decentralized identity systems.
2. Blockchain as an enabler: the analysis underscores the potential of blockchain technology in addressing digital identity management challenges. Blockchain-based frameworks demonstrate superior capabilities in creating decentralized identities that adhere to interoperability standards, offering a promising solution for secure and user-controlled digital identity management.
3. Interoperability and open standards: a critical finding is the paramount importance of compatibility with open standards and interoperable protocols. Frameworks that prioritize these aspects facilitate seamless integration across diverse systems and enable secure transfer of PII. This interoperability is crucial for users interacting with multiple services and organizations requiring identity verification.
4. Variability in framework approaches: the evaluation reveals diverse approaches among the frameworks. For instance, Sovrin, uPort, and Jolocom employ trust-based decentralized identity models with verifiable identity systems and decentralized governance. This diversity in approaches contributes to the richness of the SSI ecosystem but also highlights the need for standardization.
5. Identified gaps and challenges: some frameworks, such as ShoCard and Civic, demonstrate significant gaps, particularly in areas like existence, portability, and interoperability. These shortcomings are often linked to reliance on external identity validators and lack of DID method implementation, pointing to areas requiring focused improvement.
6. Trade-offs in SSI implementation: the analysis reveals inherent trade-offs between different SSI principles. Future development of SSI solutions must address these trade-offs to meet the multifaceted needs of users, organizations, and regulatory bodies effectively.
7. Implications for future research and development: this comprehensive assessment provides a critical roadmap for advancing the design, implementation, and adoption of SSI frameworks. It highlights the need for continued research to address current limitations and further align frameworks with SSI principles.
8. Paradigm shift in digital identity management: the evaluation indicates a significant paradigm shift toward decentralized, user-centric identity management. This transition presents both opportunities and challenges for stakeholders across the digital identity ecosystem.

Finally, while significant progress has been made in developing SSI frameworks that align with key principles of decentralized identity management, there remains substantial room for improvement and standardization. The findings of this study serve as a valuable foundation for researchers, developers, and policymakers to drive the evolution of a more secure, human-centric, and interoperable digital identity landscape. As the field progresses, addressing the identified challenges and leveraging the strengths of blockchain technology will be crucial in realizing the full potential of self-sovereign identity systems.

Author contributions

RP: conceptualization, investigation, methodology, writing–original draft, and writing–review and editing. JG-R: investigation, supervision, writing–original draft, and writing–review and editing, DL-S: investigation, project administration, writing–original draft, and writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

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

Publisher's note

References

Alizadeh, M., Andersson, K., and Schelen, O. (2022). Comparative analysis of decentralized identity approaches. *IEEE Access* 10, 92273–92283. doi:10.1109/ACCESS.2022.3202553

Allen, C. (2016). Self-sovereing identity principles. Available at: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md (Accessed May 6, 2024).

Aublin, P.-L., Mokhtar, S.-B., and Quéma, V. (2013). "Rbft: redundant byzantine fault tolerance," in *2013 IEEE 33rd international conference on distributed computing systems*, 297–306. doi:10.1109/ICDCS.2013.53

BOTLabs GmbH (2020). Kilt protocol - white paper. Available at: https://www.kilt.io/wp-content/uploads/2020/01/KILT-White-Paper-v2020-Jan-15.pdf (Accessed May 23, 2023).

BOTLabs GmbH (2022). Kilt protodol: Kilt is a blockchain protocol for issuing self-sovereign verifiable, revocable, anonymous credentials in the web 3.0. Available at: https://github.com/KILTprotocol (Accessed October 01, 2023).

Civic Technologies Inc (2020). Civic wallet - digital wallet for money and cryptocurrency. Available at: https://github.com/civicteam (Accessed July 23, 2023).

Coinmarketcap (2024). Kilt Protocol precio, gráficos, capitalización bursátil y otras métricas vert CoinMarketCap. Available at: https://coinmarketcap.com/currencies/kiltprotocol/(Accessed July 23, 2023).

Developer Hub, C. (2020). Civic: we provide on-chain identity layer creating trust across web3. Available at: https://docs.civic.com/(Accessed September 29, 2023).

Dib, O., and Toumi, K. (2020). Decentralized identity systems: architecture, challenges, solutions and future directions. *Ann. Emerg. Technol. Comput.* 4, 19–40. doi:10.33166/AETiC.2020.05.002

Dunphy, P., and Petitcolas, F. A. (2018). A first look at identity management schemes on the blockchain. *IEEE Secur. Priv.* 16, 20–29. doi:10.1109/MSP.2018.3111247

Eddine, B. N., Ouaddah, A., and Mezrioui, A. (2021). "Exploring blockchain-based self sovereign identity systems: challenges and comparative analysis," in *2021 3rd conference on blockchain research and applications for innovative networks and services, BRAINS 2021*, 21–22. doi:10.1109/BRAINS52497.2021.9569821

Etherscan (2022). The ethereum blockchain explorer. Available at: https://etherscan.io/(Accessed September 28, 2023).

Ferdous, S., Chowdhury, F., and Alassafi, M. (2019). In search of self-sovereign identity leveraging blockchain technology. *IEEE Access* 7, 103059–103079. doi:10.1109/ACCESS.2019.2931173

Gilani, K., Bertin, E., Hatin, J., and Crespi, N. (2020). "A survey on blockchain-based identity management and decentralized privacy for personal data," in *2020 2nd conference on blockchain research and applications for innovative networks and services, BRAINS 2020*, 97–101. doi:10.1109/BRAINS49436.2020.9223312

Graph Foundation (2022). The graph: Apis for a vibrant decentralized future. Available at: https://thegraph.com/en/(Accessed September 28, 2023).

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation Technol.* 9, 159–189. doi:10.1080/17579961.2017.1377914

Haddouti, S., and Kettani, E.-C. (2019). Analysis of identity management systems using blockchain technology. *2019 Int. Conf. Adv. Commun. Technol. Netw. (CommNet)* 10, 1–7. doi:10.1109/COMMNET.2019.8742375

Heng, H. (2017). "The application of blockchain technology in e-government in China," in *2017 26th international conference on computer communication and networks (ICCCN)*, 1–4. doi:10.1109/ICCCN.2017.8038519

Hyperledger Foundation (2022). Hyperledger indy. Available at: https://github.com/hyperledger/indy-sdk (Accessed June 16, 2024).

Idena network (2018). Idena: cryptoidentity is the building block for web 3.0. Available at: https://docs.idena.io/(Accessed September 30, 2023).

Idena network (2022). Idena: proof-of-person blockchain. it allows for proof of humanity and uniqueness for its participants by running ai-hard turing test globally at the same time. Available at: https://github.com/idena-network (Accessed September 30, 2023).

Identity, P. (2020). Shocard: it's your identity. own it. Available at: https://www.shocard.com/(Accessed June 28, 2023).

Identity Foundation (2021a). Sidetree protocol. Available at: https://github.com/decentralized-identity/sidetree (Accessed November 11, 2023).

Identity Foundation (2021b). Universal resolver driver for identity overlay network (ion) dids v1. Available at: https://github.com/decentralized-identity/uni-resolver-driver-did-ion (Accessed September 30, 2023).

Identity Foundation (2022a). The identity overlay network (ion). Available at: https://github.com/decentralized-identity/ion (Accessed September 30, 2023).

Identity Foundation (2022b). Universal resolver. Available at: https://github.com/decentralized-identity/universal-resolver/(Accessed June 09, 2023).

Jolocom, io (2020). Jolocom: own your digital self. Available at: https://github.com/jolocom (Accessed May 17, 2024).

Kaneriya, J., and Patel, H. (2020). "A comparative survey on blockchain based self sovereign identity system," in *Proceedings of the 3rd international conference on intelligent sustainable systems* (Thoothukudi, India: ICISS), 1150–1155. doi:10.1109/ICISS49785.2020.9315899

Kiva (2020). Kiva protocol - building the credit bureau of the future. Available at: https://www.kiva.org/protocol (Accessed April 28, 2024).

Kondova, G., and Erbguth, J. (2020). "Self-sovereign identity on public blockchains and the gdpr," in *Proceedings of the ACM symposium on applied computing* (New York, NY, USA: Association for Computing Machinery), SAC '20), 342–345. doi:10.1145/3341105.3374066

Kuperberg, M. (2020). Blockchain-based identity management: a survey from the enterprise and ecosystem perspective. *IEEE Trans. Eng. Manag.* 67, 1008–1027. doi:10.1109/TEM.2019.2926471

Li, Y., Yazdanmehr, A., Wang, J., and Rao, H. R. (2019). Responding to identity theft: a victimization perspective. *Decis. Support Syst.* 121, 13–24. doi:10.1016/j.dss.2019.04.002

Litentry (2022). Litentry. Available at: https://github.com/litentry/(Accessed September 28, 2023).

Litentry Technologies (2021). Litentry network. Available at: https://docs.litentry.com/parachain/get-started/litentry-network (Accessed May 17, 2023).

Liu, Y., He, D., Obaidat, M., Kumar, N., Khan, M., and Raymond-Choo, K.-K. (2020). Blockchain-based identity management systems: a review. *J. Netw. Comput. Appl.* 166, 102731. doi:10.1016/j.jnca.2020.102731

Naik, N., and Jenkins, P. (2020a). "Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems," in *Isse 2020 - 6th IEEE international symposium on systems engineering, proceedings* (Vienna, Austria: Institute of Electrical and Electronics Engineers Inc.), 1–6. doi:10.1109/ISSE49799.2020.9272212

Naik, N., and Jenkins, P. (2020b). "Uport open-source identity management system: an assessment of self-sovereign identity and user-centric data platform built on blockchain," in *Isse 2020 - 6th IEEE international symposium on systems engineering, proceedings* (Vienna, Austria: Institute of Electrical and Electronics Engineers Inc.), 1–7. doi:10.1109/ISSE49799.2020.9272223

Naik, N., and Jenkins, P. (2020c). "Your identity is yours: take back control of your identity using gdpr compatible self-sovereign identity," in *Proceedings of 2020 7th IEEE international conference on behavioural and social computing, BESC 2020* (Bournemouth, United Kingdom: Institute of Electrical and Electronics Engineers Inc.), 1–6. doi:10.1109/BESC51023.2020.9348298

Naik, N., and Jenkins, P. (2021a). "Does sovrin network offer sovereign identity?," in *Isse 2021 - 7th IEEE international symposium on systems engineering, proceedings* (Vienna, Austria: Institute of Electrical and Electronics Engineers Inc.), 1–6. doi:10.1109/ISSE51541.2021.9582472

Naik, N., and Jenkins, P. (2021b). "Sovrin network for decentralized digital identity: analysing a self-sovereign identity system based on distributed ledger technology," in *Isse 2021 - 7th IEEE international symposium on systems engineering, proceedings* (Vienna, Austria: Institute of Electrical and Electronics Engineers Inc.), 1–6. doi:10.1109/ISSE51541.2021.9582551

Nawari, N. O., and Ravindran, S. (2019). Blockchain technology and BIM process: review and potentialapplications. *J. Inf. Technol. Constr.* 24, 209–238.

OnFinality (2022). Blockchain infrastructure made smarter. Available at: https://www.onfinality.io/(Accessed January 28, 2024).

Parity Technologies (2020). Parity substrate: build your own blockchain. Available at: https://www.parity.io/technologies/substrate/(Accessed November 23, 2023).

Pava-Diaz, R., Paez-Mendez, R., and Niño-Vasquez, L. (2023). A bibliometric study of scientific production on self-sovereign identity. *Ingeniería* 28, e19656. doi:10.14483/23448393.19656

Pava-Diaz, R., Paez-Mendez, R., Niño-Vasquez, L., and Lopez-Sarmiento, D. (2022). Preprocesamiento de publicaciones acerca de indentidad digital descentralizada y autogobernada. Available at: https://figshare.com/articles/dataset/dx_doi_org_10_6084_m9_figshare_6025748/6025748 Accessed: 15 May 2024

Peck, M. E. (2017). Blockchains: how they work and why they'll change the world. *IEEE Spectr.* 54, 26–35. doi:10.1109/MSPEC.2017.8048836

Priisalu, J., and Ottis, R. (2017). Personal control of privacy and data: Estonian experience. *Health Technol.* 7, 441–451. doi:10.1007/s12553-017-0195-1

Satybaldy, A., Nowostawski, M., and Ellingsen, J. (2020). "Self-sovereign identity systems: evaluation framework" in *IFIP advances in information and communication technology* (Paris, France: LNCS), 576, 447–461. doi:10.1007/978-3-030-42504-3_28

ShoCard Inc (2017). Identity management verified using the blockchain. Available at: https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf (Accessed January 12, 2024).

Sicilia, M. A., and Visvizi, A. (2019). Blockchain and oecd data repositories: opportunities and policymaking implications. *Libr. Hi Tech.* 37, 30–42. doi:10.1108/LHT-12-2017-0276

Sovrin Foundation (2019). Sovrin governance framework. Available at: https://sovrin.org/library/sovrin-governance-framework/(Accessed May 05, 2024).

Stokkink, Q., Ishmaev, G., Epema, D., and Pouwelse, J. (2021). "A truly self-sovereign identity system," in *2021 IEEE 46th conference on local computer networks (LCN)*, 1–8. doi:10.1109/LCN52139.2021.9525011

The ID2020 Alliance (2019). The ID2020 Alliance is a global partnership maximizing the potential of digital ID to improve lives. Available at: https://id2020.org/(Accessed June 11, 2023).

Veramo (2016). Veramo core development: tools for verifiable data and ssi. Available at: https://github.com/uport-project/(Accessed May 16, 2024).

W3C Community Group (2022). Webassembly. Available at: https://webassembly.org//(Accessed May 23, 2023).

Wang, F., and De Filippi, P. (2020). Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion. *Front. Blockchain* 2. doi:10.3389/fbloc.2019.00028

Web3 Foundation (2017). Polkadot: vision for a heterogeneous multi-chain framework. Available at: https://polkadot.network/PolkaDotPaper.pdf (Accessed February 27, 2024).

Web3 Foundation (2022). Kusama: Polkadot's canary network. Available at: https://guide.kusama.network/docs/kusama-getting-started (Accessed January 27, 2024).

Windley, P. J. (2021). Sovrin: an identity metasystem for self-sovereign identity. *Front. Blockchain 4* 4. doi:10.3389/fbloc.2021.6267262021.626726